Safety Risk Management for Medical Devices

Elahi, Bijan

DOI
10.1016/B978-0-323-85755-0.00042-4

Publication date
2022

Document Version
Final published version

Citation (APA)
Elahi, B. (2022). *Safety Risk Management for Medical Devices*. (2nd ed.) Elsevier.
https://doi.org/10.1016/B978-0-323-85755-0.00042-4

About the author

Award-winning, international educator, author, and consultant

Bijan Elahi has worked in risk management for medical devices for over 28 years at the largest medical device companies in the world, as well as small startups. He is the Medtronic corporate Advisor and Technical Fellow on safety risk management of medical devices. Bijan is also a lecturer at the Drexel University (United States), the Delft University of Technology (the Netherlands), and the Eindhoven University of Technology (the Netherlands), where he teaches risk management to doctoral students in engineering.

He offers education and consulting on risk-management worldwide. Bijan is a frequently invited speaker at professional conferences and is also a contributor to ISO 14971, the international standard on the application of risk management to medical devices.

bijan@medtechsafety.com

https://medtechsafety.com

Acknowledgments

The creation of this book reflects my life's journey through 40 years of engineering, a journey that has been touched and influenced by many people and organizations, far too many to list here. But I want to acknowledge and thank a few individuals and organizations who most directly have contributed to this book.

- First and foremost, my wife Jamie, for her constant support, and being a non-technical reviewer of my manuscript to ensure smooth and fluent readability.
- Mr. Sandy Weininger, PhD, Division of Biomedical Physics (DBP), Office of Science and Engineering Laboratories (OSEL), Center for Devices and Radiological Health (CDRH) – the United States Food and Drug Administration (FDA), who reviewed my manuscript.
- Mr. M.L., Technical Specialist, Active Implantable Medical Devices, British Standards Institution (BSI), who reviewed my manuscript.
- Ms. Magdalena Scheijgrond who introduced me to Elsevier Publishing.

For permission to make quotations and references to many international standards, I am grateful to BSI:

> *Permission to reproduce extracts from British Standards is granted by BSI Standards Limited (BSI). No other use of this material is permitted. British Standards can be obtained in PDF or hard copy formats from the BSI online shop.*
>
> ***http://www.bsigroup.com/Shop.***

And finally, I thank my students and colleagues who encouraged me to write this book to capture the best knowledge and practices in medical device risk management.

Appendix A: Glossary

Term	Definition
ADE	Adverse Device Effect
AE	Adverse Event
AFAP	As Far As Possible; equivalent to ALAP
ALAP	As Low As Possible; equivalent to AFAP
ALARA	As Low As Reasonably Achievable
ALARP	As Low As Reasonably Practicable
Benefit	Positive impact or desirable outcome of the use of a medical device on the health of an individual, or a positive impact on patient management or public health [1]. In the context of risk management, benefit refers to Clinical Benefit and is defined as: positive impact or desirable outcome of a diagnostic procedure or therapeutic intervention on the health of an individual or a positive impact on patient management or public health. Benefits can be described in terms of magnitude, probability and duration, among others [17].
BRA	Benefit-Risk Analysis
CAPA	Corrective and Preventive Actions
CCF	Common Cause Failure
CDRH	Center for Devices and Radiological Health – part of US FDA
CE	Clinical Evaluation
CFR	Code of Federal Regulation
CHL	Clinical Hazards List
CIP	Clinical Investigation Plan
CRC	Cyclic Redundancy Check
DFMEA	Design Failure Modes and Effects Analysis
DMR	Device Master Record

(*Continued*)

(Continued)

Term	Definition
EMBASE	Database published by Elsevier, contains over 11 million records with over 500,000 citations added annually. EMBASE's international journal collection contains over 5000 biomedical journals from 70 countries.
Essential Design Output (EDO)	Those design outputs that are essential to the proper functioning of the device – those functions that are related to safety and efficacy [21 CFR Section 820.30].
Essential Performance	Performance of a clinical function, other than that related to basic safety, where loss or degradation beyond the limits specified by the manufacturer results in an unacceptable risk.
Essential Requirements	MDD/AIMDD Annex I. Requirements having to do with safe and effective performance of medical devices.
Eudamed	European Databank of Medical Devices
Failure	Inability of an entity to achieve its purpose. This could be with no faults.
Failure Mode	The manner in which a product (system, sub-system, or component) can fail to perform its desired function, or meet its process or design requirements.
Fault	An anomalous condition for a part. Could result in failures.
FCA	Field Corrective Action – an action taken by a manufacturer on a marketed product for technical or medical reasons to prevent or reduce the risk of a serious incident.
FMEA	Failure Modes and Effects Analysis
FSCA	Field Safety Corrective Action – corrective action taken by a manufacturer for technical or medical reasons to prevent or reduce the risk of a serious incident in relation to a device made available on the market [2].
FSN	Field Safety Notice
FT	Fault Tree
FTA	Fault Tree Analysis
GSPR	General Safety and Performance Requirements
GUI	Graphical User Interface
HAL	Harms Assessment List

(Continued)

(Continued)

Term	Definition
HHA, HHE	Health Hazard [Analysis, Appraisal, Evaluation]
HiPPO	Highest Paid Person in the Office
HS	Hazardous Situation
IB	Investigator's Brochure
ICH	International Conference for Harmonization
IFU	Information for Use
IMDRF	International Medical Device Regulators Forum http://www.imdrf.org/
INCOSE	International Council on Systems Engineering
IS	Information for Safety
ISAO	Information Sharing Analysis Organization
KOL	Key Opinion Leader
Legacy Device	Medical device which was legally placed on the market and is still marketed today but for which there is insufficient objective evidence that it is in compliance with the current version of ISO 14971.
Legacy software	Medical Device Software which was legally placed on the market and is still marketed today but for which there is insufficient objective evidence that it was developed in compliance with the current version of the standard IEC 62304 [10].
MD	Medical Doctor; Physician
MDCG	Medical Device Coordination Group
MDD	Medical Device Directive
MDR	Medical Device Reporting – Mandatory reporting requirement to the FDA
MDR	EU 2017/745 Medical Device Regulation
ME	Medical Electrical equipment/systems
MedDRA	Medical Dictionary for Regulatory Activities https://www.meddra.org/
MedTech	Medical Technology

(*Continued*)

(Continued)

Term	Definition
NB	Notified Body
NBRG	Notified Bodies Recommendation Group
OJEU	Official Journal of the European Union
OR	Operating Room
PFD	Process Flow Diagram
PFMEA	Process Failure Modes and Effects Analysis
PHA	Preliminary Hazard Analysis
PM	Protective Measure
PMCF	Post-Market Clinical Follow-up
PMOA	Primary Mode of Action
PMS	Post-Market Surveillance
PMSR	Post-Market Surveillance Report
Pre-clinical Test	Bench test, or animal test
PSUR	Periodic Safety Update Report
QC	Quality Control
QMS	Quality Management System
R&D	Research and Development team/organization
RACT	Risk Assessment and Control Table
RC	Risk Control
RFD	Request for Designation (regarding combination devices)
RM	Risk Management
RMF	Risk Management File
RMP	Risk Management Plan
RMR	Risk Management Report
RMT	Risk Management Team
RPM	Revolutions per Minute
RPN	Risk Priority Number

(*Continued*)

(Continued)

Term	Definition
SADE	Serious Adverse Device Effect
SAE	Serious Adverse Event
SaMD	Software as a Medical Device
SD	Inherently Safe Design and Manufacture
Serious Incident	Any incident that directly or indirectly led, might have led, or might lead to any of the following: (a) the death of a patient, user or other person; (b) the temporary or permanent serious deterioration of a patient's, user's or other person's state of health; (c) a serious public health threat [2].
SFMEA	Software Failure Modes and Effects Analysis
SME	Subject Matter Expert
Software defect	An error in design/implementation of the software.
Software failure	A software condition that causes the System not to perform according to its specification.
Software fault	A software condition that causes the software not to perform as intended.
Software Item	Any identifiable part of a computer program, i.e., source code, object code, control code, control data, or a collection of these items [10].
Software System	Integrated collection of Software Items organized to accomplish a specific function or set of functions [10].
Software Unit	Software Item that is not subdivided into other items [10].
SOP	Standard Operating Procedure
SoS	System of Systems
SOTA	State of the Art
SOUP	Software of Unknown Provenance
SSCP	Summary of Safety and Clinical Performance
Standard of Care	• The level at which the average, prudent clinical care provider would practice; • Appropriate treatment based on scientific evidence and collaboration between professionals.

(*Continued*)

(Continued)

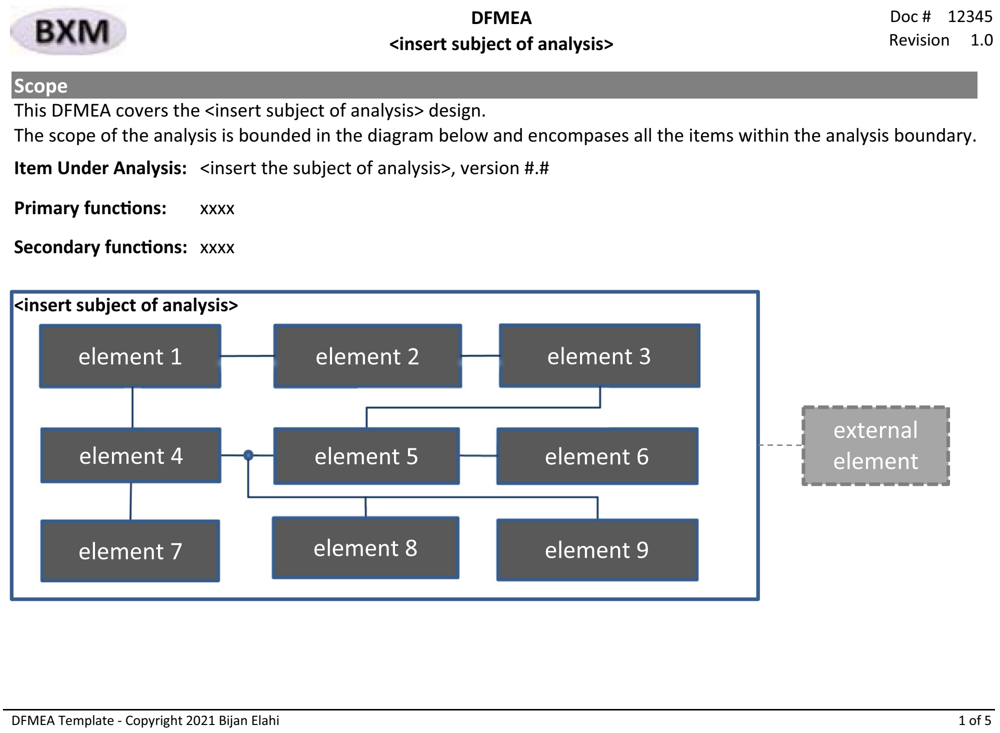
Term	Definition
State of the Art	Developed stage of technical capability at a given time as regards products, processes, and services, based on the relevant consolidated findings of science, technology and experience [1].
SW	Software
TBD	To Be Determined
UI	User Interface
UMFMEA	Use-Misuse Failure Modes and Effects Analysis
USA	United States of America
Use Error	User action or lack of user action while using the medical device that leads to a different result than that intended by the manufacturer or expected by the user [19].
VF	Ventricular Fibrillation

Appendix B: Templates

In the following pages certain templates are provided as an aid to risk management practitioners.

- DFMEA template
- SFMEA template
- PFMEA template
- UMFMEA template
- RACT template

B.1 DFMEA TEMPLATE



BXM

DFMEA
<insert subject of analysis>

Doc # 12345
Revision 1.0

Scope

This DFMEA covers the <insert subject of analysis> design.
The scope of the analysis is bounded in the diagram below and encompases all the items within the analysis boundary.

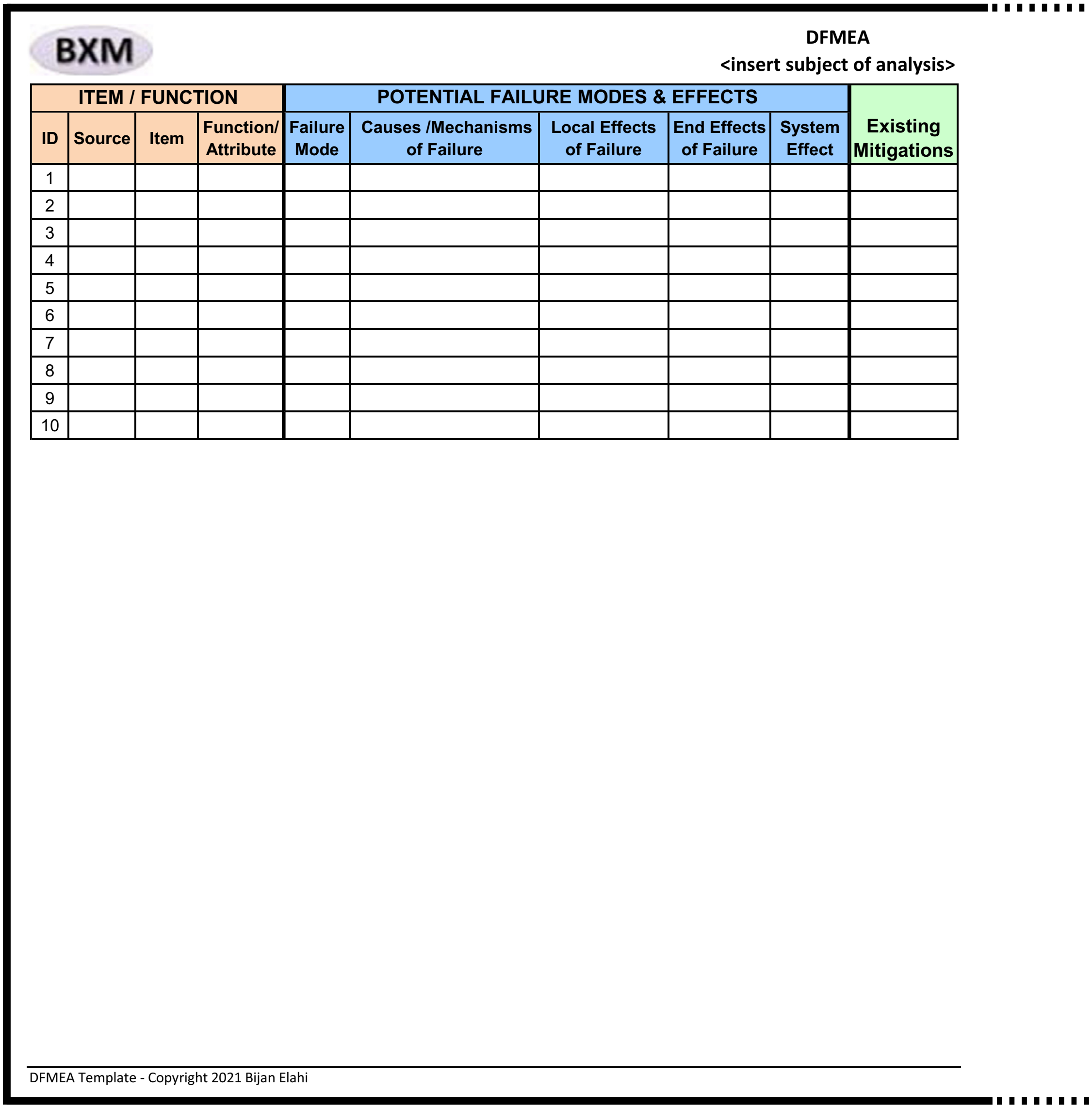
Item Under Analysis: <insert the subject of analysis>, version #.#

Primary functions: xxxx

Secondary functions: xxxx

<insert subject of analysis>
element 1
element 2
element 3
element 4
element 5
element 6
element 7
element 8
element 9
external element

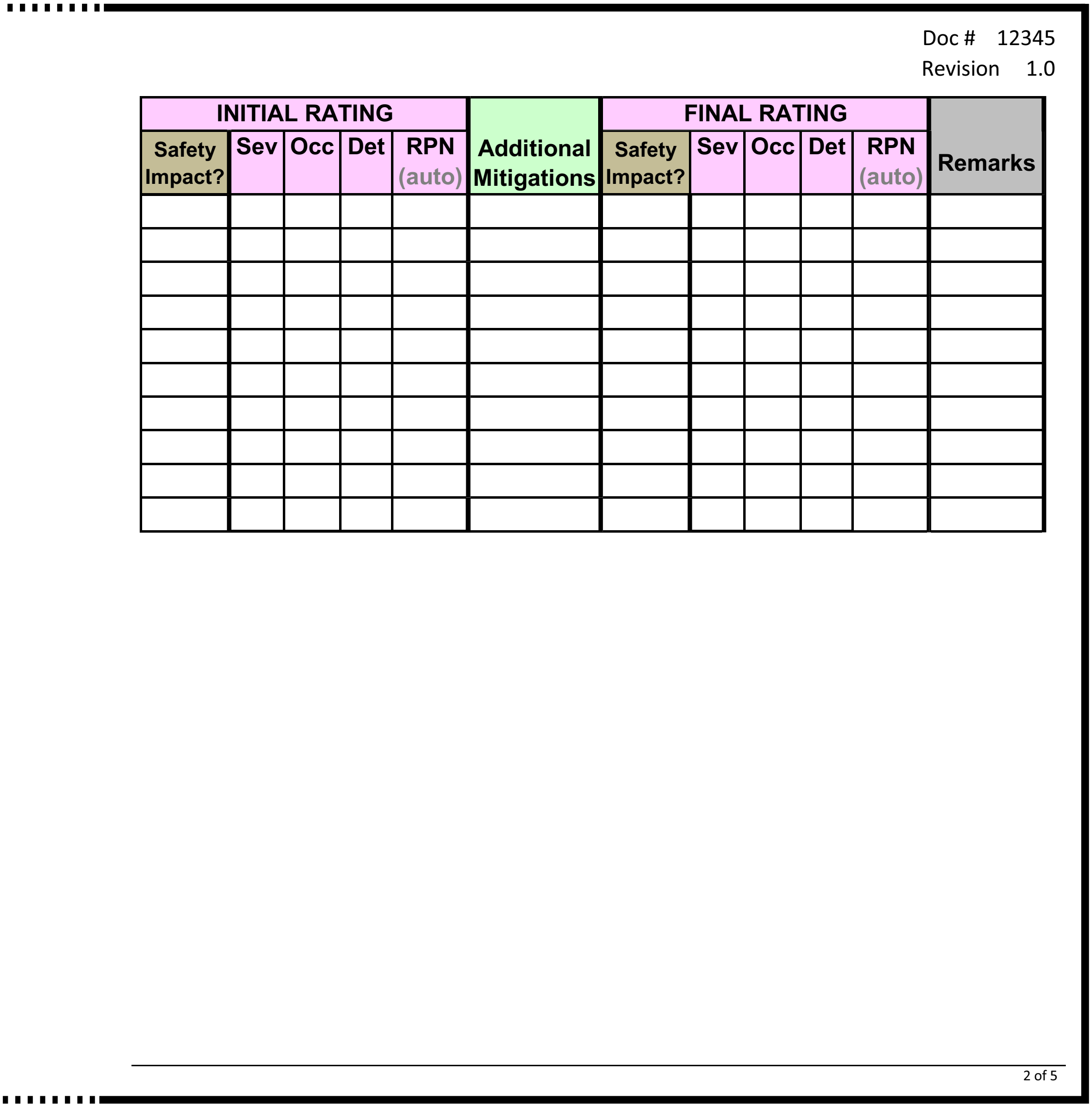
DFMEA Template - Copyright 2021 Bijan Elahi 1 of 5



BXM

DFMEA
<insert subject of analysis>

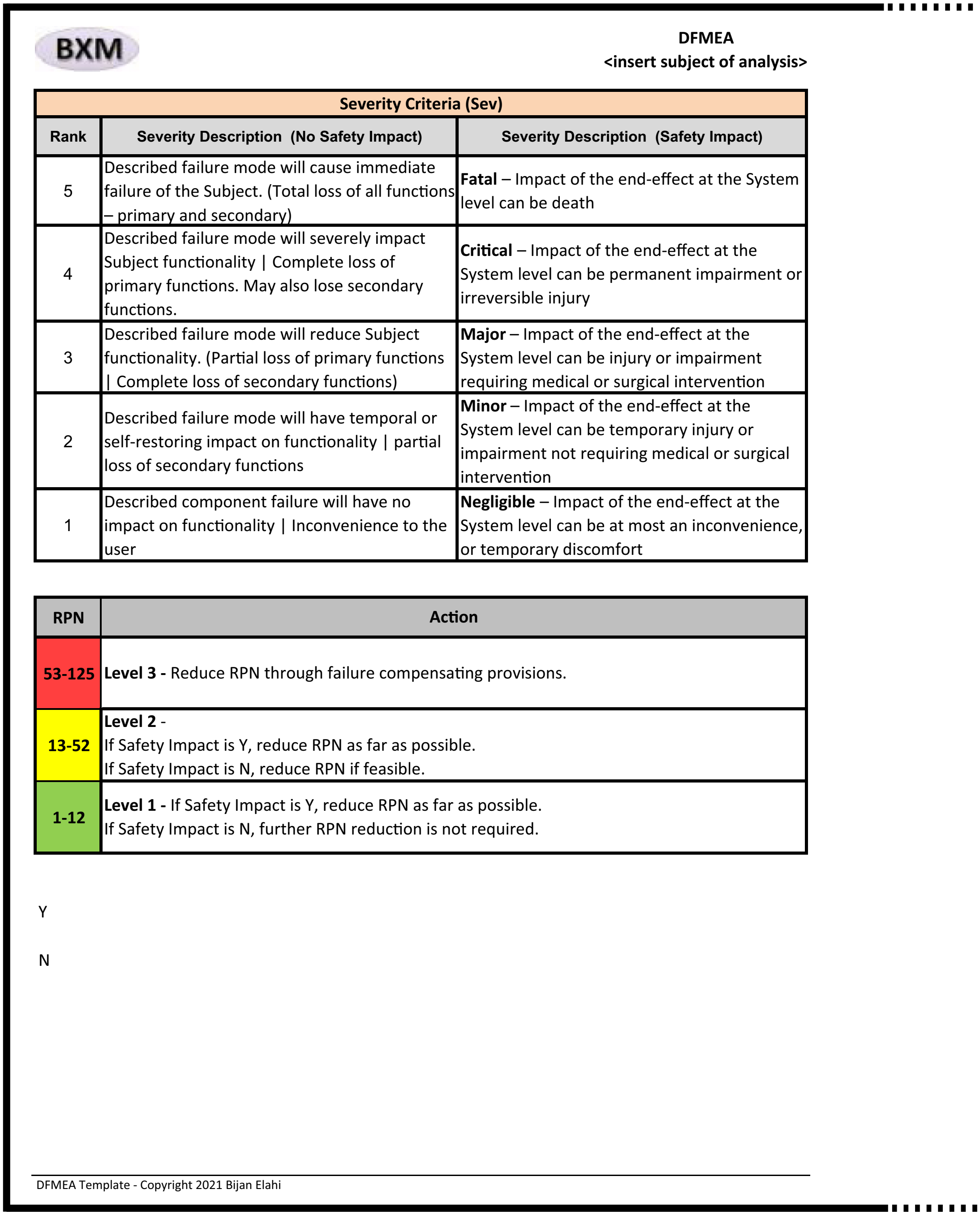
ITEM / FUNCTION				POTENTIAL FAILURE MODES & EFFECTS					Existing Mitigations
ID	Source	Item	Function/ Attribute	Failure Mode	Causes /Mechanisms of Failure	Local Effects of Failure	End Effects of Failure	System Effect	
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									



Doc # 12345
Revision 1.0

INITIAL RATING					Additional Mitigations	FINAL RATING					Remarks
Safety Impact?	Sev	Occ	Det	RPN (auto)		Safety Impact?	Sev	Occ	Det	RPN (auto)	

2 of 5



BXM

DFMEA
<insert subject of analysis>

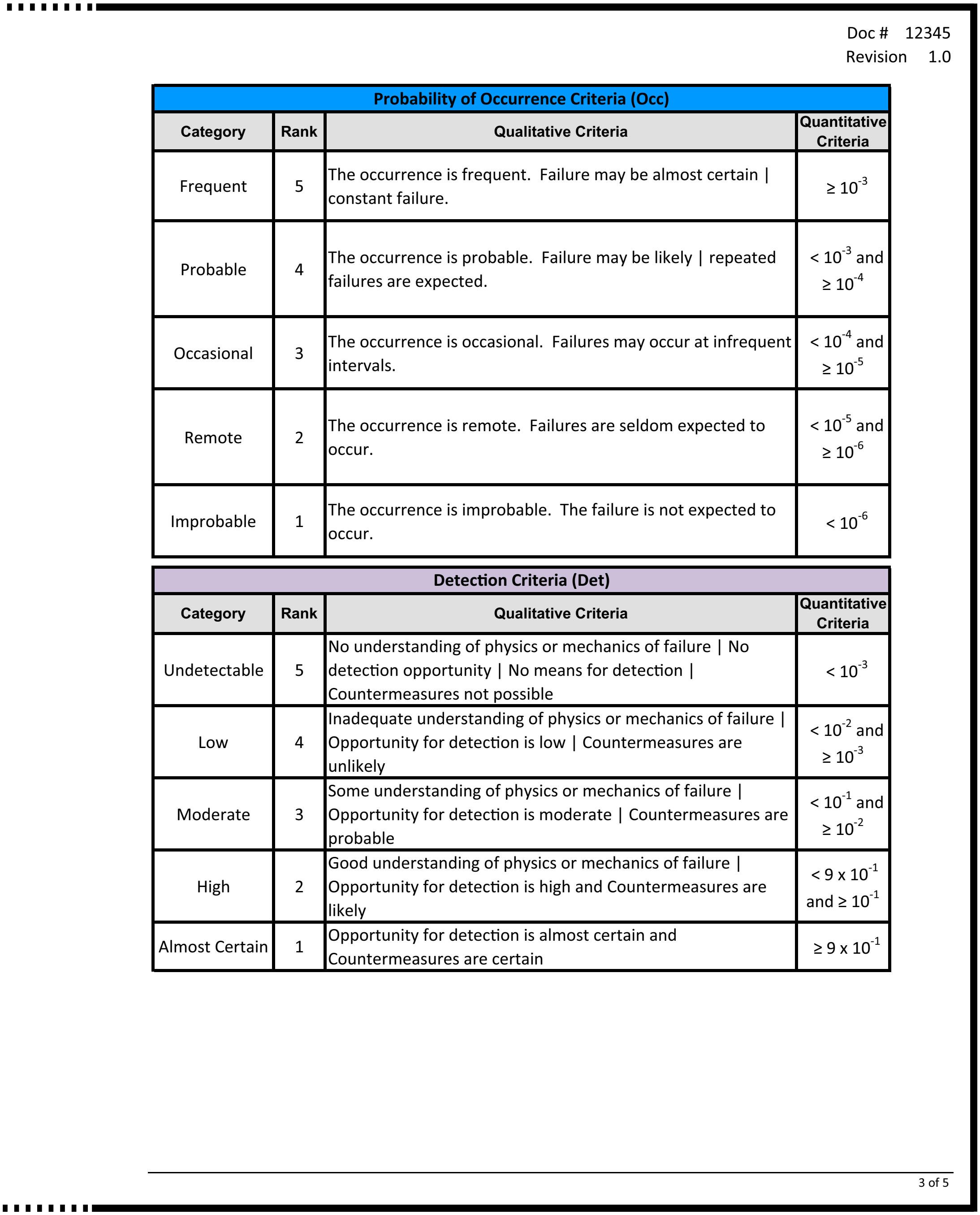
Severity Criteria (Sev)		
Rank	**Severity Description (No Safety Impact)**	**Severity Description (Safety Impact)**
5	Described failure mode will cause immediate failure of the Subject. (Total loss of all functions – primary and secondary)	**Fatal** – Impact of the end-effect at the System level can be death
4	Described failure mode will severely impact Subject functionality | Complete loss of primary functions. May also lose secondary functions.	**Critical** – Impact of the end-effect at the System level can be permanent impairment or irreversible injury
3	Described failure mode will reduce Subject functionality. (Partial loss of primary functions | Complete loss of secondary functions)	**Major** – Impact of the end-effect at the System level can be injury or impairment requiring medical or surgical intervention
2	Described failure mode will have temporal or self-restoring impact on functionality | partial loss of secondary functions	**Minor** – Impact of the end-effect at the System level can be temporary injury or impairment not requiring medical or surgical intervention
1	Described component failure will have no impact on functionality | Inconvenience to the user	**Negligible** – Impact of the end-effect at the System level can be at most an inconvenience, or temporary discomfort

RPN	Action
53-125	**Level 3 -** Reduce RPN through failure compensating provisions.
13-52	**Level 2 -** If Safety Impact is Y, reduce RPN as far as possible. If Safety Impact is N, reduce RPN if feasible.
1-12	**Level 1 -** If Safety Impact is Y, reduce RPN as far as possible. If Safety Impact is N, further RPN reduction is not required.

Y

N

DFMEA Template - Copyright 2021 Bijan Elahi

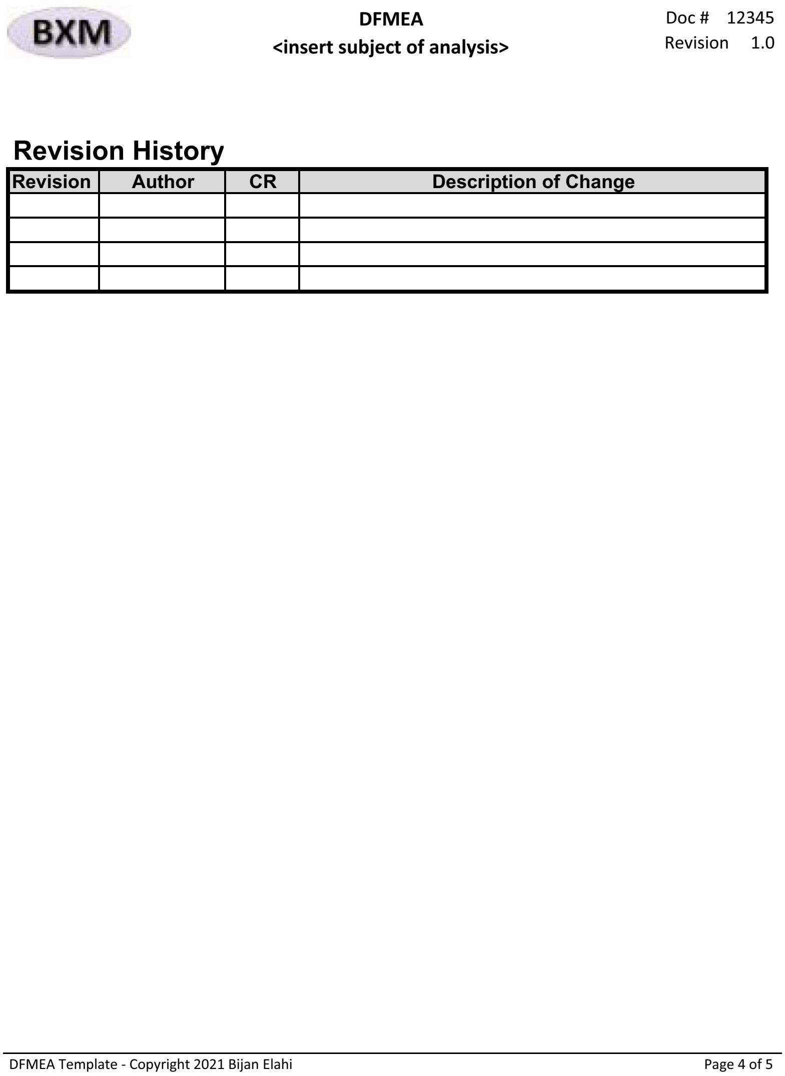


Doc # 12345
Revision 1.0

Probability of Occurrence Criteria (Occ)			
Category	**Rank**	**Qualitative Criteria**	**Quantitative Criteria**
Frequent	5	The occurrence is frequent. Failure may be almost certain | constant failure.	≥ 10^{-3}
Probable	4	The occurrence is probable. Failure may be likely | repeated failures are expected.	< 10^{-3} and ≥ 10^{-4}
Occasional	3	The occurrence is occasional. Failures may occur at infrequent intervals.	< 10^{-4} and ≥ 10^{-5}
Remote	2	The occurrence is remote. Failures are seldom expected to occur.	< 10^{-5} and ≥ 10^{-6}
Improbable	1	The occurrence is improbable. The failure is not expected to occur.	< 10^{-6}

Detection Criteria (Det)			
Category	**Rank**	**Qualitative Criteria**	**Quantitative Criteria**
Undetectable	5	No understanding of physics or mechanics of failure | No detection opportunity | No means for detection | Countermeasures not possible	< 10^{-3}
Low	4	Inadequate understanding of physics or mechanics of failure | Opportunity for detection is low | Countermeasures are unlikely	< 10^{-2} and ≥ 10^{-3}
Moderate	3	Some understanding of physics or mechanics of failure | Opportunity for detection is moderate | Countermeasures are probable	< 10^{-1} and ≥ 10^{-2}
High	2	Good understanding of physics or mechanics of failure | Opportunity for detection is high and Countermeasures are likely	< 9 x 10^{-1} and ≥ 10^{-1}
Almost Certain	1	Opportunity for detection is almost certain and Countermeasures are certain	≥ 9 x 10^{-1}

3 of 5



BXM

DFMEA
<insert subject of analysis>

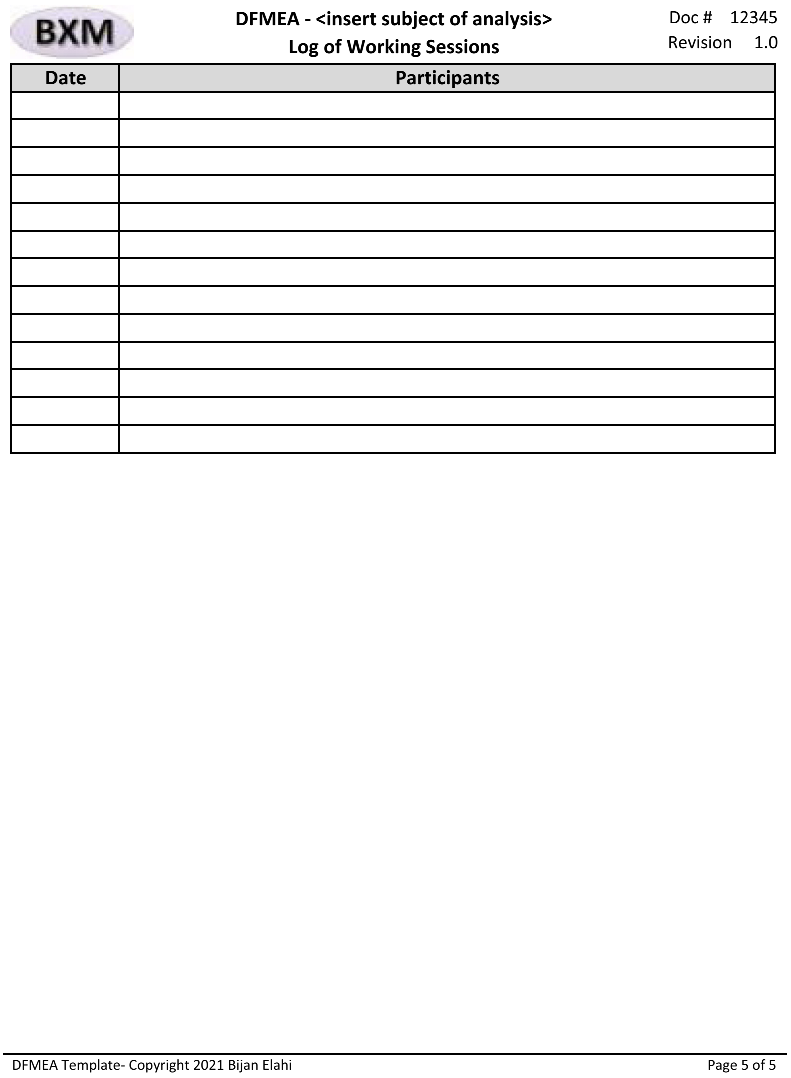
Doc # 12345
Revision 1.0

Revision History

Revision	Author	CR	Description of Change

DFMEA Template - Copyright 2021 Bijan Elahi

Page 4 of 5



BXM

DFMEA - <insert subject of analysis>
Log of Working Sessions

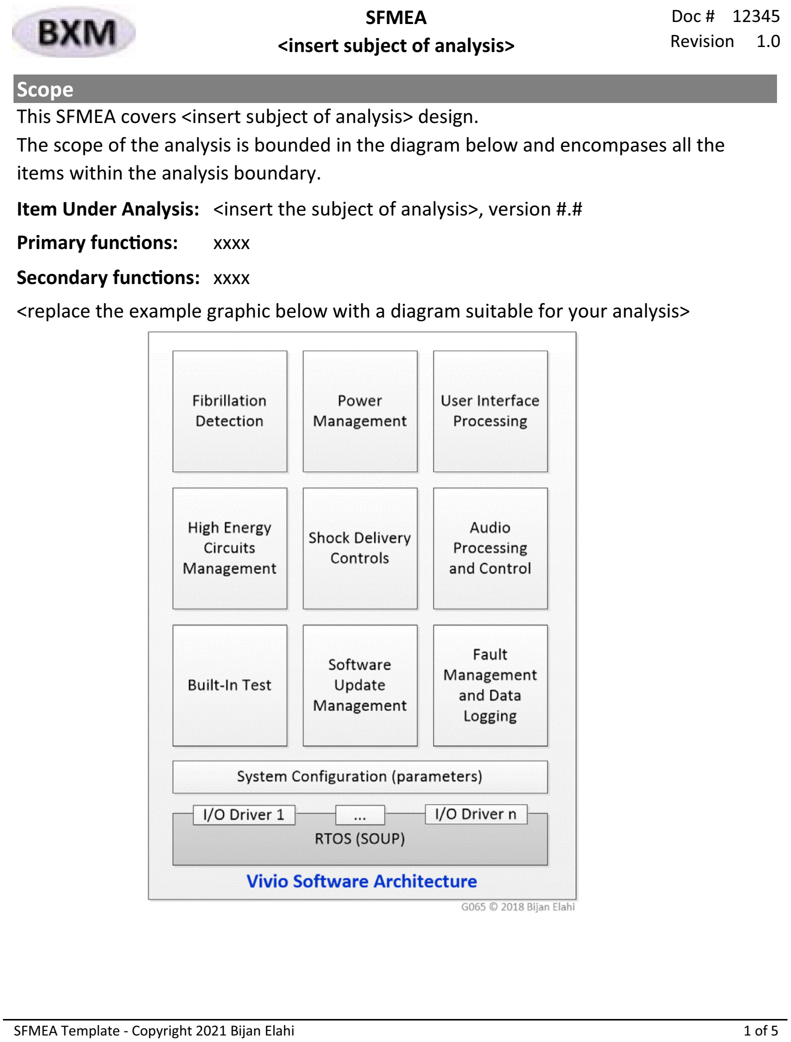
Doc # 12345
Revision 1.0

Date	Participants

DFMEA Template- Copyright 2021 Bijan Elahi

Page 5 of 5

B.2 SFMEA TEMPLATE



BXM

SFMEA
<insert subject of analysis>

Doc # 12345
Revision 1.0

Scope

This SFMEA covers <insert subject of analysis> design.
The scope of the analysis is bounded in the diagram below and encompases all the items within the analysis boundary.

Item Under Analysis: <insert the subject of analysis>, version #.#

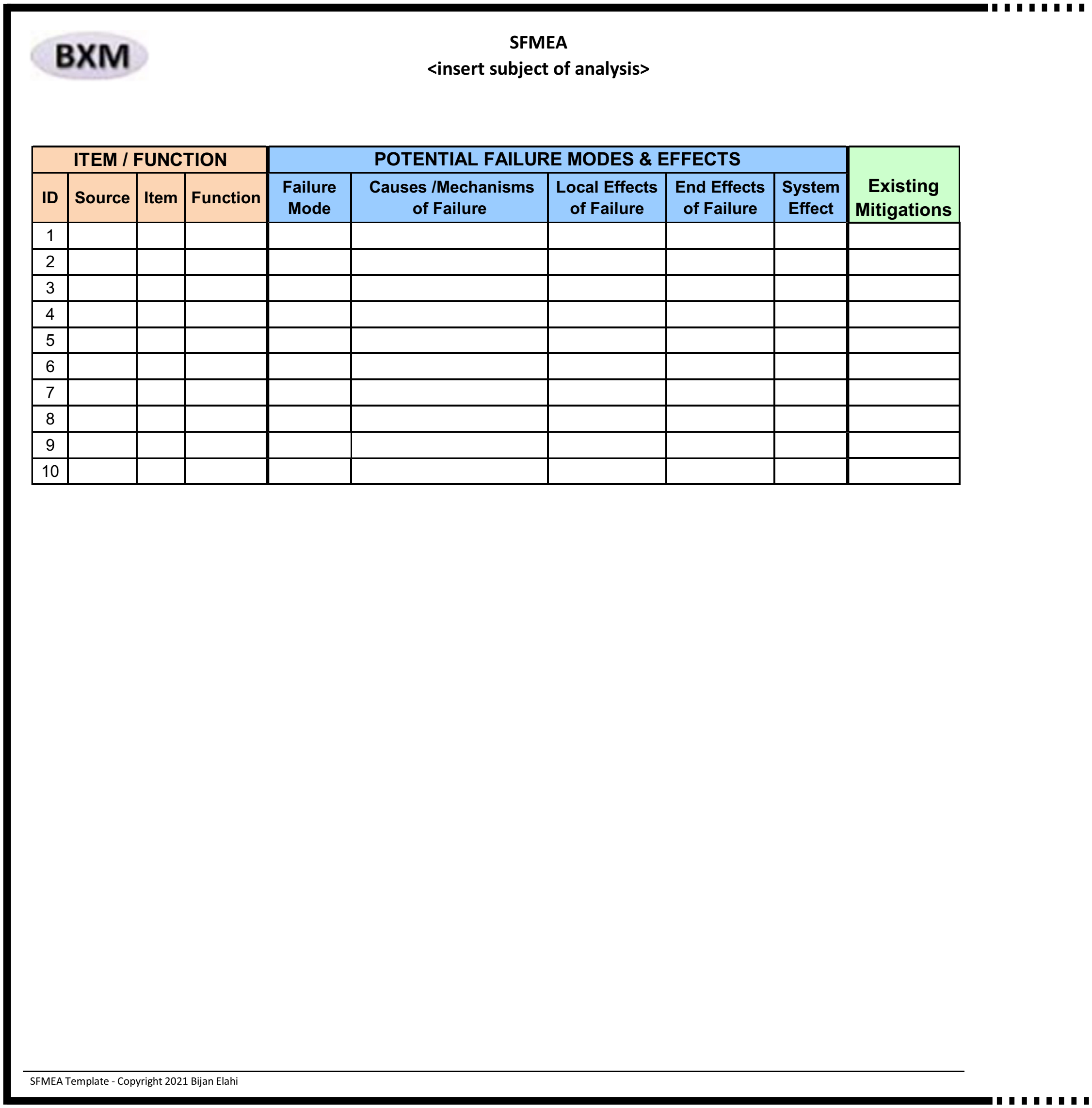
Primary functions: xxxx

Secondary functions: xxxx

<replace the example graphic below with a diagram suitable for your analysis>

Fibrillation Detection
Power Management
User Interface Processing
High Energy Circuits Management
Shock Delivery Controls
Audio Processing and Control
Built-In Test
Software Update Management
Fault Management and Data Logging
System Configuration (parameters)
I/O Driver 1
...
I/O Driver n
RTOS (SOUP)
Vivio Software Architecture
G065 © 2018 Bijan Elahi

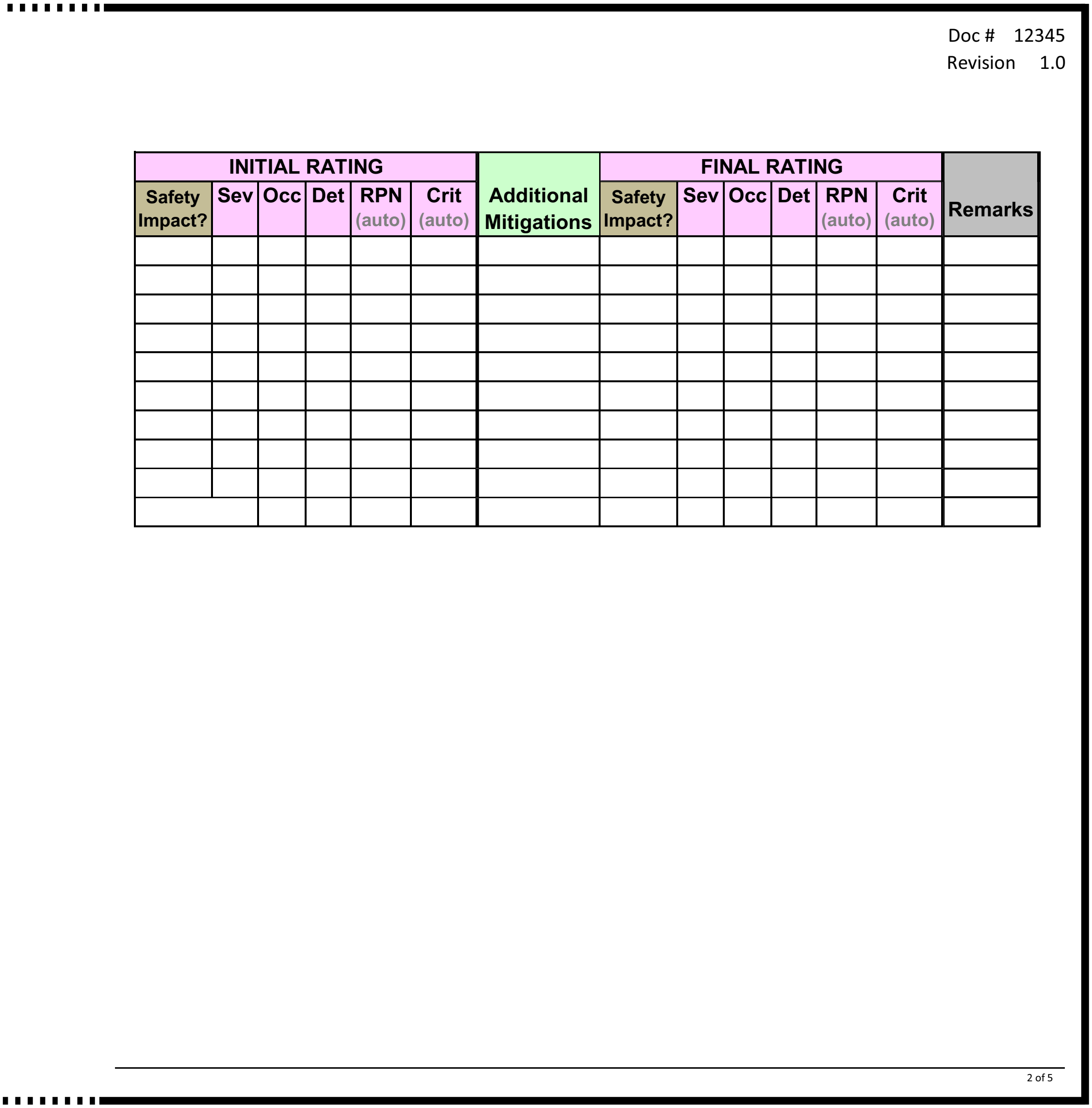
SFMEA Template - Copyright 2021 Bijan Elahi 1 of 5



BXM

SFMEA
<insert subject of analysis>

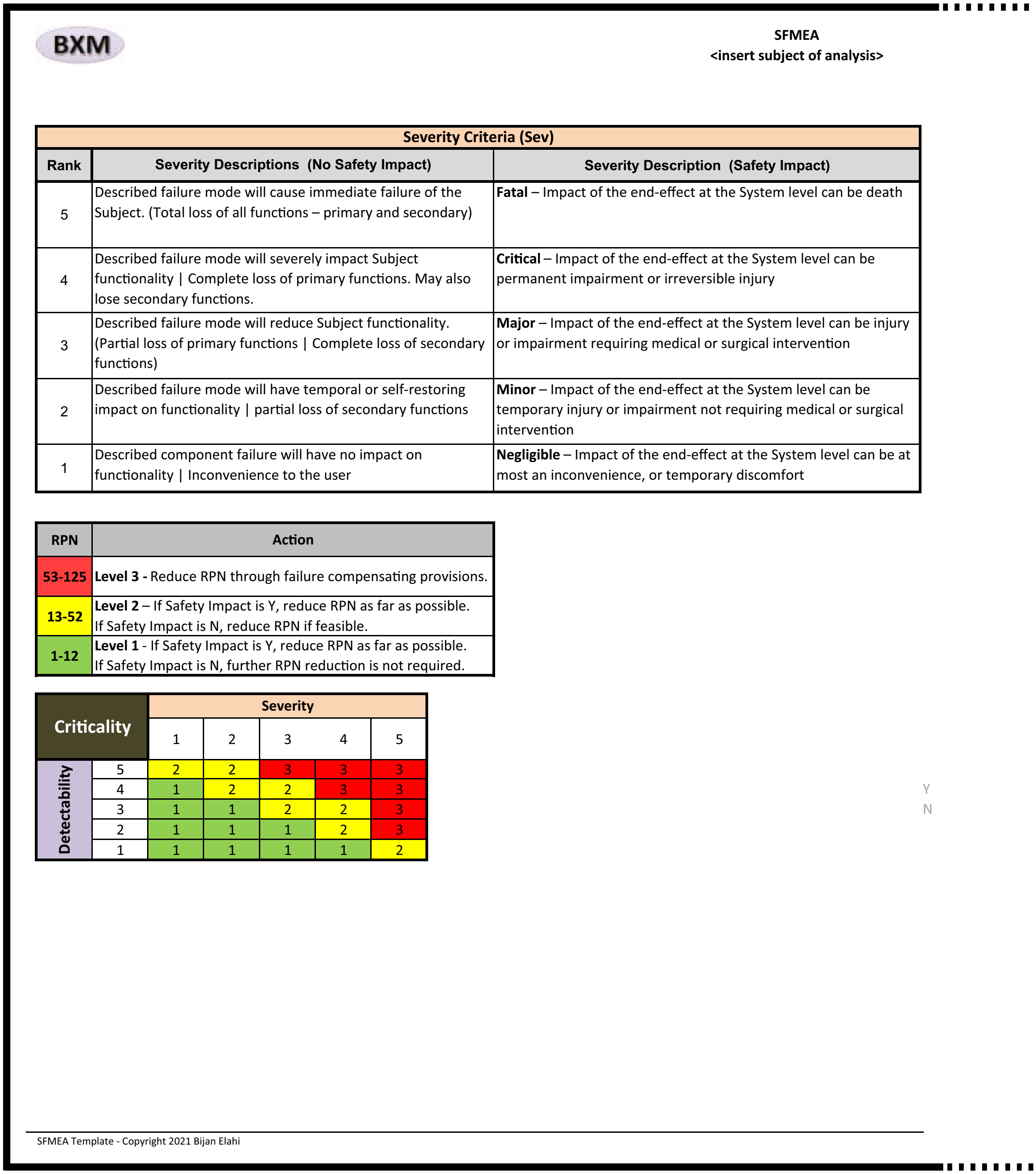
ITEM / FUNCTION				POTENTIAL FAILURE MODES & EFFECTS					Existing Mitigations
ID	Source	Item	Function	Failure Mode	Causes /Mechanisms of Failure	Local Effects of Failure	End Effects of Failure	System Effect	
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									



Doc # 12345
Revision 1.0

INITIAL RATING						Additional Mitigations	FINAL RATING						Remarks
Safety Impact?	Sev	Occ	Det	RPN (auto)	Crit (auto)		Safety Impact?	Sev	Occ	Det	RPN (auto)	Crit (auto)	

2 of 5



SFMEA
<insert subject of analysis>

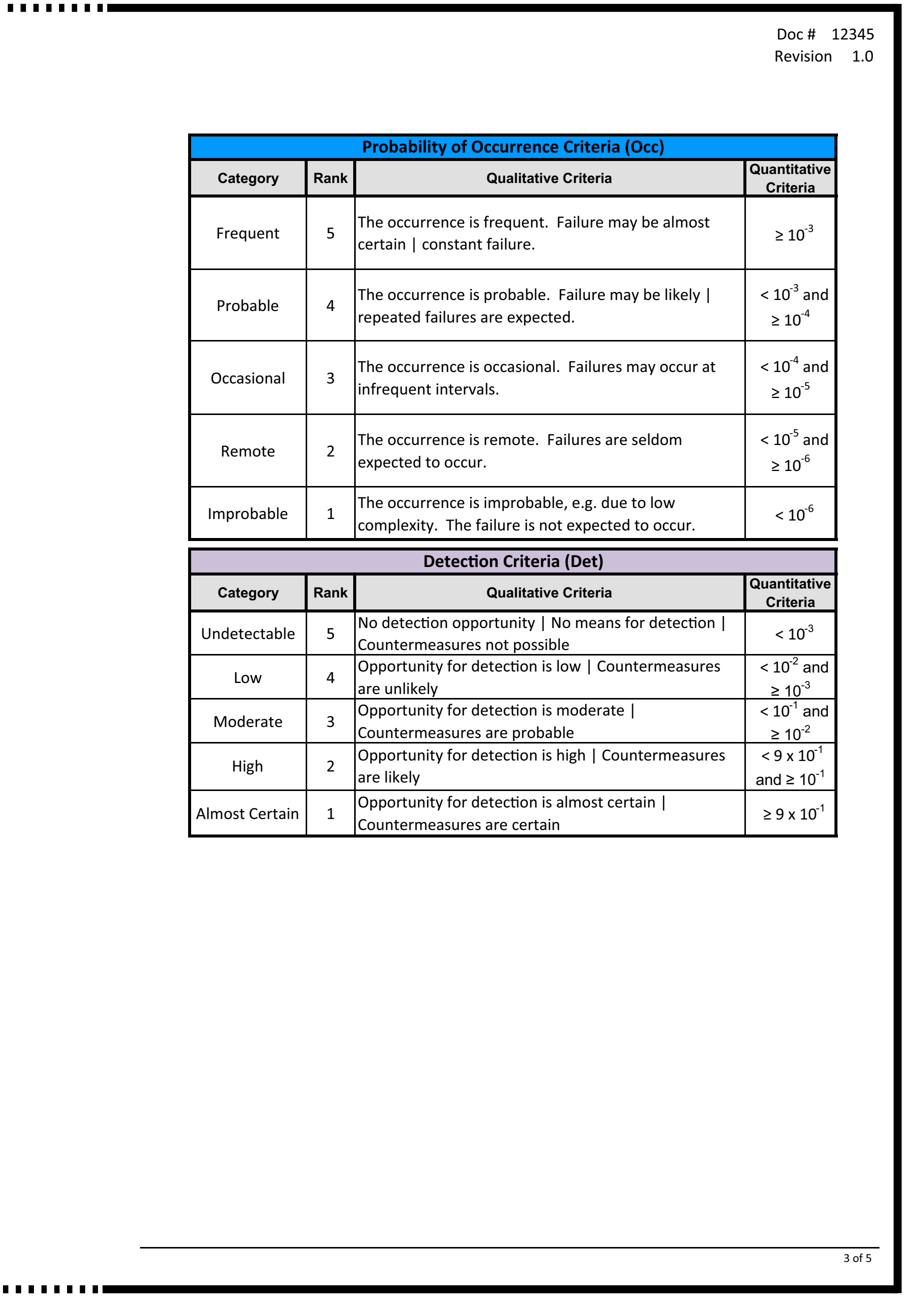
Severity Criteria (Sev)		
Rank	**Severity Descriptions (No Safety Impact)**	**Severity Description (Safety Impact)**
5	Described failure mode will cause immediate failure of the Subject. (Total loss of all functions – primary and secondary)	**Fatal** – Impact of the end-effect at the System level can be death
4	Described failure mode will severely impact Subject functionality | Complete loss of primary functions. May also lose secondary functions.	**Critical** – Impact of the end-effect at the System level can be permanent impairment or irreversible injury
3	Described failure mode will reduce Subject functionality. (Partial loss of primary functions | Complete loss of secondary functions)	**Major** – Impact of the end-effect at the System level can be injury or impairment requiring medical or surgical intervention
2	Described failure mode will have temporal or self-restoring impact on functionality | partial loss of secondary functions	**Minor** – Impact of the end-effect at the System level can be temporary injury or impairment not requiring medical or surgical intervention
1	Described component failure will have no impact on functionality | Inconvenience to the user	**Negligible** – Impact of the end-effect at the System level can be at most an inconvenience, or temporary discomfort

RPN	Action
53-125	**Level 3 -** Reduce RPN through failure compensating provisions.
13-52	**Level 2** – If Safety Impact is Y, reduce RPN as far as possible. If Safety Impact is N, reduce RPN if feasible.
1-12	**Level 1** - If Safety Impact is Y, reduce RPN as far as possible. If Safety Impact is N, further RPN reduction is not required.

Criticality		Severity				
		1	2	3	4	5
Detectability	5	2	2	3	3	3
	4	1	2	2	3	3
	3	1	1	2	2	3
	2	1	1	1	2	3
	1	1	1	1	1	2

Y
N

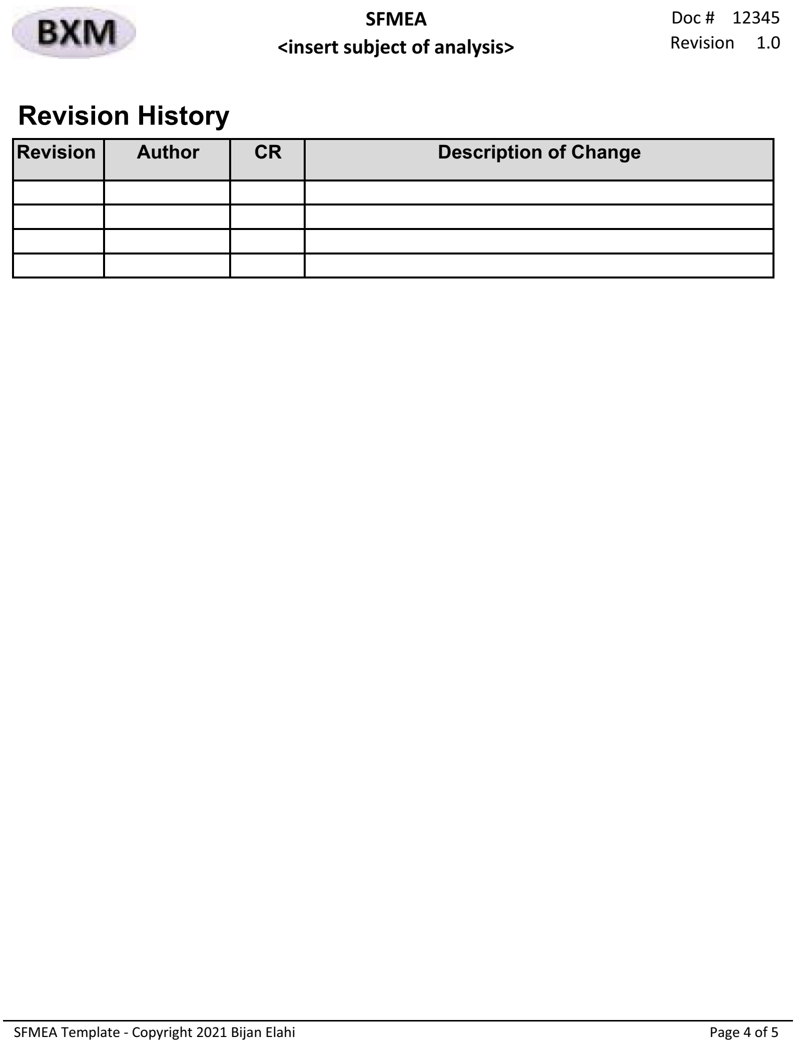
SFMEA Template - Copyright 2021 Bijan Elahi



Doc # 12345
Revision 1.0

Probability of Occurrence Criteria (Occ)			
Category	**Rank**	**Qualitative Criteria**	**Quantitative Criteria**
Frequent	5	The occurrence is frequent. Failure may be almost certain | constant failure.	$\geq 10^{-3}$
Probable	4	The occurrence is probable. Failure may be likely | repeated failures are expected.	$< 10^{-3}$ and $\geq 10^{-4}$
Occasional	3	The occurrence is occasional. Failures may occur at infrequent intervals.	$< 10^{-4}$ and $\geq 10^{-5}$
Remote	2	The occurrence is remote. Failures are seldom expected to occur.	$< 10^{-5}$ and $\geq 10^{-6}$
Improbable	1	The occurrence is improbable, e.g. due to low complexity. The failure is not expected to occur.	$< 10^{-6}$

Detection Criteria (Det)			
Category	**Rank**	**Qualitative Criteria**	**Quantitative Criteria**
Undetectable	5	No detection opportunity | No means for detection | Countermeasures not possible	$< 10^{-3}$
Low	4	Opportunity for detection is low | Countermeasures are unlikely	$< 10^{-2}$ and $\geq 10^{-3}$
Moderate	3	Opportunity for detection is moderate | Countermeasures are probable	$< 10^{-1}$ and $\geq 10^{-2}$
High	2	Opportunity for detection is high | Countermeasures are likely	$< 9 \times 10^{-1}$ and $\geq 10^{-1}$
Almost Certain	1	Opportunity for detection is almost certain | Countermeasures are certain	$\geq 9 \times 10^{-1}$



BXM

SFMEA
<insert subject of analysis>

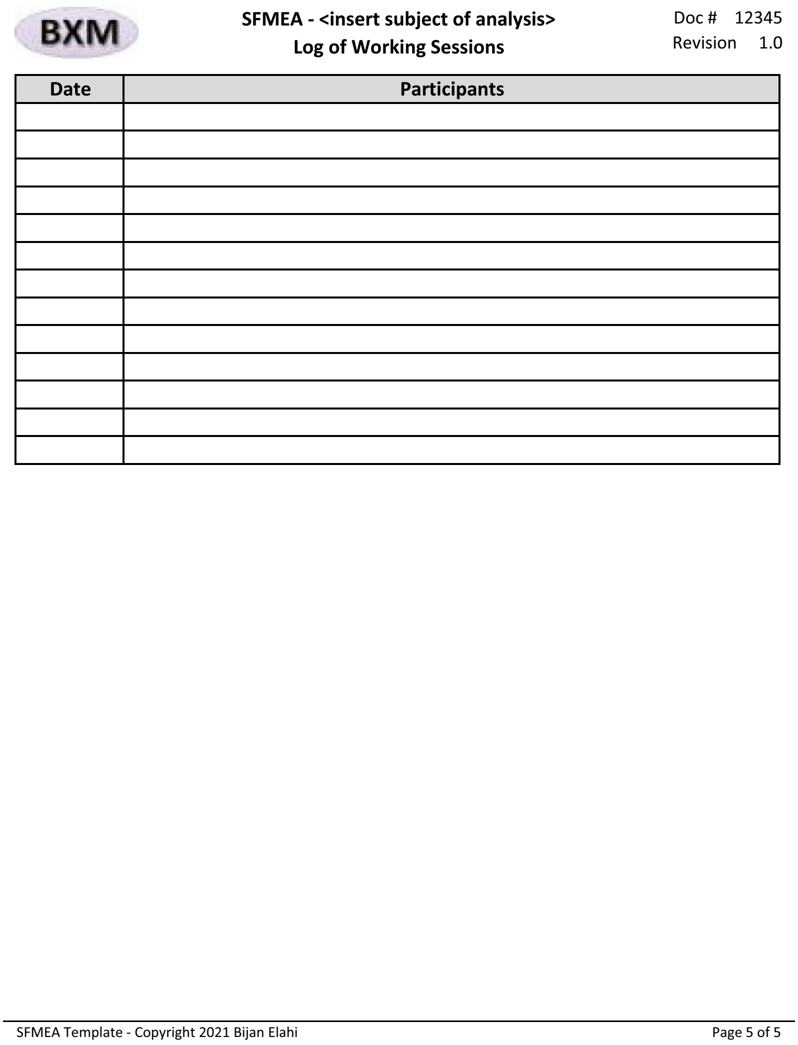
Doc # 12345
Revision 1.0

Revision History

Revision	Author	CR	Description of Change

SFMEA Template - Copyright 2021 Bijan Elahi

Page 4 of 5



BXM

SFMEA - <insert subject of analysis>
Log of Working Sessions

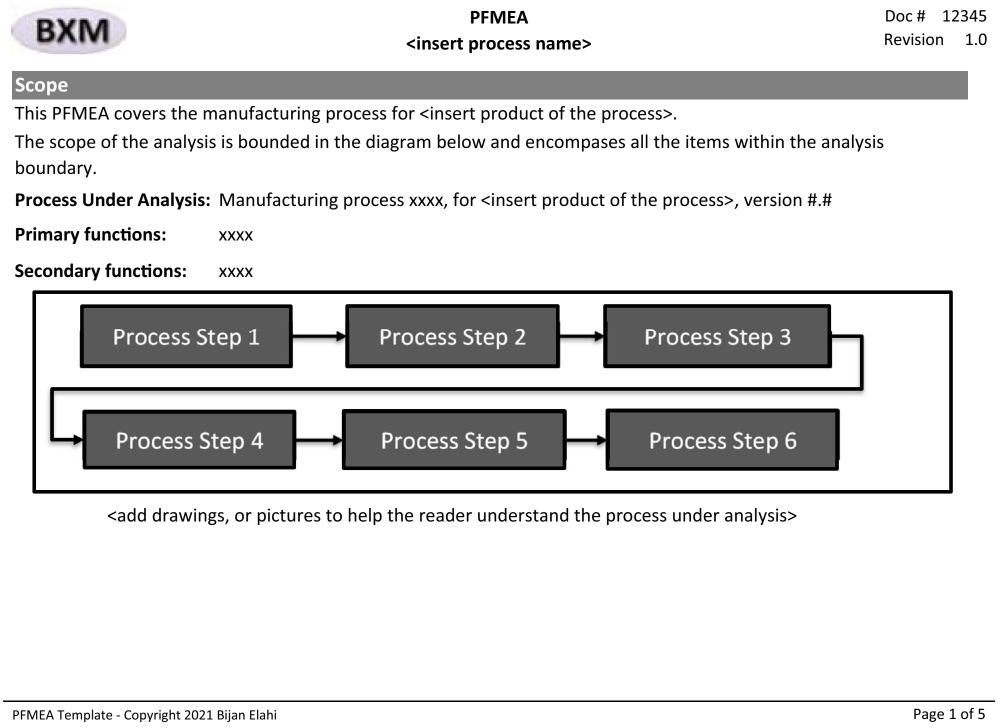
Doc # 12345
Revision 1.0

Date	Participants

SFMEA Template - Copyright 2021 Bijan Elahi

Page 5 of 5

B.3 PFMEA TEMPLATE



PFMEA
<insert process name>

Doc # 12345
Revision 1.0

Scope

This PFMEA covers the manufacturing process for <insert product of the process>.

The scope of the analysis is bounded in the diagram below and encompases all the items within the analysis boundary.

Process Under Analysis: Manufacturing process xxxx, for <insert product of the process>, version #.#

Primary functions: xxxx

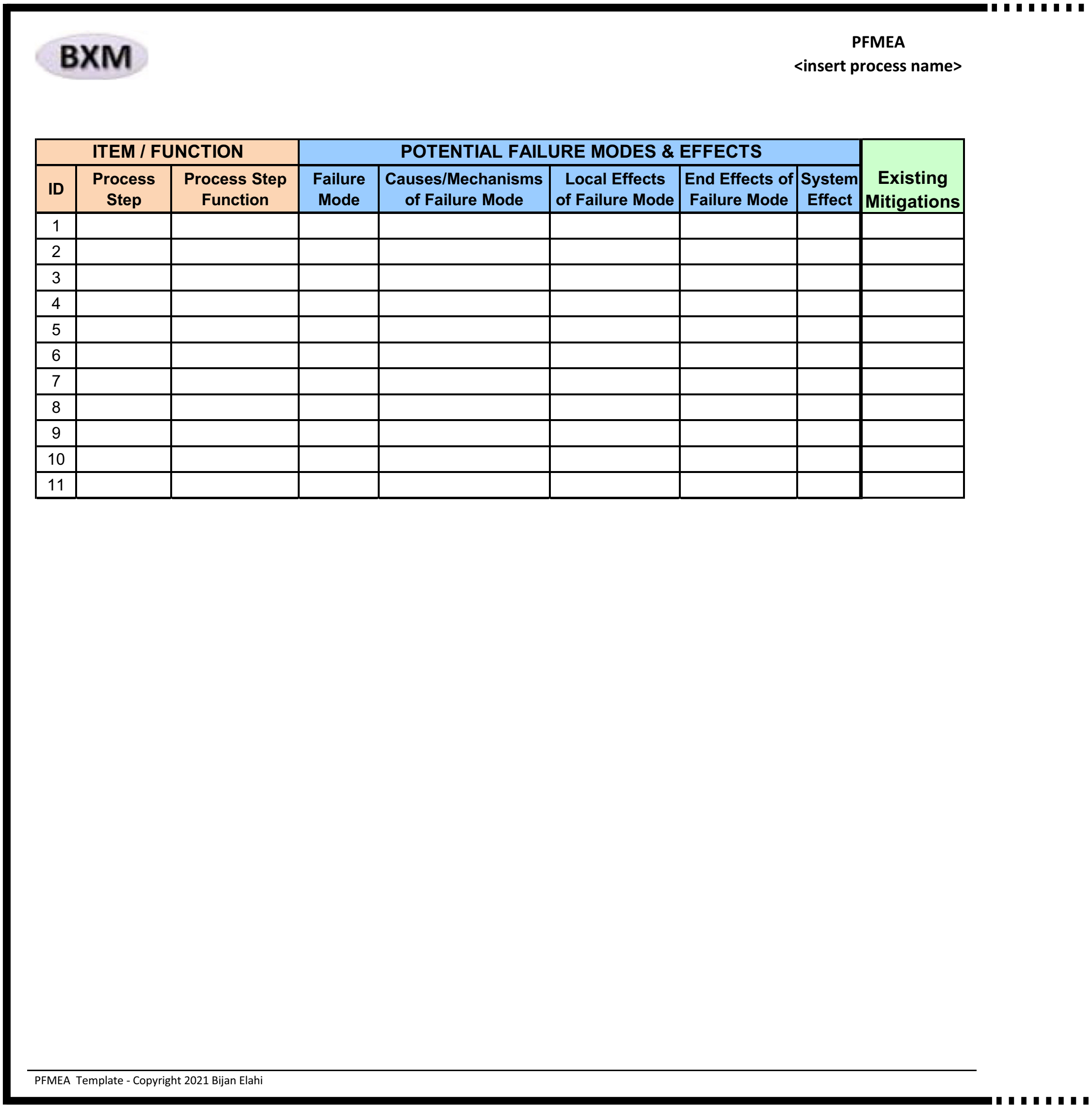
Secondary functions: xxxx

Process Step 1 → Process Step 2 → Process Step 3 → Process Step 4 → Process Step 5 → Process Step 6

<add drawings, or pictures to help the reader understand the process under analysis>

PFMEA Template - Copyright 2021 Bijan Elahi

Page 1 of 5

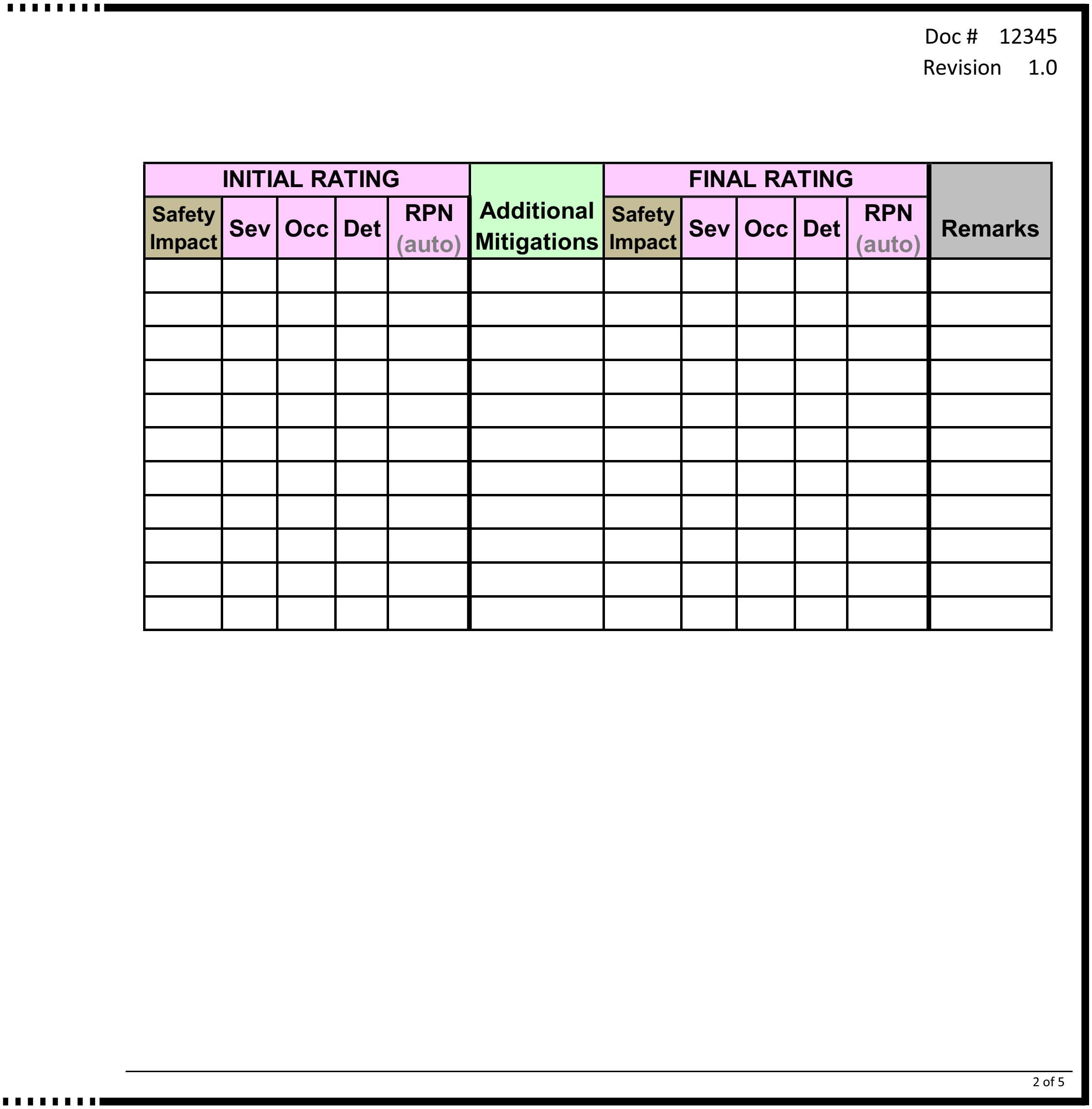


BXM

PFMEA
<insert process name>

ITEM / FUNCTION			POTENTIAL FAILURE MODES & EFFECTS					Existing Mitigations
ID	Process Step	Process Step Function	Failure Mode	Causes/Mechanisms of Failure Mode	Local Effects of Failure Mode	End Effects of Failure Mode	System Effect	
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								

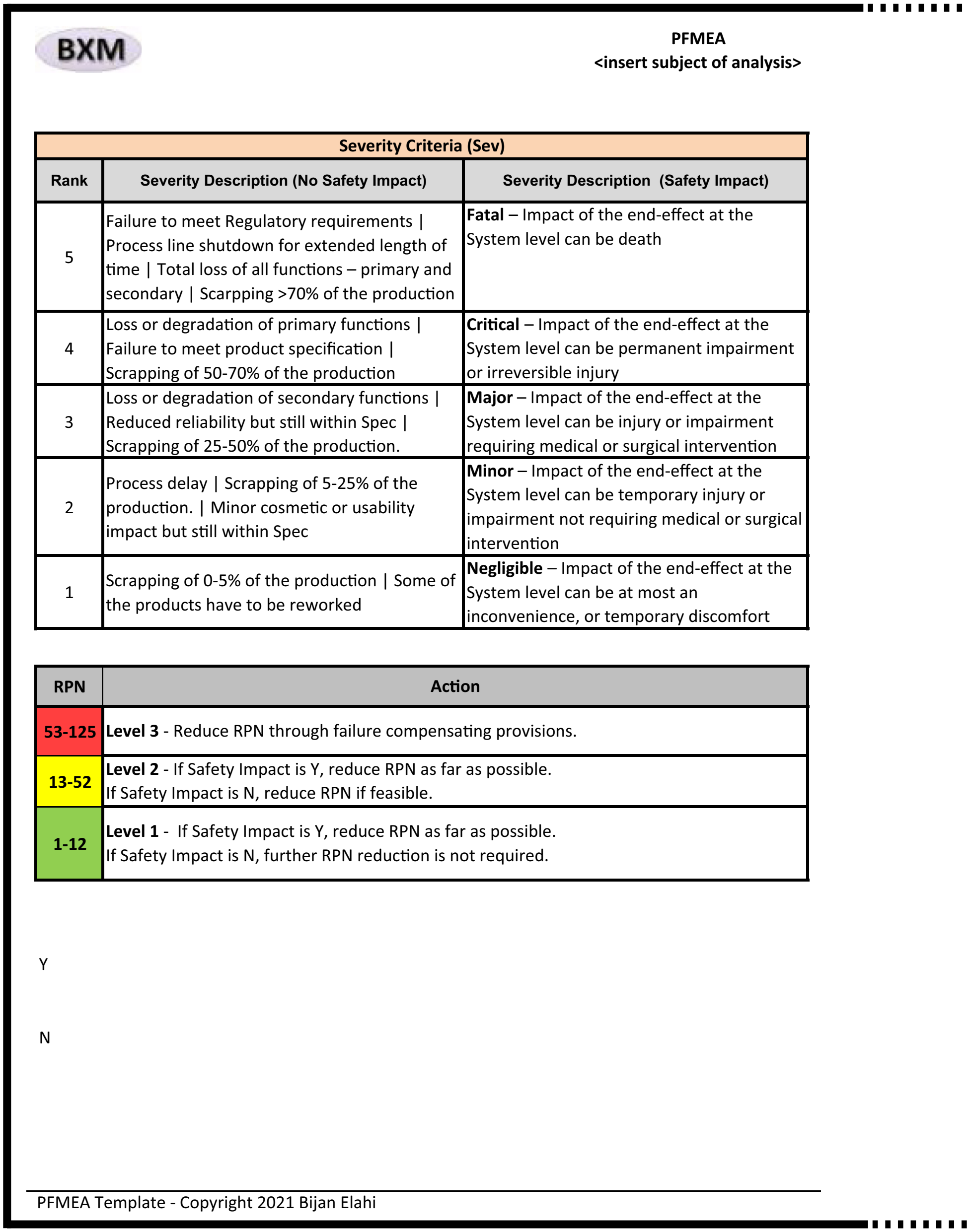
PFMEA Template - Copyright 2021 Bijan Elahi



Doc # 12345
Revision 1.0

INITIAL RATING					Additional Mitigations	FINAL RATING					Remarks
Safety Impact	Sev	Occ	Det	RPN (auto)		Safety Impact	Sev	Occ	Det	RPN (auto)	

2 of 5



BXM

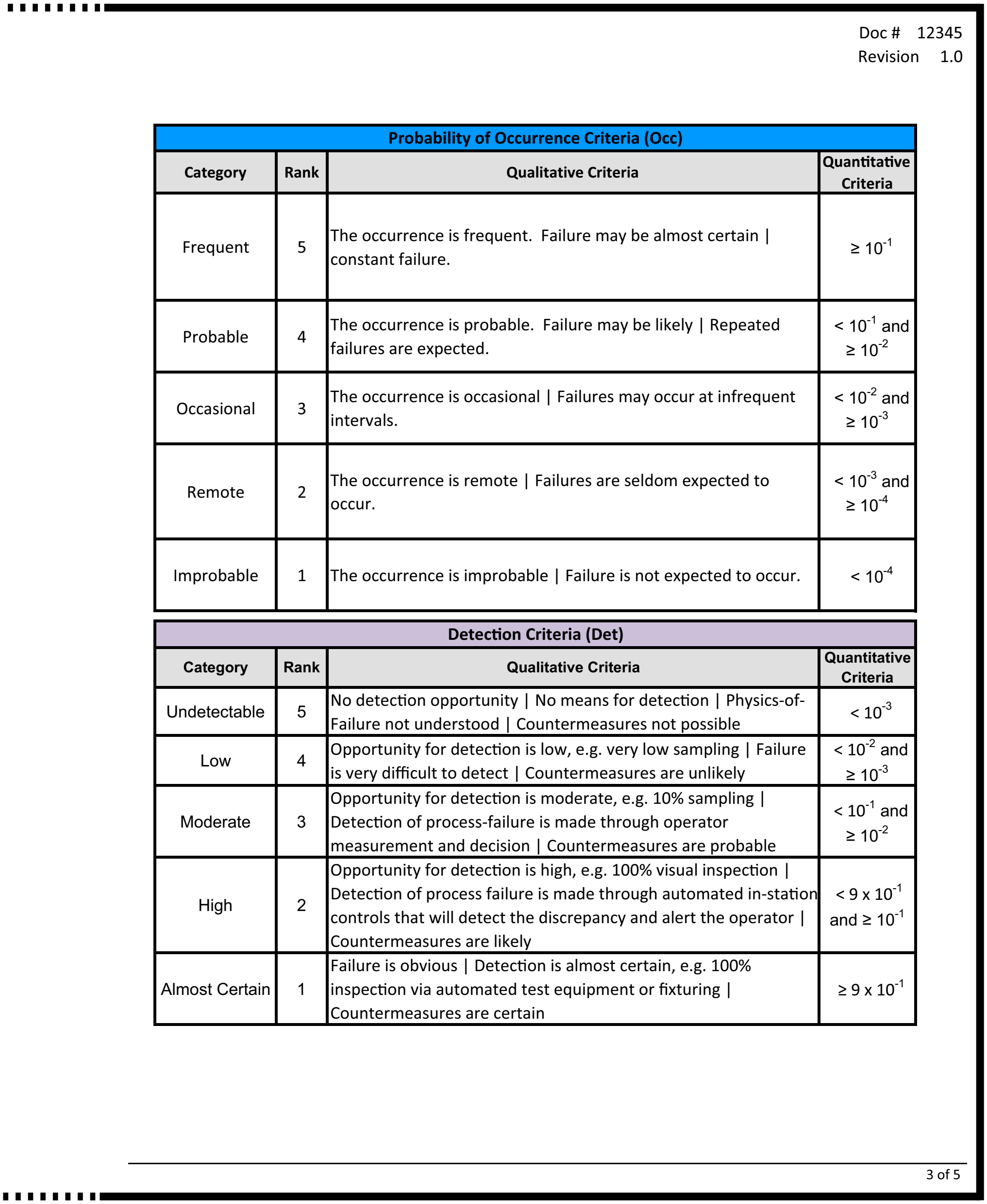
PFMEA
<insert subject of analysis>

Severity Criteria (Sev)		
Rank	**Severity Description (No Safety Impact)**	**Severity Description (Safety Impact)**
5	Failure to meet Regulatory requirements | Process line shutdown for extended length of time | Total loss of all functions – primary and secondary | Scarpping >70% of the production	**Fatal** – Impact of the end-effect at the System level can be death
4	Loss or degradation of primary functions | Failure to meet product specification | Scrapping of 50-70% of the production	**Critical** – Impact of the end-effect at the System level can be permanent impairment or irreversible injury
3	Loss or degradation of secondary functions | Reduced reliability but still within Spec | Scrapping of 25-50% of the production.	**Major** – Impact of the end-effect at the System level can be injury or impairment requiring medical or surgical intervention
2	Process delay | Scrapping of 5-25% of the production. | Minor cosmetic or usability impact but still within Spec	**Minor** – Impact of the end-effect at the System level can be temporary injury or impairment not requiring medical or surgical intervention
1	Scrapping of 0-5% of the production | Some of the products have to be reworked	**Negligible** – Impact of the end-effect at the System level can be at most an inconvenience, or temporary discomfort

RPN	Action
53-125	**Level 3** - Reduce RPN through failure compensating provisions.
13-52	**Level 2** - If Safety Impact is Y, reduce RPN as far as possible. If Safety Impact is N, reduce RPN if feasible.
1-12	**Level 1** - If Safety Impact is Y, reduce RPN as far as possible. If Safety Impact is N, further RPN reduction is not required.

Y

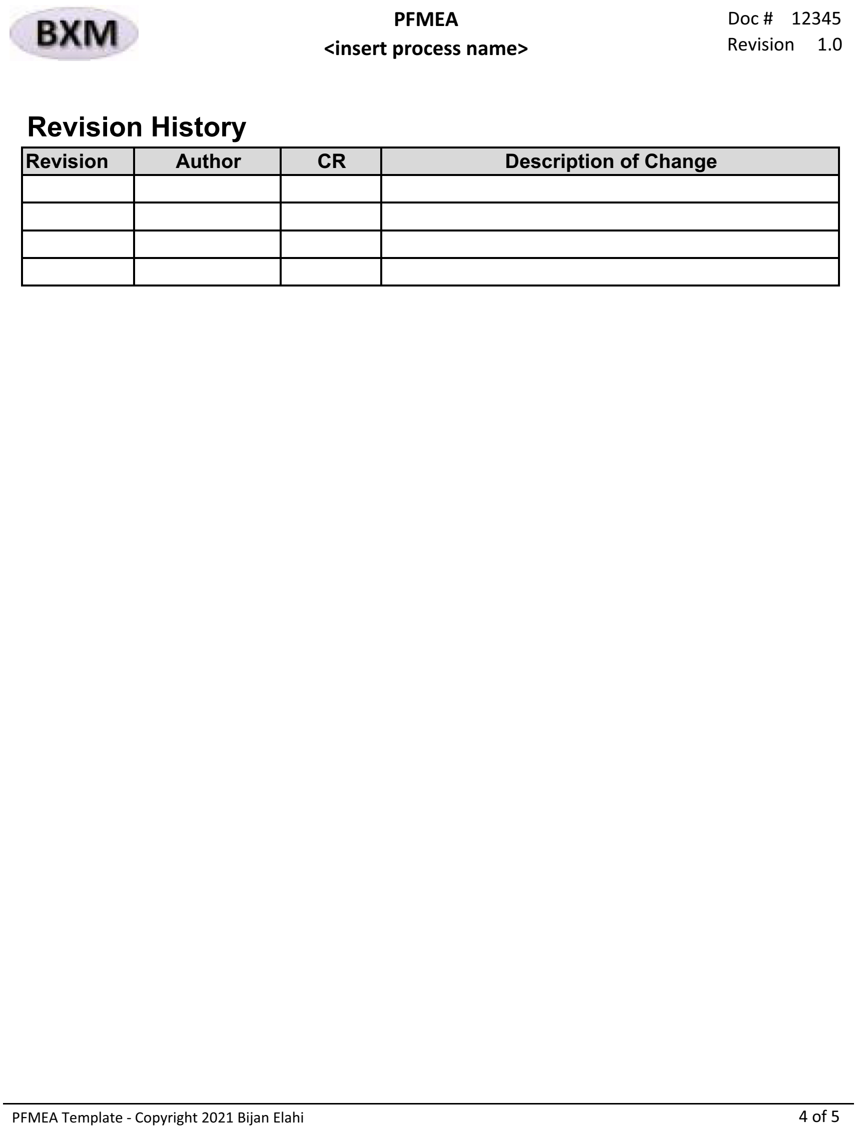
N



Doc # 12345
Revision 1.0

Probability of Occurrence Criteria (Occ)			
Category	**Rank**	**Qualitative Criteria**	**Quantitative Criteria**
Frequent	5	The occurrence is frequent. Failure may be almost certain | constant failure.	$\geq 10^{-1}$
Probable	4	The occurrence is probable. Failure may be likely | Repeated failures are expected.	$< 10^{-1}$ and $\geq 10^{-2}$
Occasional	3	The occurrence is occasional | Failures may occur at infrequent intervals.	$< 10^{-2}$ and $\geq 10^{-3}$
Remote	2	The occurrence is remote | Failures are seldom expected to occur.	$< 10^{-3}$ and $\geq 10^{-4}$
Improbable	1	The occurrence is improbable | Failure is not expected to occur.	$< 10^{-4}$

Detection Criteria (Det)			
Category	**Rank**	**Qualitative Criteria**	**Quantitative Criteria**
Undetectable	5	No detection opportunity | No means for detection | Physics-of-Failure not understood | Countermeasures not possible	$< 10^{-3}$
Low	4	Opportunity for detection is low, e.g. very low sampling | Failure is very difficult to detect | Countermeasures are unlikely	$< 10^{-2}$ and $\geq 10^{-3}$
Moderate	3	Opportunity for detection is moderate, e.g. 10% sampling | Detection of process-failure is made through operator measurement and decision | Countermeasures are probable	$< 10^{-1}$ and $\geq 10^{-2}$
High	2	Opportunity for detection is high, e.g. 100% visual inspection | Detection of process failure is made through automated in-station controls that will detect the discrepancy and alert the operator | Countermeasures are likely	$< 9 \times 10^{-1}$ and $\geq 10^{-1}$
Almost Certain	1	Failure is obvious | Detection is almost certain, e.g. 100% inspection via automated test equipment or fixturing | Countermeasures are certain	$\geq 9 \times 10^{-1}$



BXM

PFMEA
<insert process name>

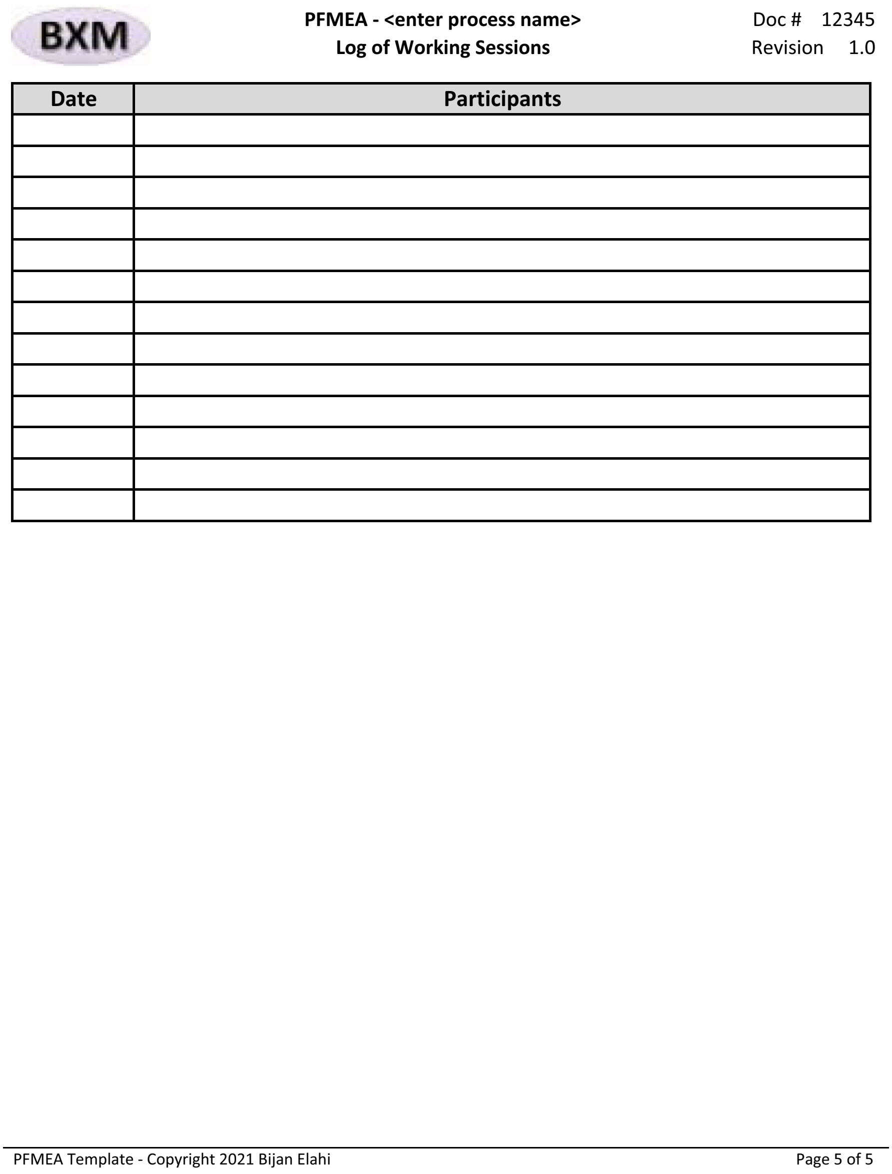
Doc # 12345
Revision 1.0

Revision History

Revision	Author	CR	Description of Change

PFMEA Template - Copyright 2021 Bijan Elahi

4 of 5



BXM

PFMEA - <enter process name>
Log of Working Sessions

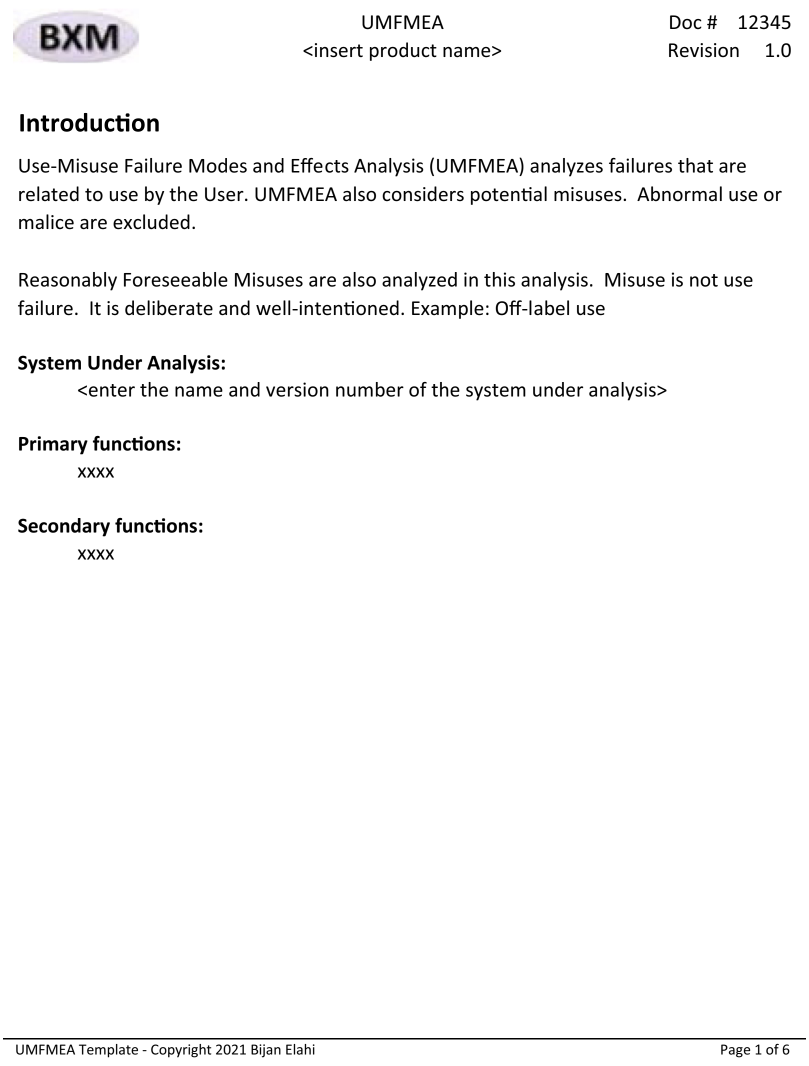
Doc # 12345
Revision 1.0

Date	Participants

PFMEA Template - Copyright 2021 Bijan Elahi

Page 5 of 5

B.4 UMFMEA TEMPLATE



BXM	UMFMEA <insert product name>	Doc # 12345 Revision 1.0

Introduction

Use-Misuse Failure Modes and Effects Analysis (UMFMEA) analyzes failures that are related to use by the User. UMFMEA also considers potential misuses. Abnormal use or malice are excluded.

Reasonably Foreseeable Misuses are also analyzed in this analysis. Misuse is not use failure. It is deliberate and well-intentioned. Example: Off-label use

System Under Analysis:

<enter the name and version number of the system under analysis>

Primary functions:

xxxx

Secondary functions:

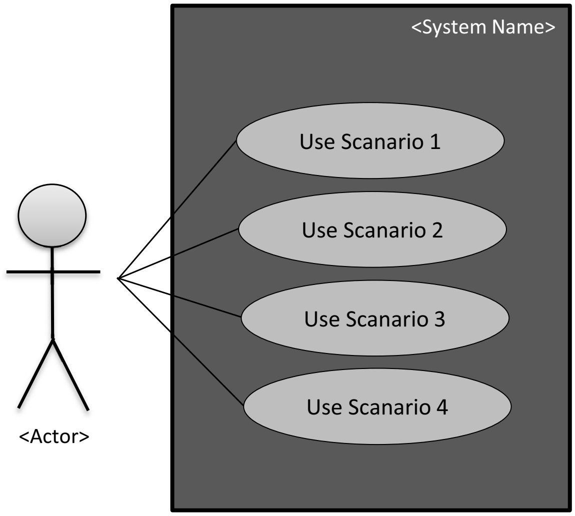
xxxx

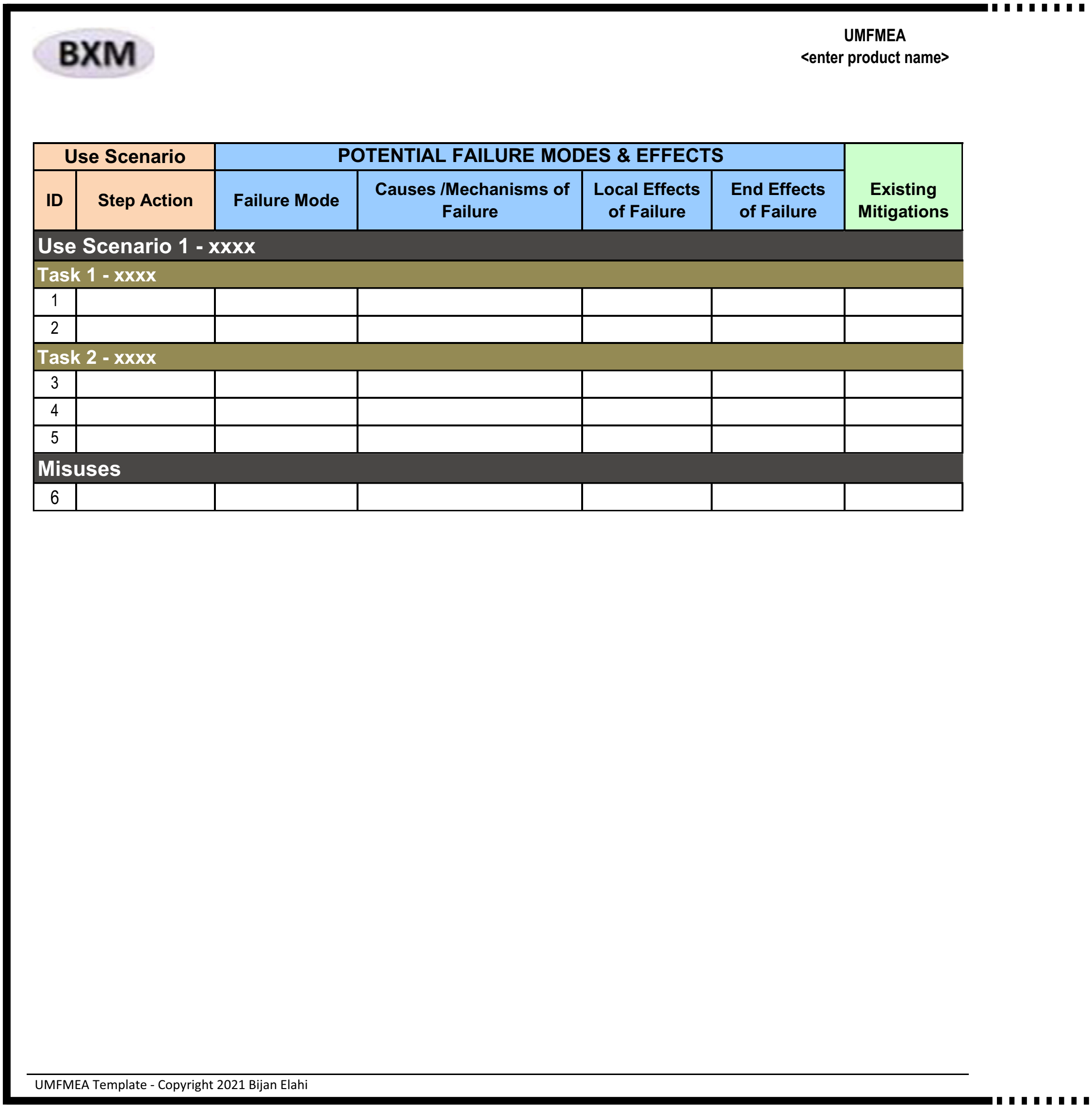
UMFMEA Template - Copyright 2021 Bijan Elahi   Page 1 of 6

BXM	UMFMEA <insert product name>	Doc # 12345 Revision 1.0

Scope

<Describe the scope of analysis: the system, context of operation, and all the actors>

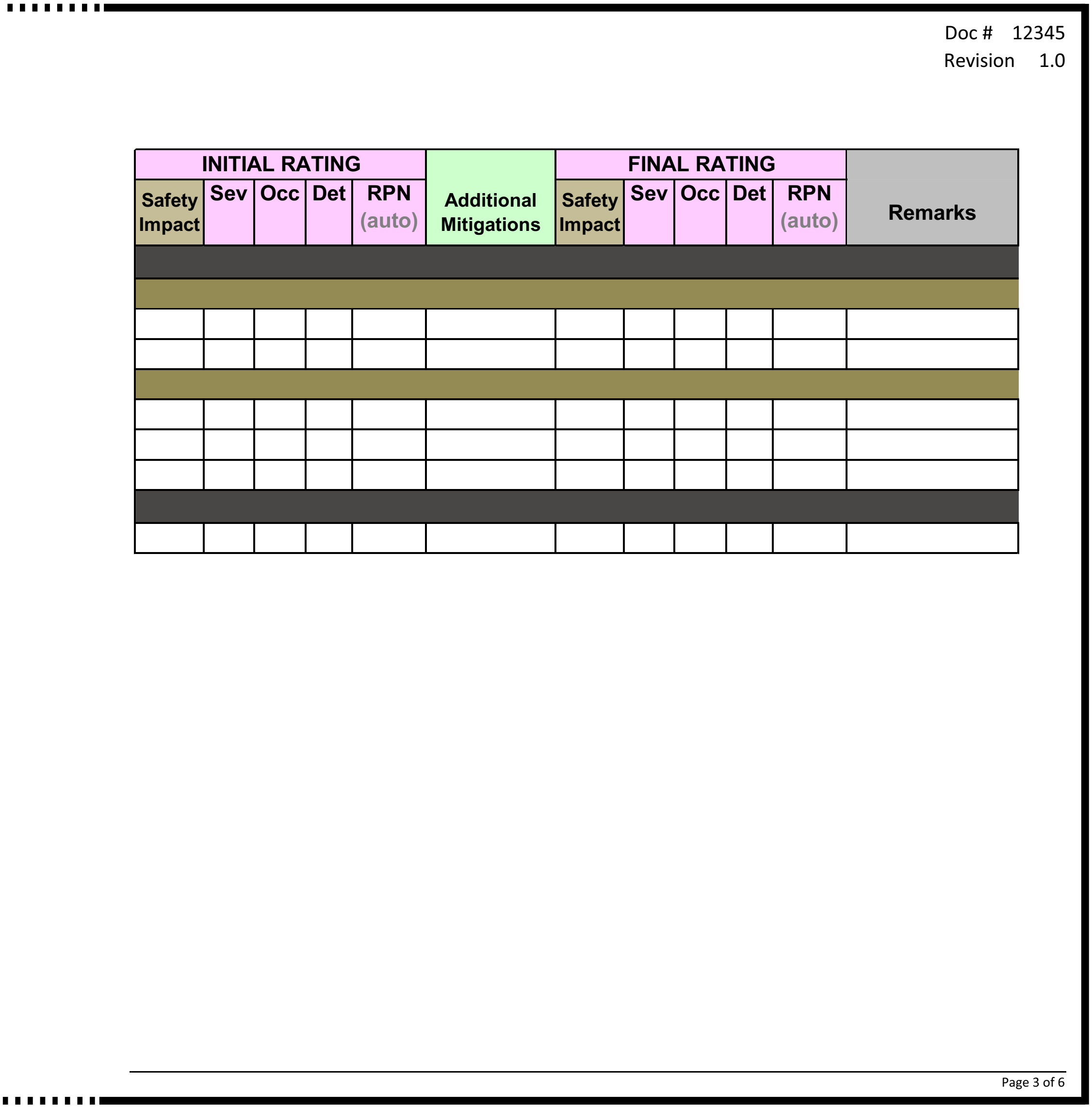




BXM

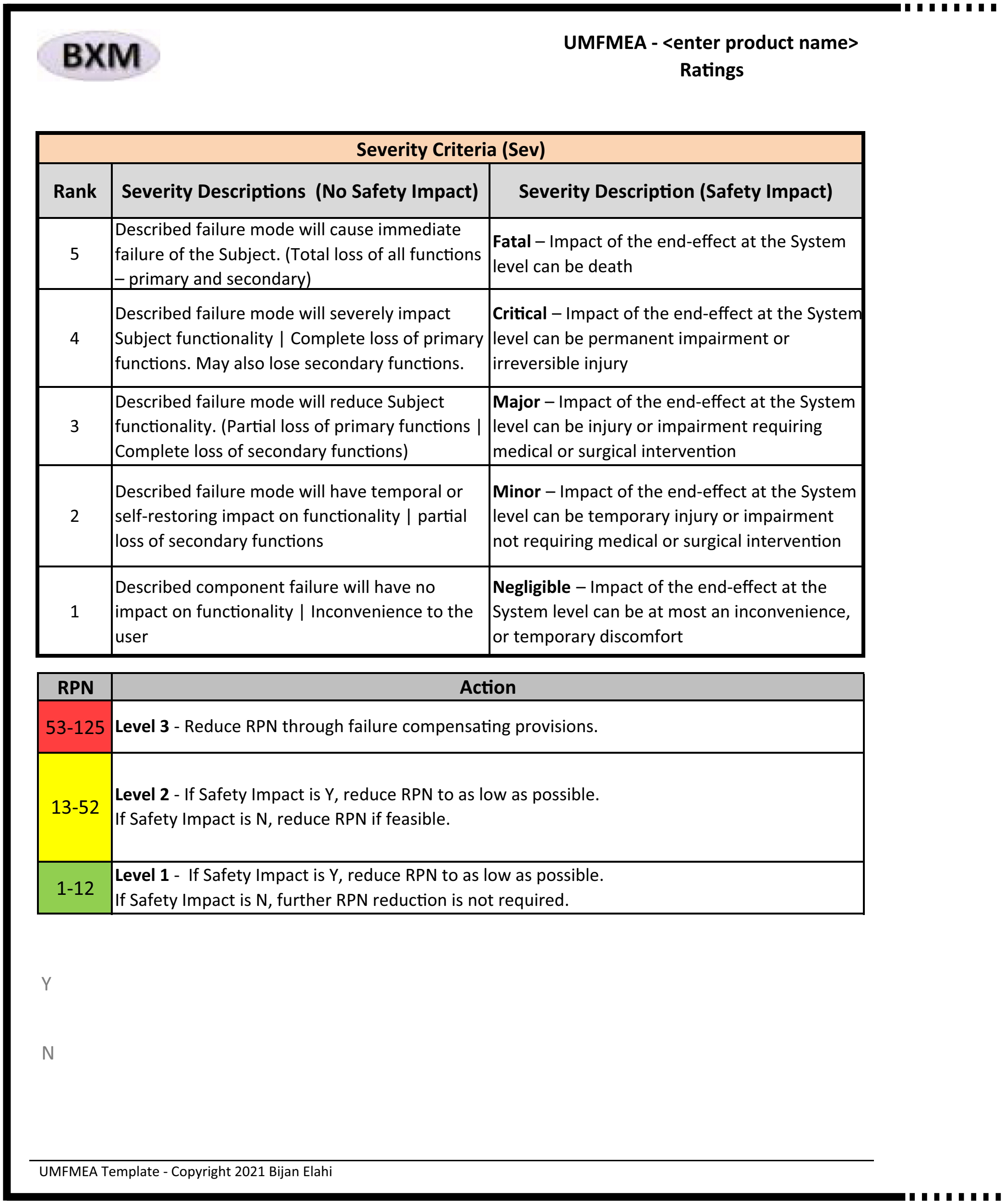
UMFMEA
<enter product name>

Use Scenario		POTENTIAL FAILURE MODES & EFFECTS				Existing Mitigations
ID	Step Action	Failure Mode	Causes /Mechanisms of Failure	Local Effects of Failure	End Effects of Failure	
Use Scenario 1 - xxxx						
Task 1 - xxxx						
1						
2						
Task 2 - xxxx						
3						
4						
5						
Misuses						
6						



Doc # 12345
Revision 1.0

INITIAL RATING					Additional Mitigations	FINAL RATING					Remarks
Safety Impact	Sev	Occ	Det	RPN (auto)		Safety Impact	Sev	Occ	Det	RPN (auto)	



BXM

UMFMEA - <enter product name>
Ratings

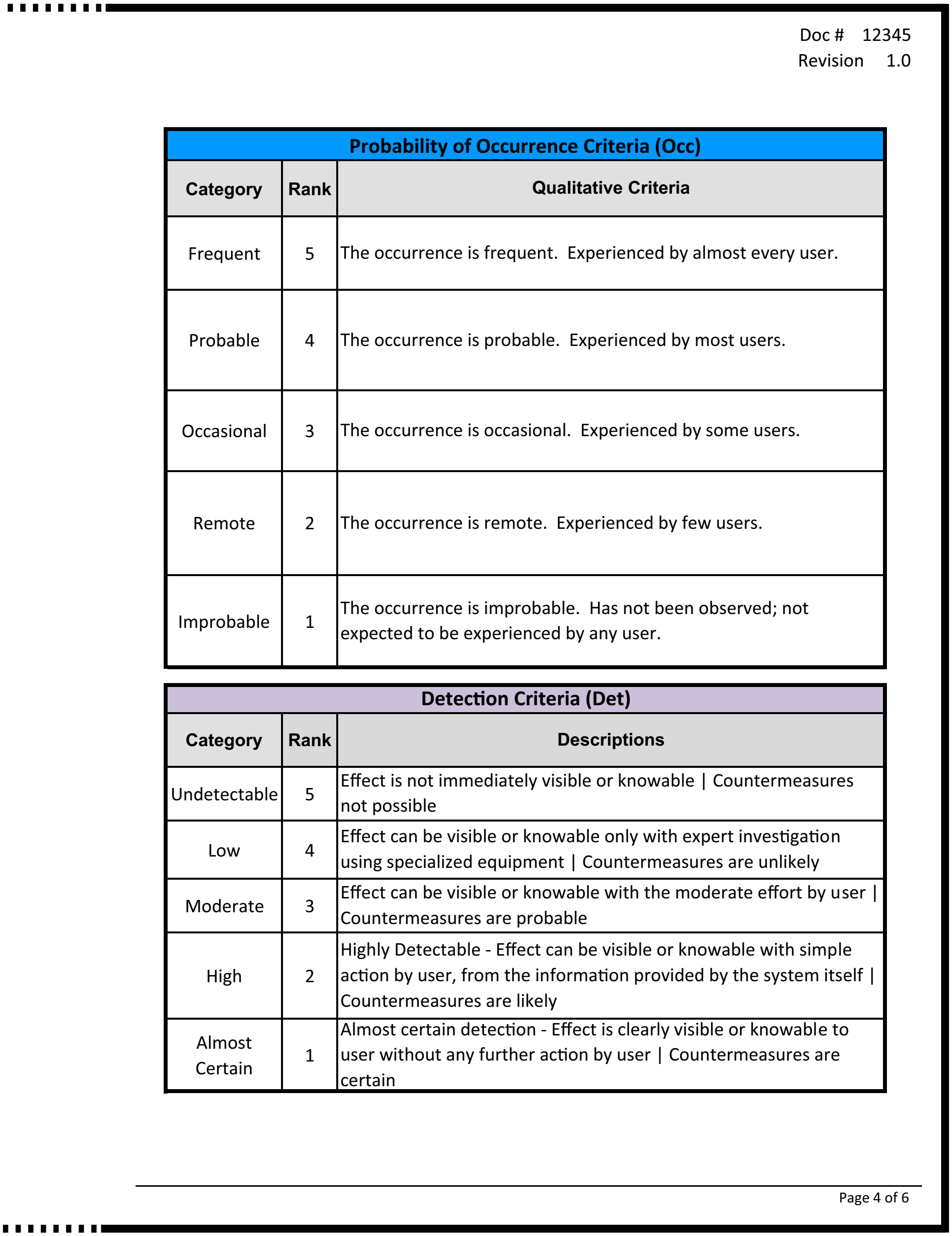
Severity Criteria (Sev)

Rank	Severity Descriptions (No Safety Impact)	Severity Description (Safety Impact)
5	Described failure mode will cause immediate failure of the Subject. (Total loss of all functions – primary and secondary)	**Fatal** – Impact of the end-effect at the System level can be death
4	Described failure mode will severely impact Subject functionality | Complete loss of primary functions. May also lose secondary functions.	**Critical** – Impact of the end-effect at the System level can be permanent impairment or irreversible injury
3	Described failure mode will reduce Subject functionality. (Partial loss of primary functions | Complete loss of secondary functions)	**Major** – Impact of the end-effect at the System level can be injury or impairment requiring medical or surgical intervention
2	Described failure mode will have temporal or self-restoring impact on functionality | partial loss of secondary functions	**Minor** – Impact of the end-effect at the System level can be temporary injury or impairment not requiring medical or surgical intervention
1	Described component failure will have no impact on functionality | Inconvenience to the user	**Negligible** – Impact of the end-effect at the System level can be at most an inconvenience, or temporary discomfort

RPN	Action
53-125	**Level 3** - Reduce RPN through failure compensating provisions.
13-52	**Level 2** - If Safety Impact is Y, reduce RPN to as low as possible. If Safety Impact is N, reduce RPN if feasible.
1-12	**Level 1** - If Safety Impact is Y, reduce RPN to as low as possible. If Safety Impact is N, further RPN reduction is not required.

Y

N

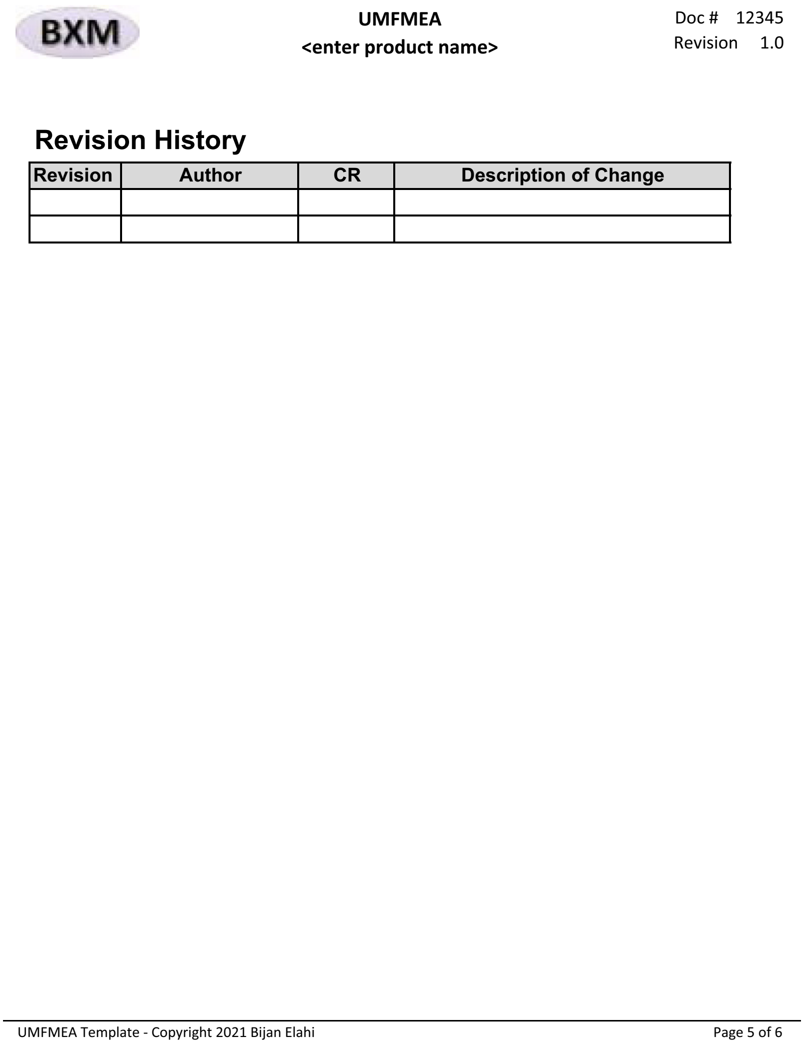


Probability of Occurrence Criteria (Occ)

Category	Rank	Qualitative Criteria
Frequent	5	The occurrence is frequent. Experienced by almost every user.
Probable	4	The occurrence is probable. Experienced by most users.
Occasional	3	The occurrence is occasional. Experienced by some users.
Remote	2	The occurrence is remote. Experienced by few users.
Improbable	1	The occurrence is improbable. Has not been observed; not expected to be experienced by any user.

Detection Criteria (Det)

Category	Rank	Descriptions
Undetectable	5	Effect is not immediately visible or knowable | Countermeasures not possible
Low	4	Effect can be visible or knowable only with expert investigation using specialized equipment | Countermeasures are unlikely
Moderate	3	Effect can be visible or knowable with the moderate effort by user | Countermeasures are probable
High	2	Highly Detectable - Effect can be visible or knowable with simple action by user, from the information provided by the system itself | Countermeasures are likely
Almost Certain	1	Almost certain detection - Effect is clearly visible or knowable to user without any further action by user | Countermeasures are certain



BXM

UMFMEA
<enter product name>

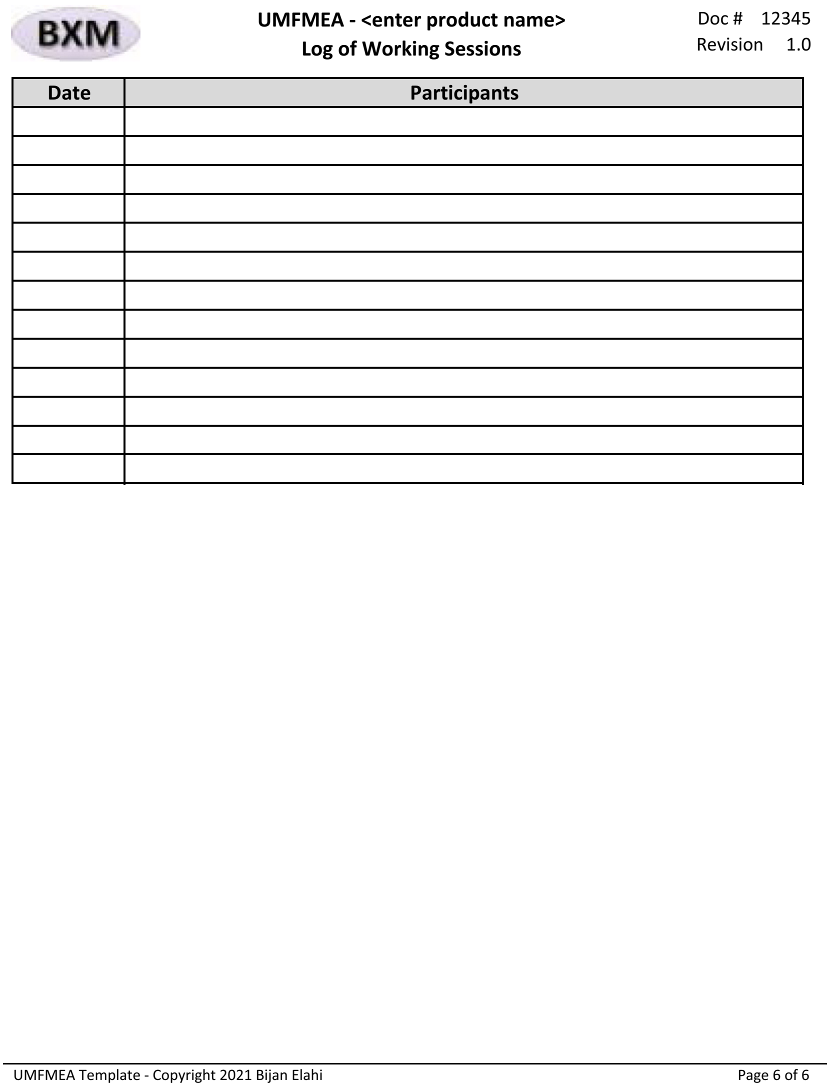
Doc # 12345
Revision 1.0

Revision History

Revision	Author	CR	Description of Change

UMFMEA Template - Copyright 2021 Bijan Elahi

Page 5 of 6



BXM

UMFMEA - <enter product name>
Log of Working Sessions

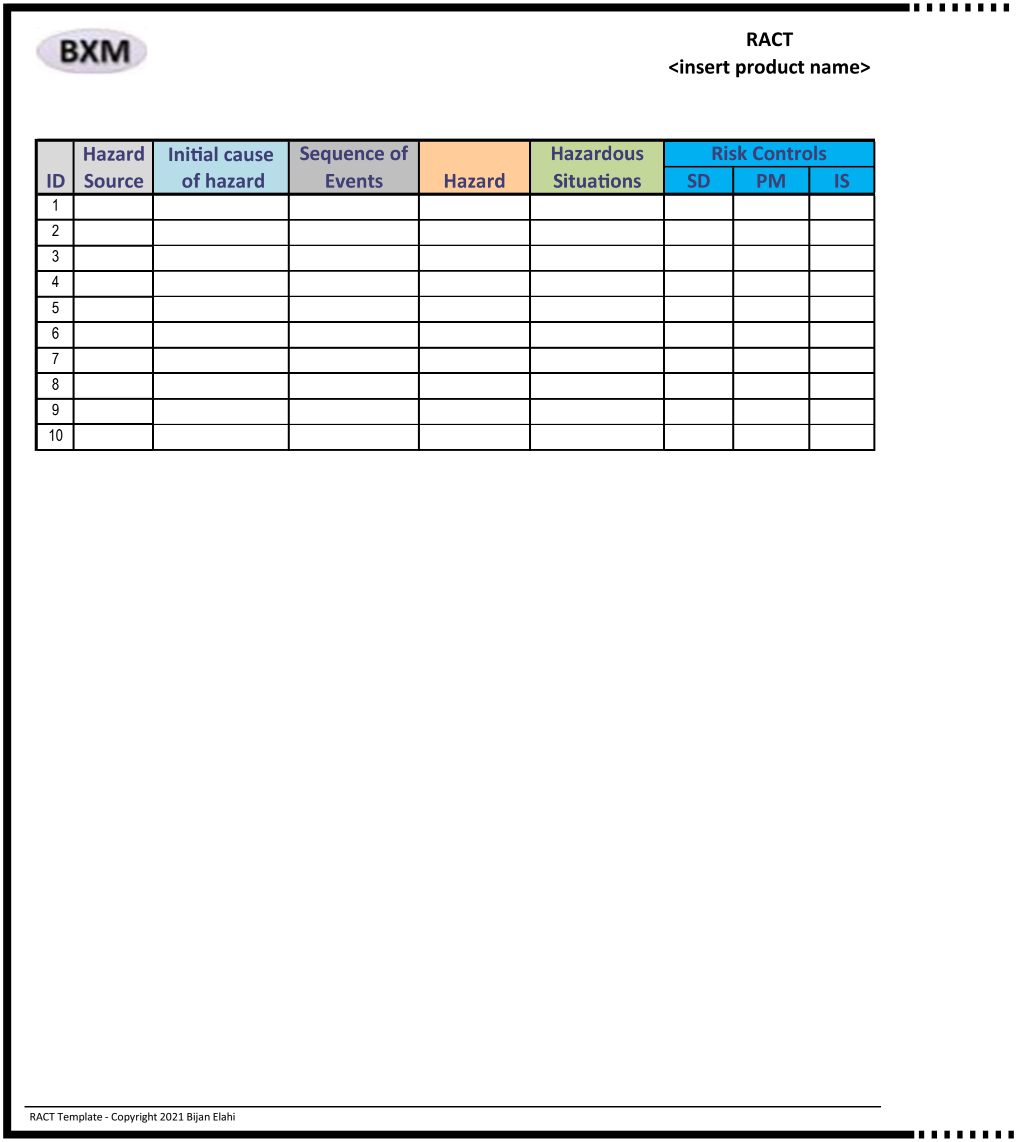
Doc # 12345
Revision 1.0

Date	Participants

UMFMEA Template - Copyright 2021 Bijan Elahi

Page 6 of 6

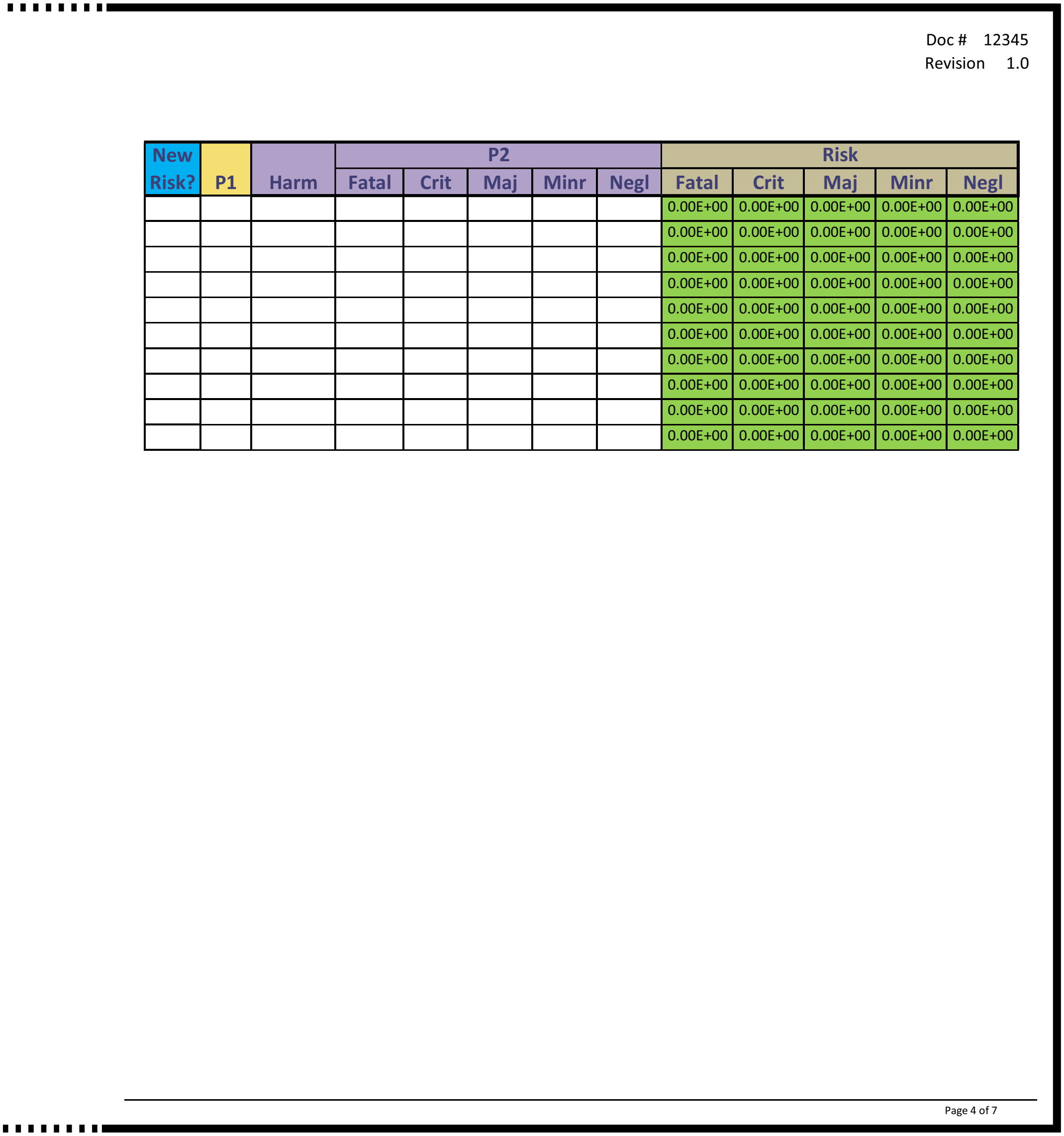
B.5 RACT TEMPLATE



BXM

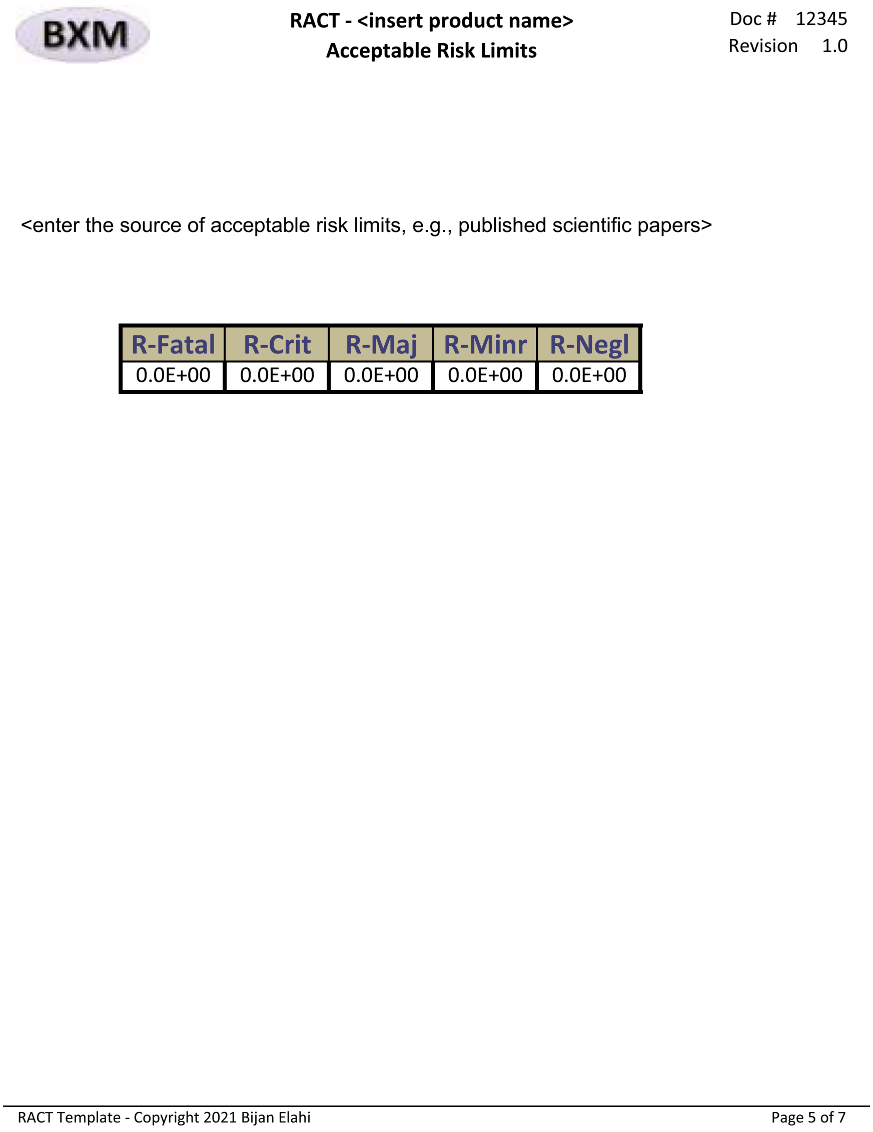
RACT
<insert product name>

ID	Hazard Source	Initial cause of hazard	Sequence of Events	Hazard	Hazardous Situations	Risk Controls		
						SD	PM	IS
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								



Doc # 12345
Revision 1.0

New			P2					Risk				
Risk?	P1	Harm	Fatal	Crit	Maj	Minr	Negl	Fatal	Crit	Maj	Minr	Negl
								0.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00
								0.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00
								0.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00
								0.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00
								0.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00
								0.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00
								0.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00
								0.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00
								0.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00
								0.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00



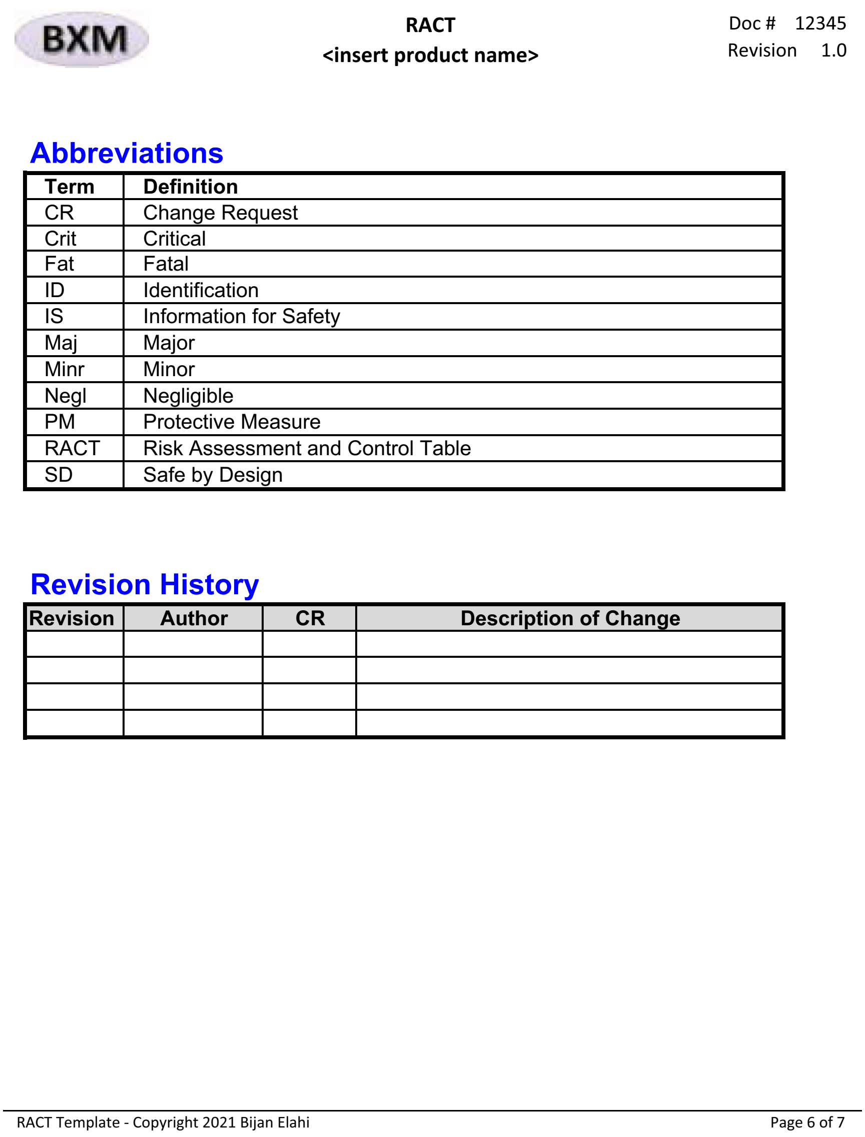
BXM

RACT - <insert product name>
Acceptable Risk Limits

Doc # 12345
Revision 1.0

<enter the source of acceptable risk limits, e.g., published scientific papers>

R-Fatal	R-Crit	R-Maj	R-Minr	R-Negl
0.0E+00	0.0E+00	0.0E+00	0.0E+00	0.0E+00



BXM

RACT
<insert product name>

Doc # 12345
Revision 1.0

Abbreviations

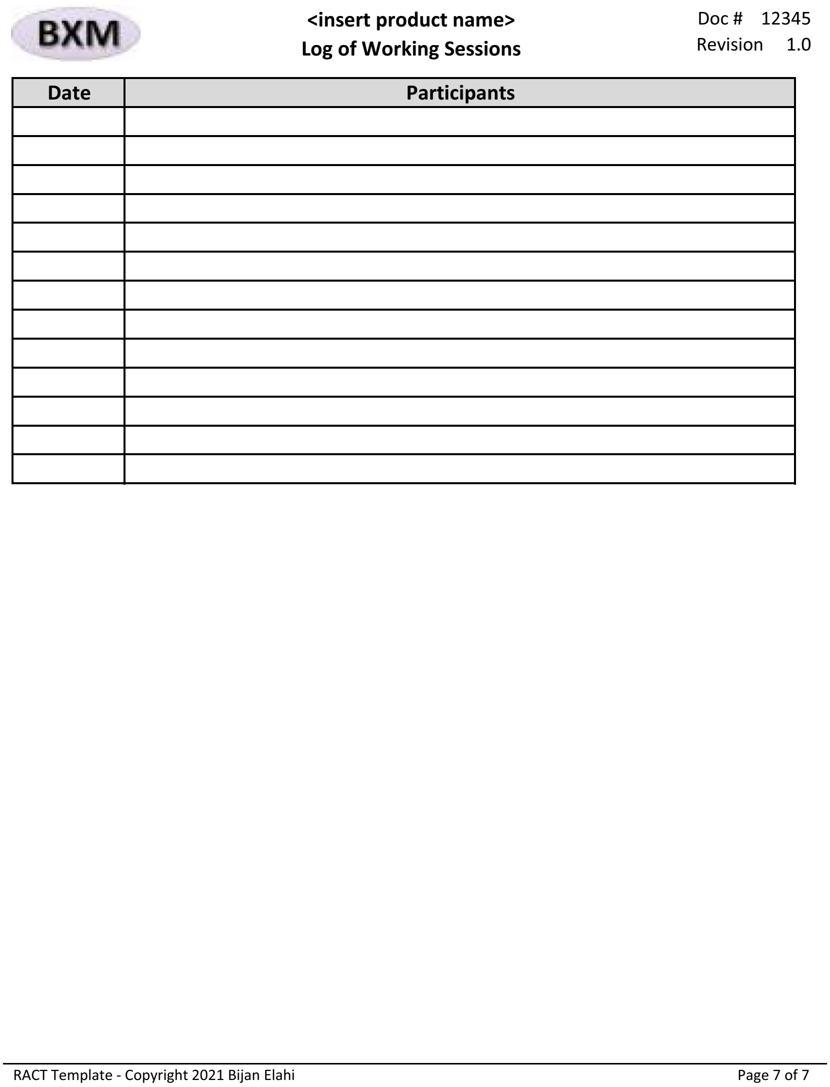
Term	Definition
CR	Change Request
Crit	Critical
Fat	Fatal
ID	Identification
IS	Information for Safety
Maj	Major
Minr	Minor
Negl	Negligible
PM	Protective Measure
RACT	Risk Assessment and Control Table
SD	Safe by Design

Revision History

Revision	Author	CR	Description of Change

RACT Template - Copyright 2021 Bijan Elahi

Page 6 of 7



BXM

<insert product name>
Log of Working Sessions

Doc # 12345
Revision 1.0

Date	Participants

RACT Template - Copyright 2021 Bijan Elahi

Page 7 of 7

Appendix C: Example Device – Vivio

In this appendix, the BXM method is applied to a hypothetical Automatic External Defibrillator (AED) named Vivio. The purpose for this example is to teach by illustration, the mechanics of the BXM method. Vivio is not a real device. The cited electronics and mechanical designs, or the Failure Modes or mitigations are not from a real device. Use the example as a vehicle to learn how risk management is done per the BXM method, and how the different elements of risk management are connected to one another.

The Vivio example is deliberately simplified and abbreviated to ease comprehension by the reader, and also to fit within the bounds of this book.

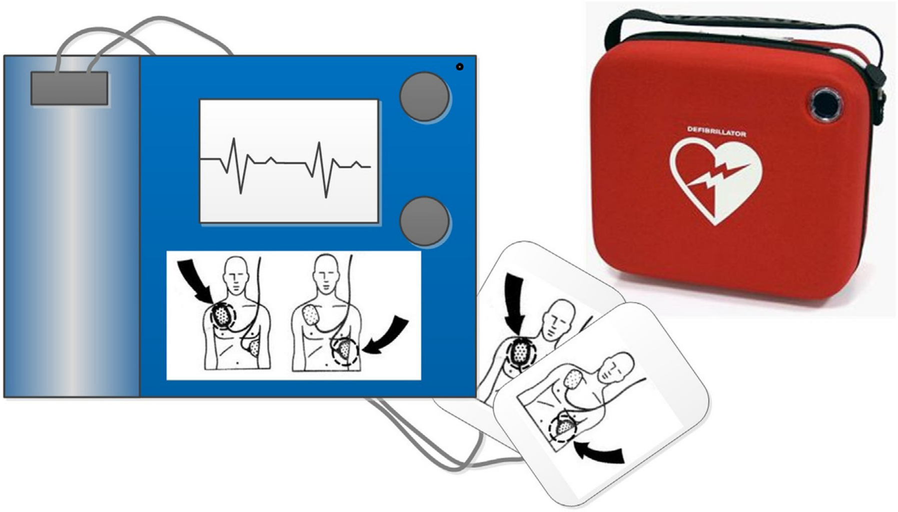
- Only *System-level* FMEAs are provided, i.e., System DFMEA, System PFMEA, and UMFMEA. Lower-level FMEAs are presumed to be performed as needed. A sample software FMEA is also provided.
- Only some of the Failure Modes with safety impact are carried forward to the RACT. In a real project, all Failure Modes in System-level FMEAs that have a safety impact should be carried forward to the RACT
- Traceability Analysis Report is not included in this Appendix because for a fictitious product references to absent elements would not be meaningful to the reader.

C.1 VIVIO PRODUCT DESCRIPTION

Vivio is an Automatic External Defibrillator (AED). It is small, lightweight, rugged, and battery operated. Vivio is intended for simple and reliable operation by minimally trained people.

Vivio is intended to treat Ventricular Fibrillation (VF), the most common cause of sudden cardiac death (SCD). VF is a chaotic quivering of the heart muscle that prevents the heart from pumping blood. The only effective treatment of VF is defibrillaiton, which is sending an electric shock across the heart, so as to reset the heart and enable it to start pumping again. A victim of VF is generally unconscious. When properly applied, Vivio automatically senses, and diagnoses the victim's heart rhythm, and if VF is detected, Vivio delivers a high voltage electric shock to the victim's heart.

Vivio is comprised of the base unit, two disposable pads, and the outer casing. The user is expected to apply the pads to the victim's bare chest according to the drawings on the pads and the device, and follow the verbal instructions given by the base unit.



C.2 VIVIO PRODUCT REQUIREMENTS

The following are the System requirement specifications for Vivio:

- Automatically detect ventricular fibrillation with a sensitivity of ≥95% and specificity of ≥90%
- Deliver at least 360 J of energy per shock
- Able to deliver a minimum of 200 shocks on a fresh battery
- Standby longevity ≥4 years on a fresh battery
- Max time between shocks: 20 seconds
- Able to detect and cope with artifacts, e.g., implanted pacemakers
- Visible indication of readiness for use
- Protective case for installation in public spaces, indoor or outdoor
- Weight: ≤2 kg (with battery, case and pads)
- Resistance to dust and water ingress:
  - While inside the case: IP54 or better
  - While outside the case: IP52 or better
- Environmental constraints:
  - Temperature: 0–50°C
  - Altitude: 0–4500 m above sea level
  - Crush resistance: 225 kg

C.3 VIVIO ARCHITECTURE

The high-level architectural design of Vivio is depicted in Fig. 66. The main blocks of Vivio design are identified in order to aid in the understanding of the product function and also to facilitate performing FMEAs on Vivio.

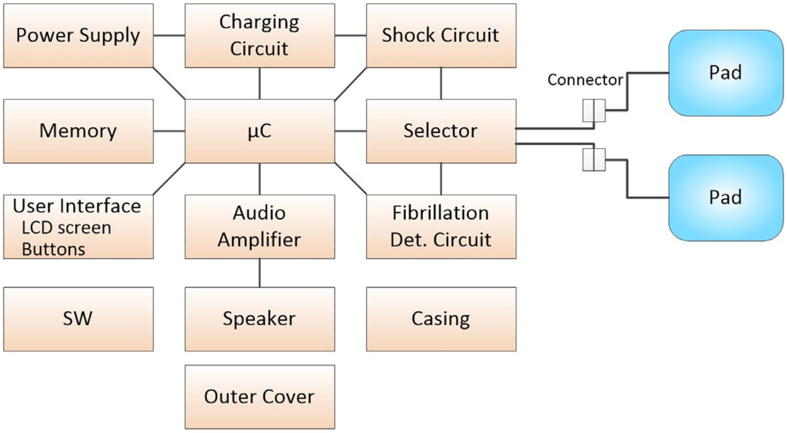
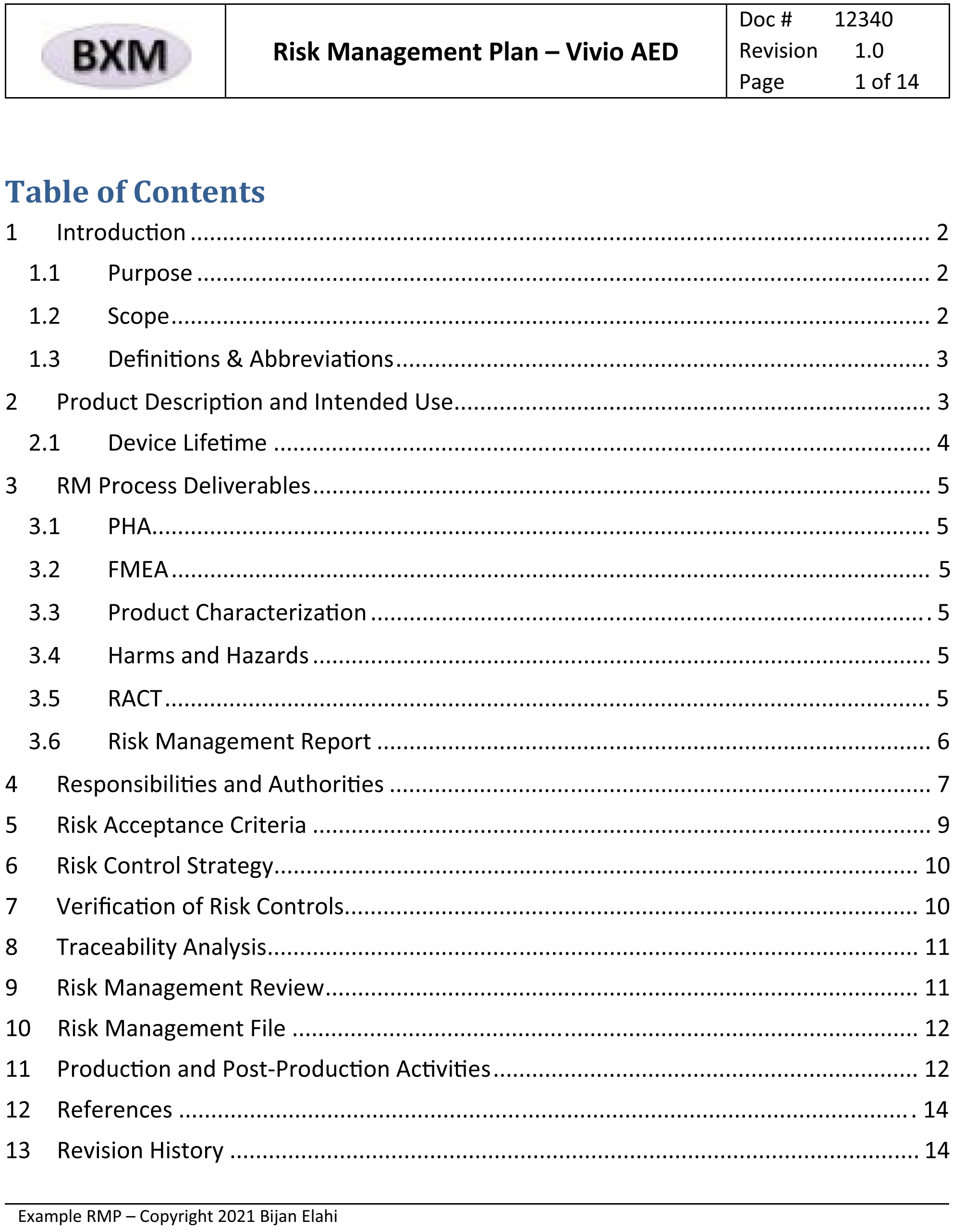


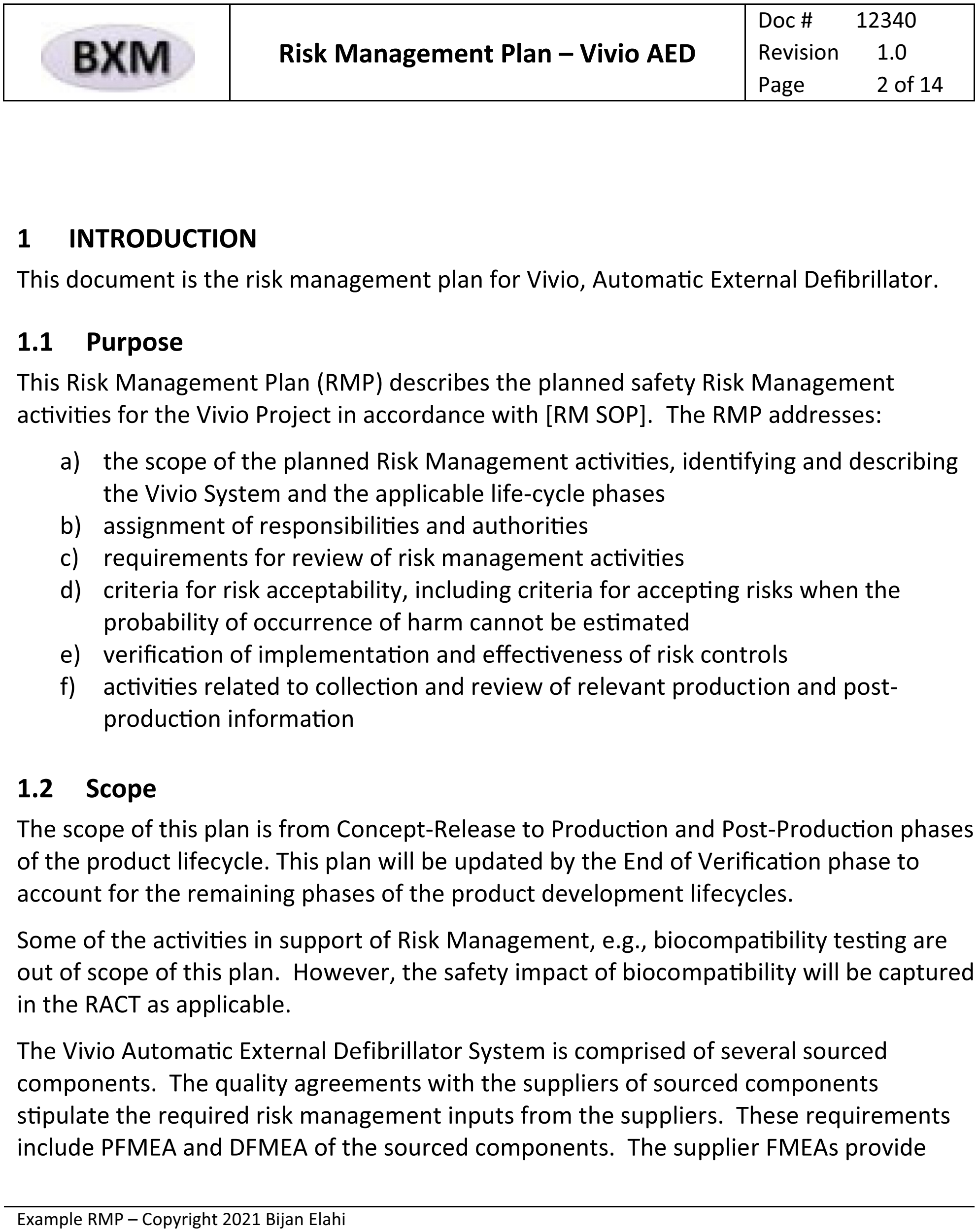
Figure 66 Vivio System Architecture.

C.4 RISK MANAGEMENT PLAN



BXM	**Risk Management Plan – Vivio AED**	Doc # 12340 Revision 1.0 Page 1 of 14

Table of Contents



BXM	**Risk Management Plan – Vivio AED**	Doc # 12340 Revision 1.0 Page 2 of 14

1 INTRODUCTION

This document is the risk management plan for Vivio, Automatic External Defibrillator.

1.1 Purpose

This Risk Management Plan (RMP) describes the planned safety Risk Management activities for the Vivio Project in accordance with [RM SOP]. The RMP addresses:

a) the scope of the planned Risk Management activities, identifying and describing the Vivio System and the applicable life-cycle phases
b) assignment of responsibilities and authorities
c) requirements for review of risk management activities
d) criteria for risk acceptability, including criteria for accepting risks when the probability of occurrence of harm cannot be estimated
e) verification of implementation and effectiveness of risk controls
f) activities related to collection and review of relevant production and post-production information

1.2 Scope

The scope of this plan is from Concept-Release to Production and Post-Production phases of the product lifecycle. This plan will be updated by the End of Verification phase to account for the remaining phases of the product development lifecycles.

Some of the activities in support of Risk Management, e.g., biocompatibility testing are out of scope of this plan. However, the safety impact of biocompatibility will be captured in the RACT as applicable.

The Vivio Automatic External Defibrillator System is comprised of several sourced components. The quality agreements with the suppliers of sourced components stipulate the required risk management inputs from the suppliers. These requirements include PFMEA and DFMEA of the sourced components. The supplier FMEAs provide input into the risk analysis of Vivio. Also, the quality agreements require that any change to the design, materials, or manufacturing of the sourced components be promptly reported to “Company” for impact analysis on Vivio risk analysis.

1.3 Definitions & Abbreviations

See [Glossary] for an overview of definitions & abbreviations used in this document.

The following definitions will be used in the RM process:

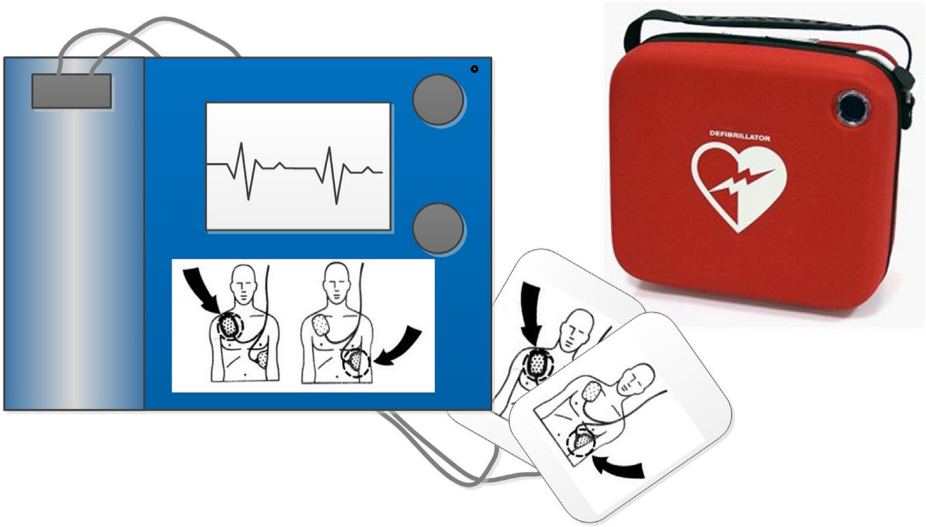
Table 1 - Definitions of Severity Classes

Class	Definition
Fatal	death
Critical	permanent impairment or irreversible injury
Major	injury or impairment requiring medical or surgical intervention
Minor	temporary injury or impairment not requiring medical or surgical intervention
Negligible	inconvenience, or temporary discomfort

2 PRODUCT DESCRIPTION AND INTENDED USE

Vivio is a portable Automatic External Defibrillator (AED), designed for indoor/outdoor storage, and use by minimally trained individuals. Vivio is equipped with a color LCD display. Vivio provides use instructions in graphic format on the LCD display, and speaks in 14 languages. Language selection is configurable for use in various geographies.

BXM	Risk Management Plan – Vivio AED	Doc # 12340 Revision 1.0 Page 4 of 14



When contact-pads are properly applied to the patient chest, Vivio automatically monitors patient's heart rhythm, detects fibrillation and emits a bi-phasic trans-thoracic shock of approximately 360 J to defibrillate the heart. Vivio operates on a primary battery, which is user-replaceable. Contact-pads are single-use products which are supplied by a third-party manufacturer. The replacement contact-pads are provided by the customer. Vivio is intended for use on adults, and children who are over 25 kg, or older than 8 years.

2.1 Device Lifetime

The Vivio AED is expected to have a device lifetime of 10 years from the date of manufacture. This is based on historical failure rates of the electronic components that are used in Vivio.

3 RM PROCESS DELIVERABLES

3.1 PHA

At the concept phase, a Preliminary Hazard Analysis [PHA] will be performed for a high-level assessment of the System risks. The [PHA] will include a Fault Tree Analysis.

3.2 FMEA

The project will execute Design, Software, Use/Misuse, and Process FMEAs according to [RM SOP]. Software FMEA will be performed subordinate to System DFMEA. At the System level, a DFMEA, PFMEA and UMFMEA will be produced.

FMEA's are conducted with the intention to identify potential causal chains that could lead to System hazards. During FMEAs Failure Modes whose End Effects do not lead to System hazards may also be identified. End effects from top-level FMEAs that could potentially lead to harms will be captured as hazards in the [RACT] for risk assessment.

3.3 Product Characterization

The risk management team will characterize Vivio using the questions listed in annex A of ISO/TR 24971:2020. The results of annex A answers will be logged in the risk management file. Characteristics that are related to safety will be included in the identification of hazards, and information for safety.

3.4 Harms and Hazards

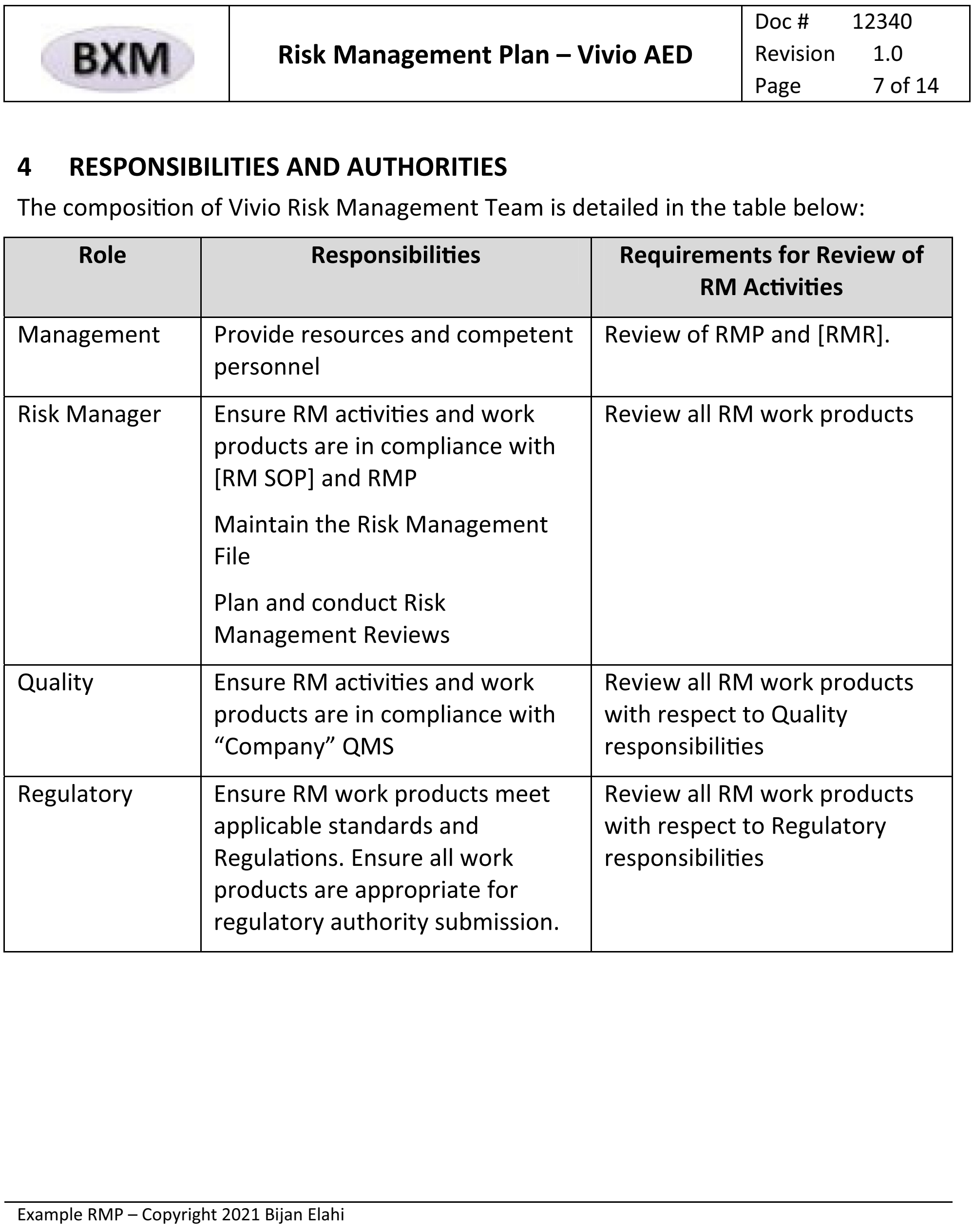
A comprehensive list of hazards and potential harms related to the use of Vivio have been identified in [CHL] and [HAL]. For each harm in [HAL], the probabilities of occurrence of the outcomes from that harm have been estimated in five severity classes as defined in **Table 1** above. This information is used in the risk estimation activity.

3.5 RACT

The results of lower-level FMEAs will be rolled up into a System DFMEA. The [RACT] will capture the hazards that are identified in the PHA and in the top-level System FMEAs. The individual risks for each hazard, hazardous situation and overall for Vivio, will be computed and evaluated for acceptability. The individual and overall residual risks will be computed using Boolean algebra.

3.6 Risk Management Report

A summary of the risk management activities and the conclusion of product risks and benefits will be captured in the Risk Management Report [RMR]. The report will also address production and post-production surveillance activities. As Vivio is a new device, the initial [RMR] will only have the results of Production information. Subsequent editions of the [RMR] will also include Post-Production results.



BXM	**Risk Management Plan – Vivio AED**	Doc # 12340 Revision 1.0 Page 7 of 14

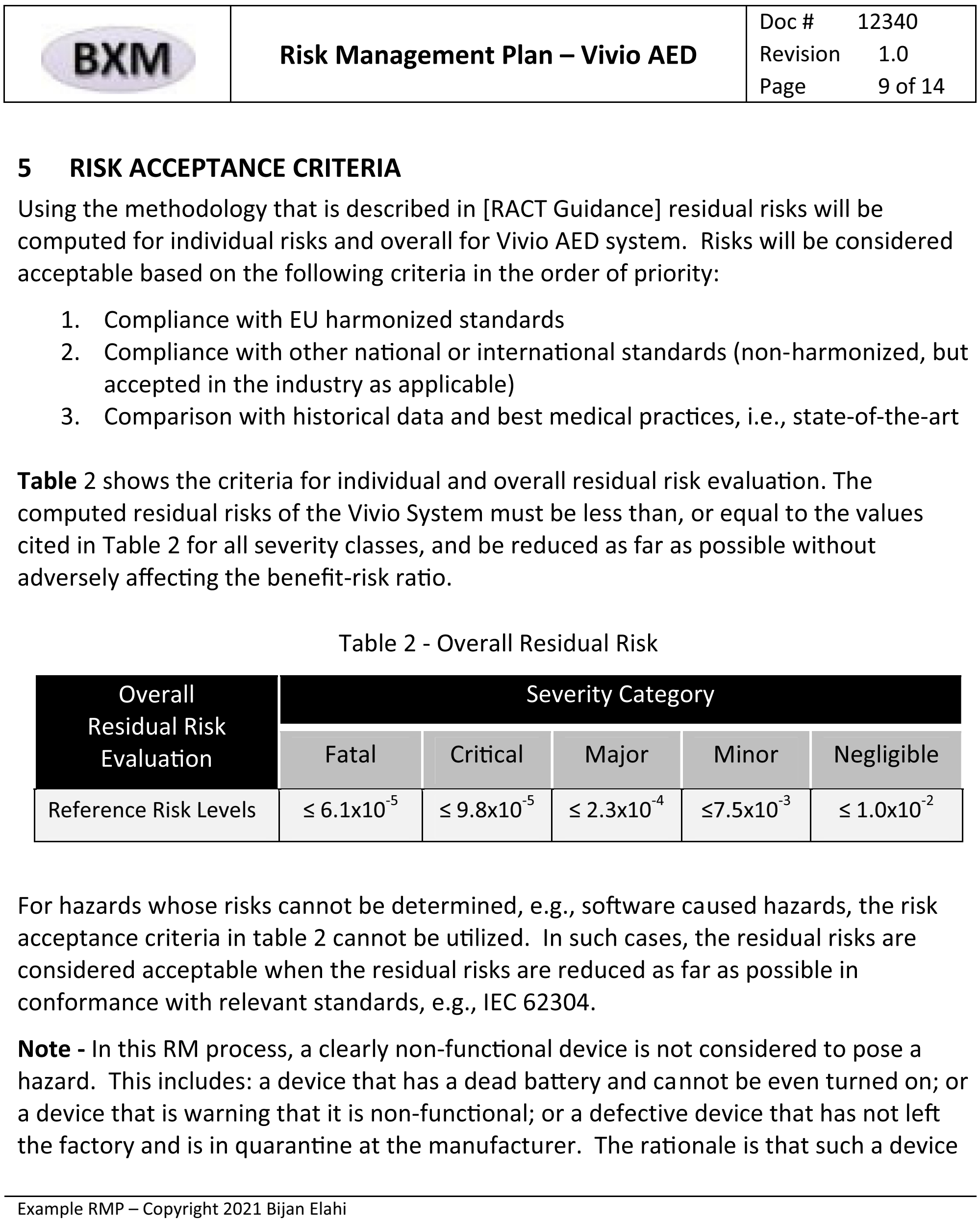
4 RESPONSIBILITIES AND AUTHORITIES

The composition of Vivio Risk Management Team is detailed in the table below:

Role	Responsibilities	Requirements for Review of RM Activities
Management	Provide resources and competent personnel	Review of RMP and [RMR].
Risk Manager	Ensure RM activities and work products are in compliance with [RM SOP] and RMP Maintain the Risk Management File Plan and conduct Risk Management Reviews	Review all RM work products
Quality	Ensure RM activities and work products are in compliance with “Company” QMS	Review all RM work products with respect to Quality responsibilities
Regulatory	Ensure RM work products meet applicable standards and Regulations. Ensure all work products are appropriate for regulatory authority submission.	Review all RM work products with respect to Regulatory responsibilities

Role	Responsibilities	Requirements for Review of RM Activities
Systems Engineering	Ensure RM work products are consistent with the system design, and risk control measures are valid, achievable and reasonable. Ensure RM work products meet applicable standards. Ensure the RM contributions by external suppliers are according to the quality agreements.	Review all RM work products with respect to Engineering responsibilities
Medical/Clinical	Ensure that the RM process makes sound choices from a medical perspective and that interactions with patient/user are correctly considered	Review all RM work products with respect to Medical/Clinical responsibilities
SMEs	Provide expert opinion/consulting to RMT as needed, to assist in technical evaluation of RM work products Ensure RM work products meet applicable standards, as appropriate.	No formal review responsibilities

Prior to integration into the [RACT], the input from suppliers will be reviewed and approved by Systems engineering as well as the RMT as defined in the table above.



BXM	**Risk Management Plan – Vivio AED**	Doc # 12340 Revision 1.0 Page 9 of 14

5 RISK ACCEPTANCE CRITERIA

Using the methodology that is described in [RACT Guidance] residual risks will be computed for individual risks and overall for Vivio AED system. Risks will be considered acceptable based on the following criteria in the order of priority:

1. Compliance with EU harmonized standards
2. Compliance with other national or international standards (non-harmonized, but accepted in the industry as applicable)
3. Comparison with historical data and best medical practices, i.e., state-of-the-art

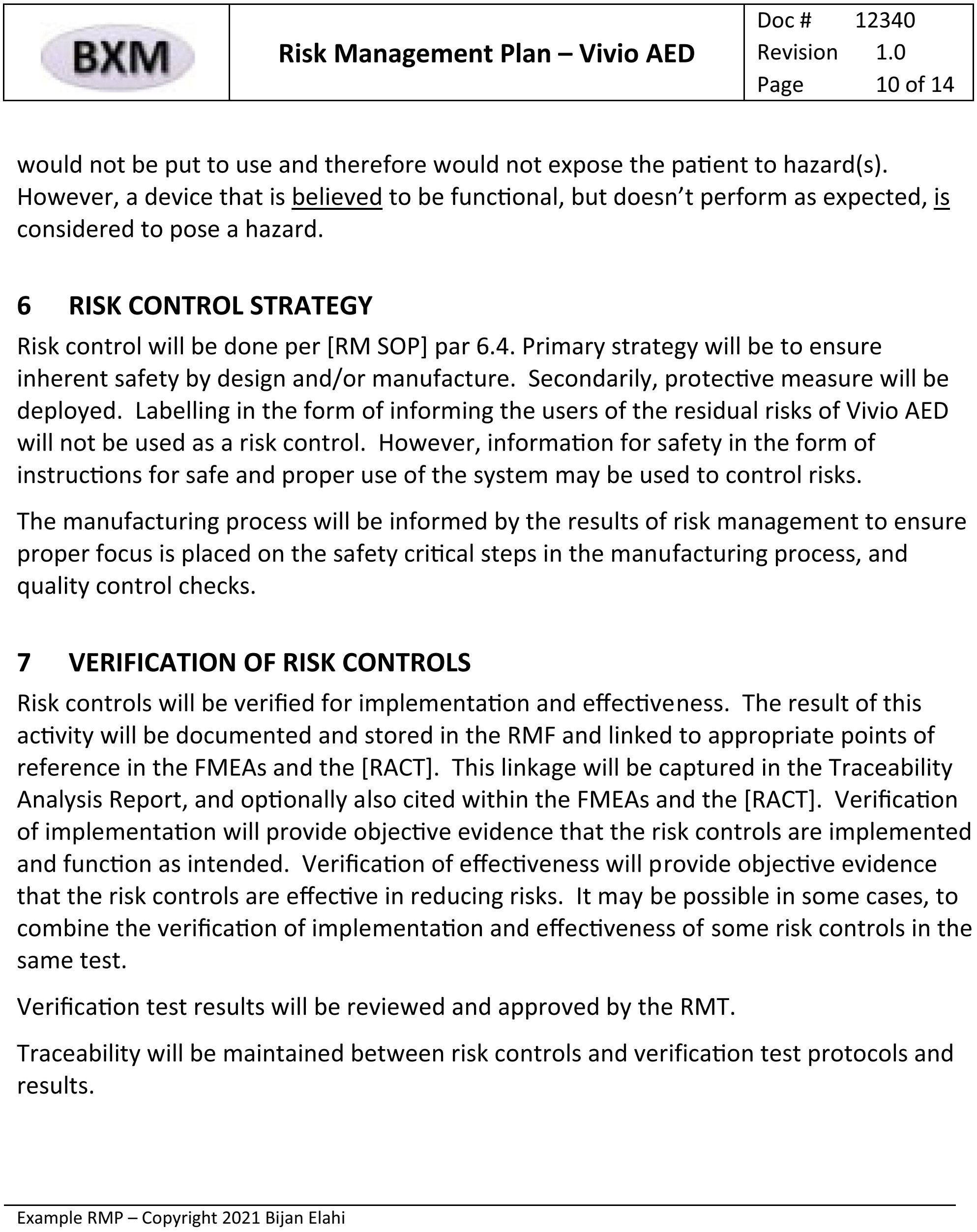
Table 2 shows the criteria for individual and overall residual risk evaluation. The computed residual risks of the Vivio System must be less than, or equal to the values cited in Table 2 for all severity classes, and be reduced as far as possible without adversely affecting the benefit-risk ratio.

Table 2 - Overall Residual Risk

Overall Residual Risk Evaluation	Severity Category				
	Fatal	Critical	Major	Minor	Negligible
Reference Risk Levels	≤ 6.1x10^{-5}	≤ 9.8x10^{-5}	≤ 2.3x10^{-4}	≤7.5x10^{-3}	≤ 1.0x10^{-2}

For hazards whose risks cannot be determined, e.g., software caused hazards, the risk acceptance criteria in table 2 cannot be utilized. In such cases, the residual risks are considered acceptable when the residual risks are reduced as far as possible in conformance with relevant standards, e.g., IEC 62304.

Note - In this RM process, a clearly non-functional device is not considered to pose a hazard. This includes: a device that has a dead battery and cannot be even turned on; or a device that is warning that it is non-functional; or a defective device that has not left the factory and is in quarantine at the manufacturer. The rationale is that such a device



would not be put to use and therefore would not expose the patient to hazard(s). However, a device that is believed to be functional, but doesn't perform as expected, is considered to pose a hazard.

6 RISK CONTROL STRATEGY

Risk control will be done per [RM SOP] par 6.4. Primary strategy will be to ensure inherent safety by design and/or manufacture. Secondarily, protective measure will be deployed. Labelling in the form of informing the users of the residual risks of Vivio AED will not be used as a risk control. However, information for safety in the form of instructions for safe and proper use of the system may be used to control risks.

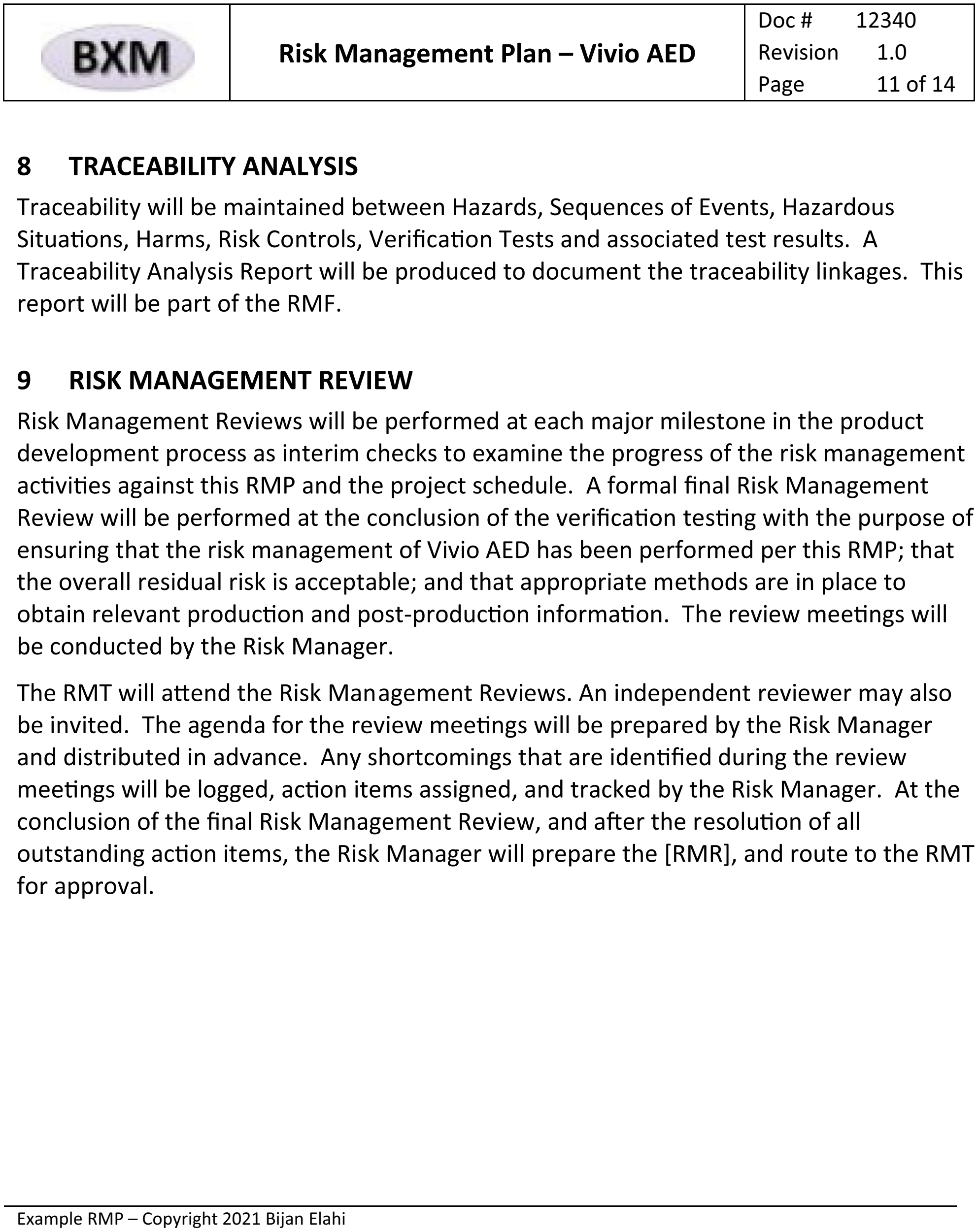
The manufacturing process will be informed by the results of risk management to ensure proper focus is placed on the safety critical steps in the manufacturing process, and quality control checks.

7 VERIFICATION OF RISK CONTROLS

Risk controls will be verified for implementation and effectiveness. The result of this activity will be documented and stored in the RMF and linked to appropriate points of reference in the FMEAs and the [RACT]. This linkage will be captured in the Traceability Analysis Report, and optionally also cited within the FMEAs and the [RACT]. Verification of implementation will provide objective evidence that the risk controls are implemented and function as intended. Verification of effectiveness will provide objective evidence that the risk controls are effective in reducing risks. It may be possible in some cases, to combine the verification of implementation and effectiveness of some risk controls in the same test.

Verification test results will be reviewed and approved by the RMT.

Traceability will be maintained between risk controls and verification test protocols and results.



BXM	**Risk Management Plan – Vivio AED**	Doc # 12340 Revision 1.0 Page 11 of 14

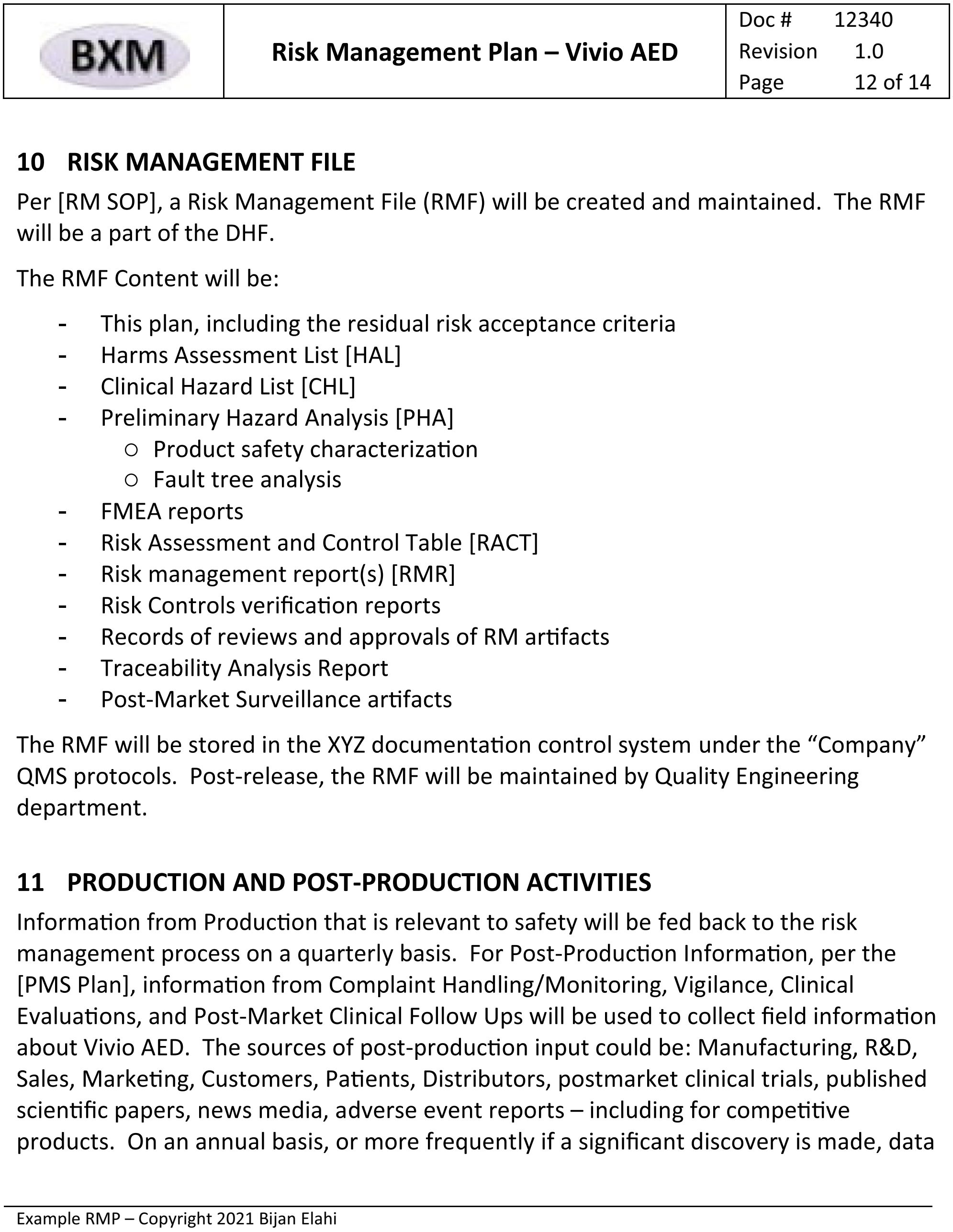
8 TRACEABILITY ANALYSIS

Traceability will be maintained between Hazards, Sequences of Events, Hazardous Situations, Harms, Risk Controls, Verification Tests and associated test results. A Traceability Analysis Report will be produced to document the traceability linkages. This report will be part of the RMF.

9 RISK MANAGEMENT REVIEW

Risk Management Reviews will be performed at each major milestone in the product development process as interim checks to examine the progress of the risk management activities against this RMP and the project schedule. A formal final Risk Management Review will be performed at the conclusion of the verification testing with the purpose of ensuring that the risk management of Vivio AED has been performed per this RMP; that the overall residual risk is acceptable; and that appropriate methods are in place to obtain relevant production and post-production information. The review meetings will be conducted by the Risk Manager.

The RMT will attend the Risk Management Reviews. An independent reviewer may also be invited. The agenda for the review meetings will be prepared by the Risk Manager and distributed in advance. Any shortcomings that are identified during the review meetings will be logged, action items assigned, and tracked by the Risk Manager. At the conclusion of the final Risk Management Review, and after the resolution of all outstanding action items, the Risk Manager will prepare the [RMR], and route to the RMT for approval.



BXM	**Risk Management Plan – Vivio AED**	Doc # 12340 Revision 1.0 Page 12 of 14

10 RISK MANAGEMENT FILE

Per [RM SOP], a Risk Management File (RMF) will be created and maintained. The RMF will be a part of the DHF.

The RMF Content will be:

- This plan, including the residual risk acceptance criteria
- Harms Assessment List [HAL]
- Clinical Hazard List [CHL]
- Preliminary Hazard Analysis [PHA]
  - Product safety characterization
  - Fault tree analysis
- FMEA reports
- Risk Assessment and Control Table [RACT]
- Risk management report(s) [RMR]
- Risk Controls verification reports
- Records of reviews and approvals of RM artifacts
- Traceability Analysis Report
- Post-Market Surveillance artifacts

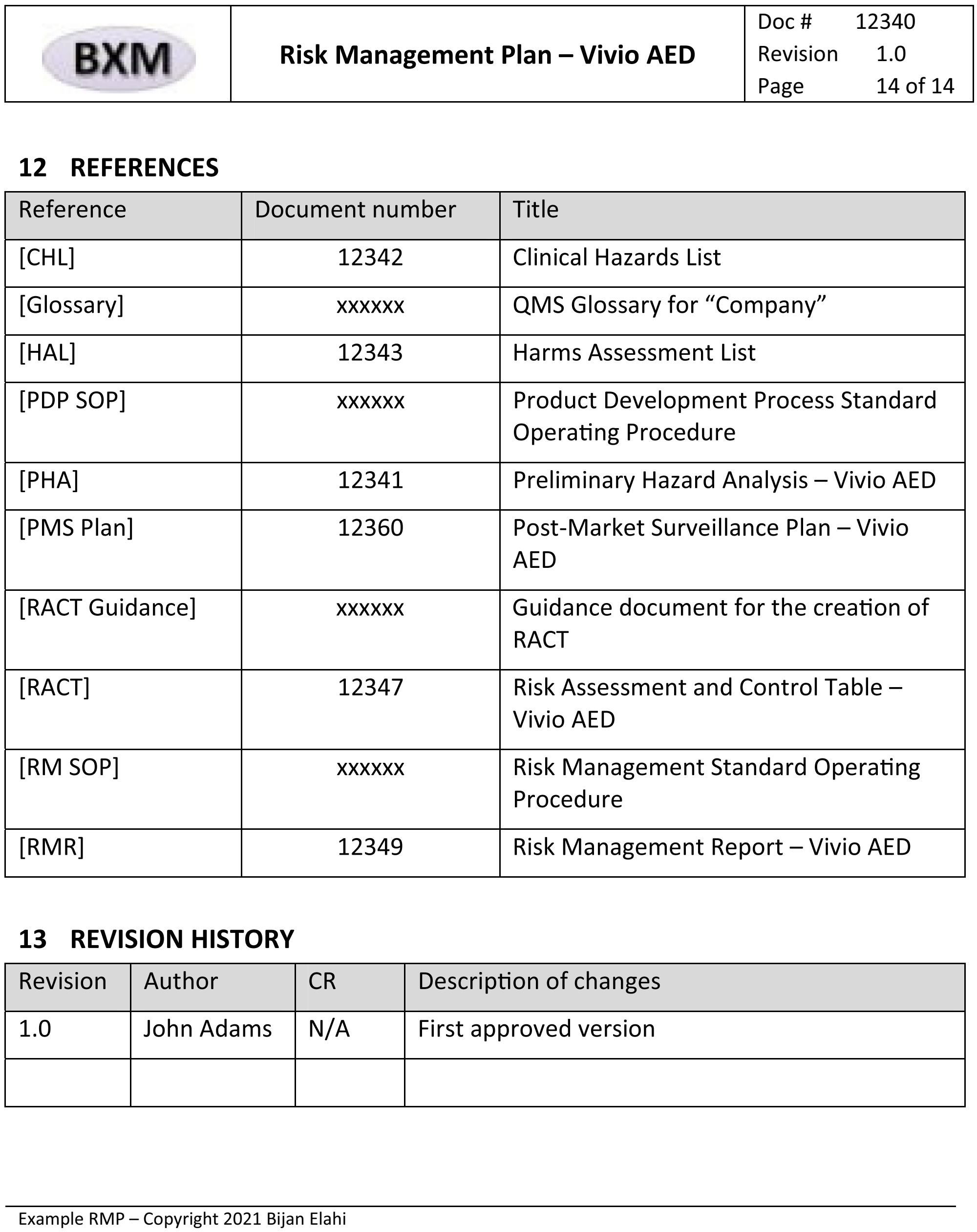
The RMF will be stored in the XYZ documentation control system under the “Company” QMS protocols. Post-release, the RMF will be maintained by Quality Engineering department.

11 PRODUCTION AND POST-PRODUCTION ACTIVITIES

Information from Production that is relevant to safety will be fed back to the risk management process on a quarterly basis. For Post-Production Information, per the [PMS Plan], information from Complaint Handling/Monitoring, Vigilance, Clinical Evaluations, and Post-Market Clinical Follow Ups will be used to collect field information about Vivio AED. The sources of post-production input could be: Manufacturing, R&D, Sales, Marketing, Customers, Patients, Distributors, postmarket clinical trials, published scientific papers, news media, adverse event reports – including for competitive products. On an annual basis, or more frequently if a significant discovery is made, data from above sources will be evaluated for relevance to Vivio AED. The ensuing actions depend on the collected information and can fall in a spectrum, including:

- Documentation of the information-collection actions, and discoveries where no change to the Vivio AED Risk Management artifacts is necessary
- Update to Vivio AED RMF including FMEAs, and [RMR] with outcomes being:
    - Overall residual risk remains acceptable and the benefits outweigh the overall residual risks
    - Overall residual risk no longer acceptable, triggering a range of other actions e.g. Health Hazard Assessment, CAPAs, Field Safety Corrective Actions, Product Hold Orders, Recalls, etc.

Also, based on the new knowledge gained from post-production information [CHL], [HAL], or [RM SOP] may be updated.



BXM	**Risk Management Plan – Vivio AED**	Doc # 12340 Revision 1.0 Page 14 of 14

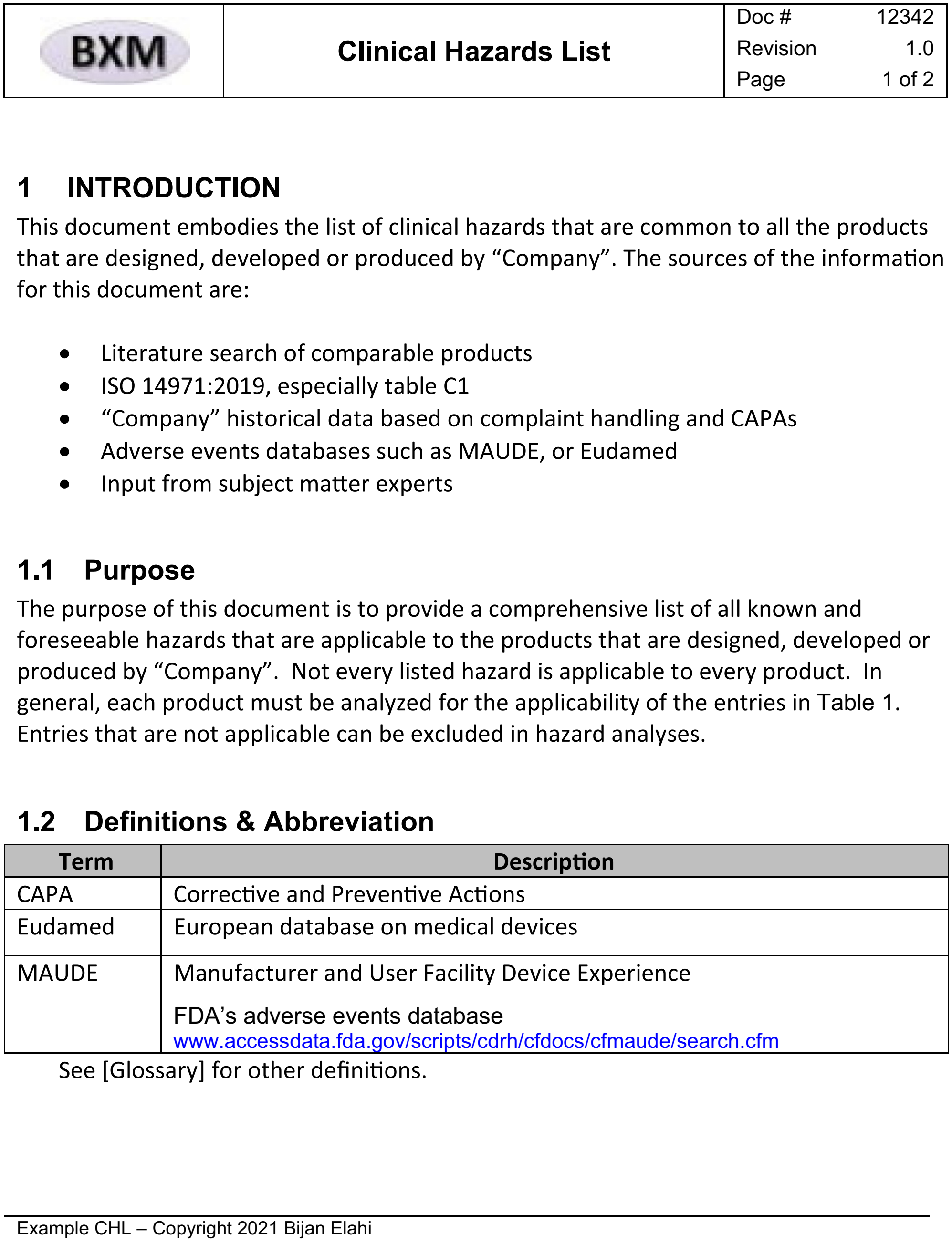
12 REFERENCES

Reference	Document number	Title
[CHL]	12342	Clinical Hazards List
[Glossary]	xxxxxx	QMS Glossary for “Company”
[HAL]	12343	Harms Assessment List
[PDP SOP]	xxxxxx	Product Development Process Standard Operating Procedure
[PHA]	12341	Preliminary Hazard Analysis – Vivio AED
[PMS Plan]	12360	Post-Market Surveillance Plan – Vivio AED
[RACT Guidance]	xxxxxx	Guidance document for the creation of RACT
[RACT]	12347	Risk Assessment and Control Table – Vivio AED
[RM SOP]	xxxxxx	Risk Management Standard Operating Procedure
[RMR]	12349	Risk Management Report – Vivio AED

13 REVISION HISTORY

Revision	Author	CR	Description of changes
1.0	John Adams	N/A	First approved version

C.5 CLINICAL HAZARDS LIST



BXM	Clinical Hazards List	Doc # 12342 Revision 1.0 Page 1 of 2

1 INTRODUCTION

This document embodies the list of clinical hazards that are common to all the products that are designed, developed or produced by “Company”. The sources of the information for this document are:

- Literature search of comparable products
- ISO 14971:2019, especially table C1
- “Company” historical data based on complaint handling and CAPAs
- Adverse events databases such as MAUDE, or Eudamed
- Input from subject matter experts

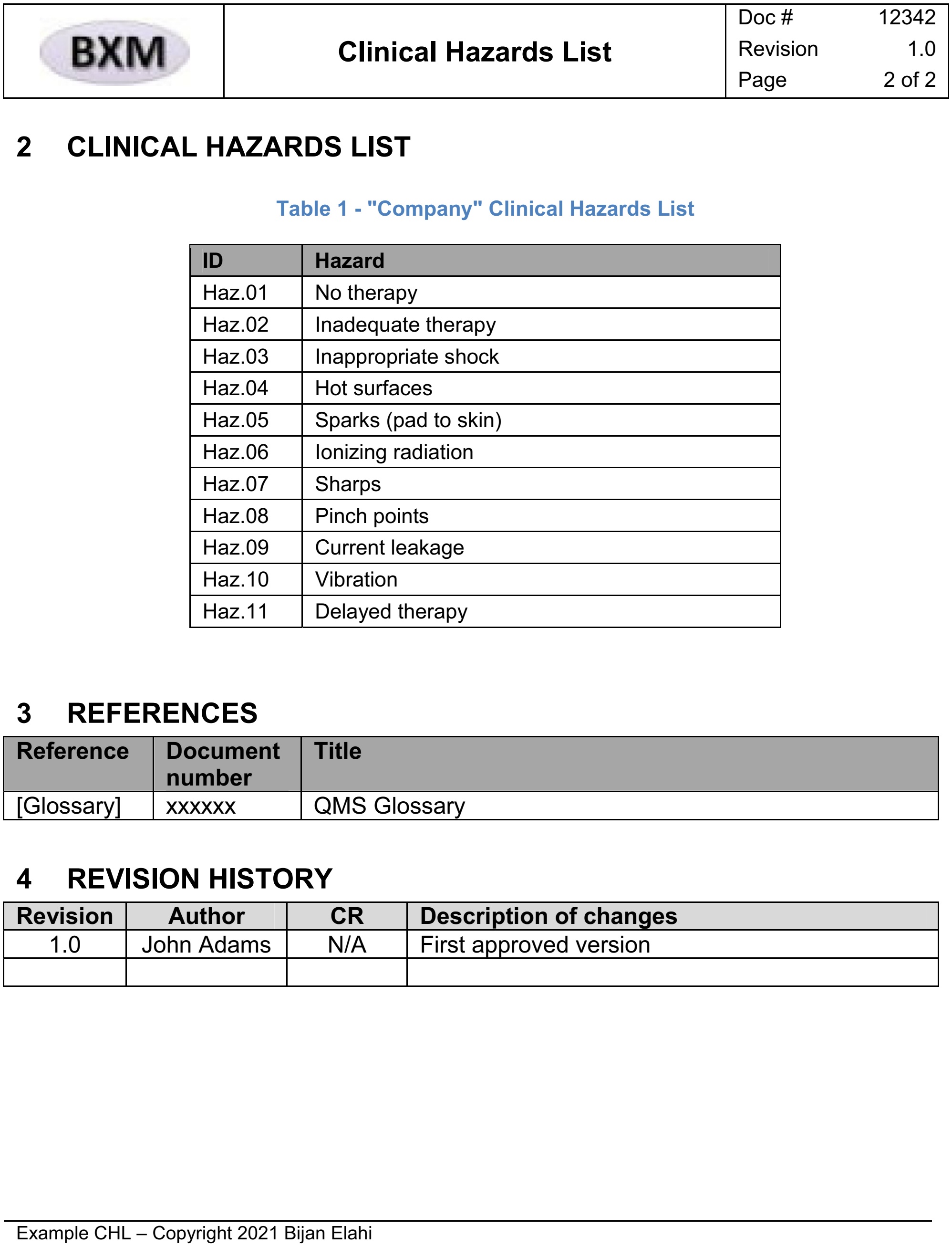
1.1 Purpose

The purpose of this document is to provide a comprehensive list of all known and foreseeable hazards that are applicable to the products that are designed, developed or produced by “Company”. Not every listed hazard is applicable to every product. In general, each product must be analyzed for the applicability of the entries in Table 1. Entries that are not applicable can be excluded in hazard analyses.

1.2 Definitions & Abbreviation

Term	Description
CAPA	Corrective and Preventive Actions
Eudamed	European database on medical devices
MAUDE	Manufacturer and User Facility Device Experience FDA’s adverse events database www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfmaude/search.cfm

See [Glossary] for other definitions.



BXM	Clinical Hazards List	Doc # Revision Page	12342 1.0 2 of 2

2 CLINICAL HAZARDS LIST

Table 1 - "Company" Clinical Hazards List

ID	Hazard
Haz.01	No therapy
Haz.02	Inadequate therapy
Haz.03	Inappropriate shock
Haz.04	Hot surfaces
Haz.05	Sparks (pad to skin)
Haz.06	Ionizing radiation
Haz.07	Sharps
Haz.08	Pinch points
Haz.09	Current leakage
Haz.10	Vibration
Haz.11	Delayed therapy

3 REFERENCES

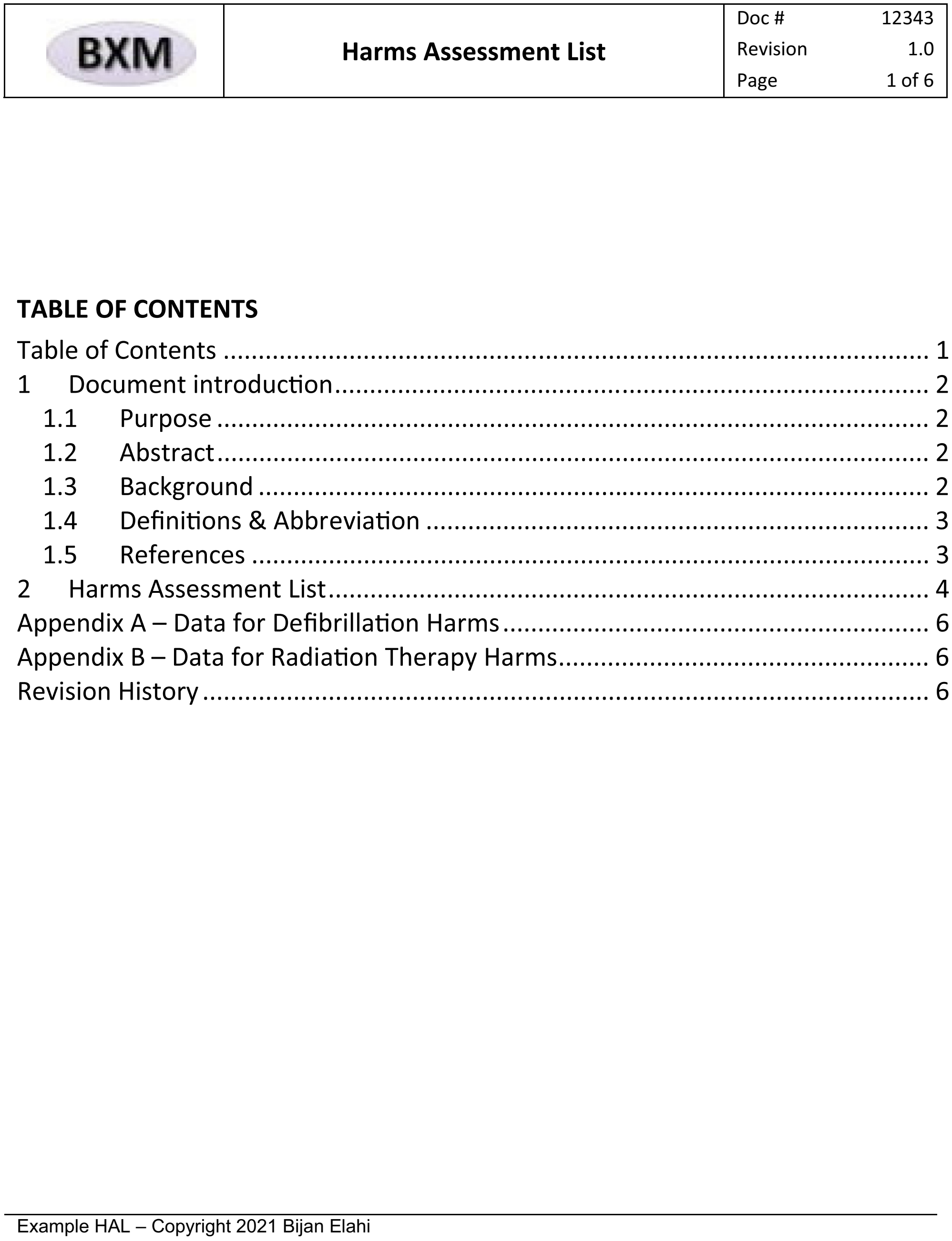
Reference	Document number	Title
[Glossary]	xxxxxx	QMS Glossary

4 REVISION HISTORY

Revision	Author	CR	Description of changes
1.0	John Adams	N/A	First approved version

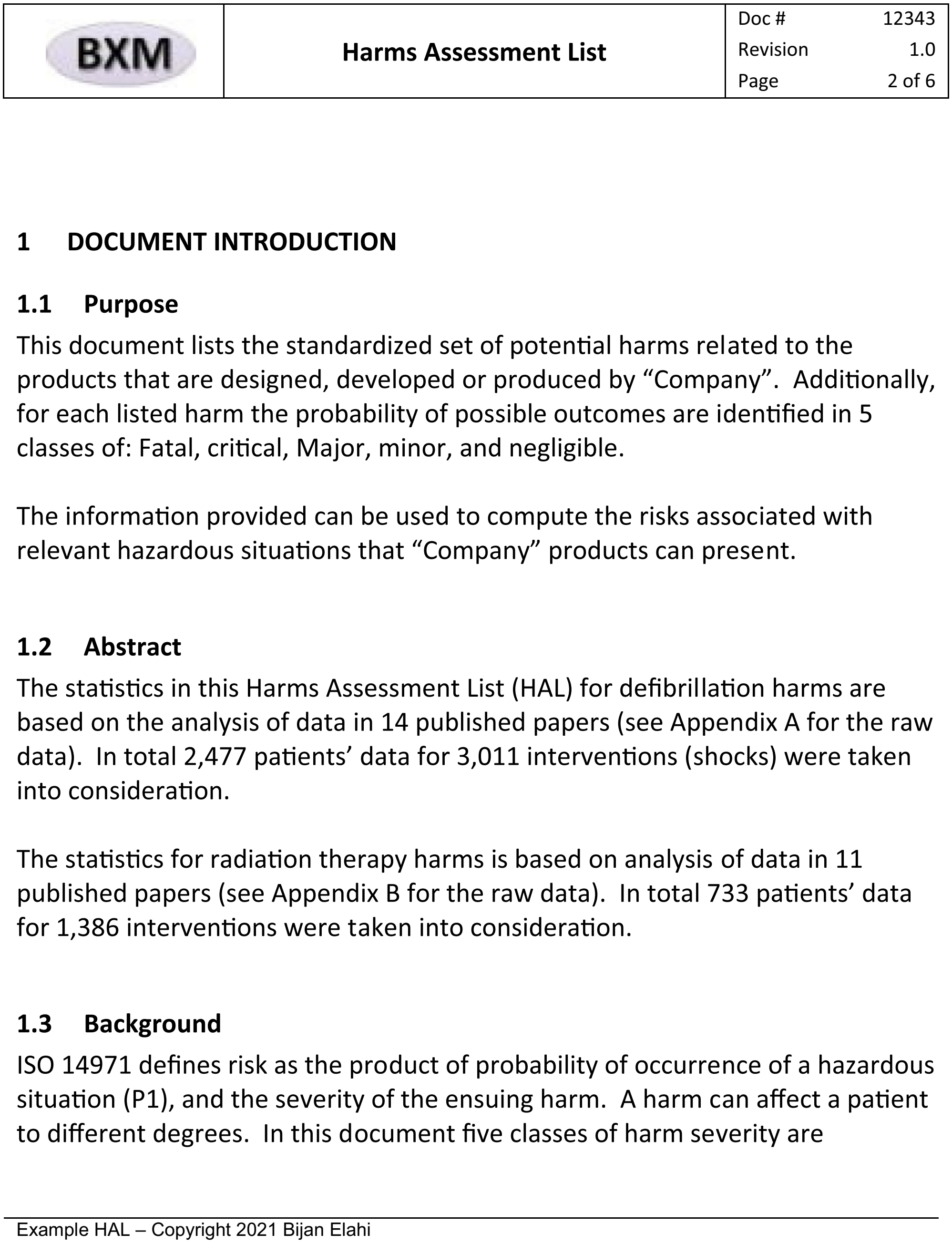
Example CHL – Copyright 2021 Bijan Elahi

C.6 HARMS ASSESSMENT LIST



BXM	Harms Assessment List	Doc # 12343 Revision 1.0 Page 1 of 6

TABLE OF CONTENTS



BXM	Harms Assessment List	Doc #	12343
		Revision	1.0
		Page	2 of 6

1 DOCUMENT INTRODUCTION

1.1 Purpose

This document lists the standardized set of potential harms related to the products that are designed, developed or produced by “Company”. Additionally, for each listed harm the probability of possible outcomes are identified in 5 classes of: Fatal, critical, Major, minor, and negligible.

The information provided can be used to compute the risks associated with relevant hazardous situations that “Company” products can present.

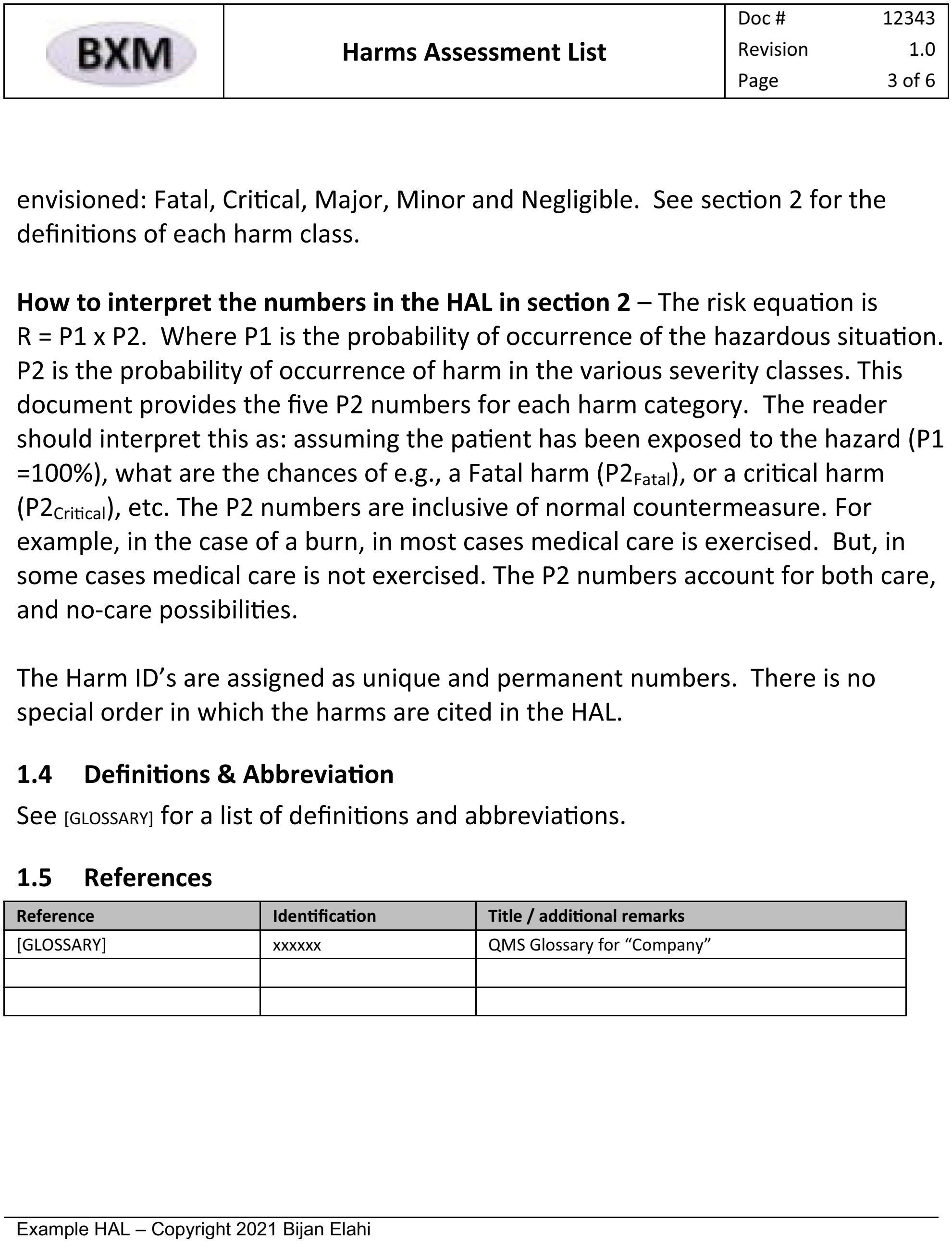
1.2 Abstract

The statistics in this Harms Assessment List (HAL) for defibrillation harms are based on the analysis of data in 14 published papers (see Appendix A for the raw data). In total 2,477 patients’ data for 3,011 interventions (shocks) were taken into consideration.

The statistics for radiation therapy harms is based on analysis of data in 11 published papers (see Appendix B for the raw data). In total 733 patients’ data for 1,386 interventions were taken into consideration.

1.3 Background

ISO 14971 defines risk as the product of probability of occurrence of a hazardous situation (P1), and the severity of the ensuing harm. A harm can affect a patient to different degrees. In this document five classes of harm severity are



envisioned: Fatal, Critical, Major, Minor and Negligible. See section 2 for the definitions of each harm class.

How to interpret the numbers in the HAL in section 2 – The risk equation is R = P1 x P2. Where P1 is the probability of occurrence of the hazardous situation. P2 is the probability of occurrence of harm in the various severity classes. This document provides the five P2 numbers for each harm category. The reader should interpret this as: assuming the patient has been exposed to the hazard (P1 =100%), what are the chances of e.g., a Fatal harm ($P2_{Fatal}$), or a critical harm ($P2_{Critical}$), etc. The P2 numbers are inclusive of normal countermeasure. For example, in the case of a burn, in most cases medical care is exercised. But, in some cases medical care is not exercised. The P2 numbers account for both care, and no-care possibilities.

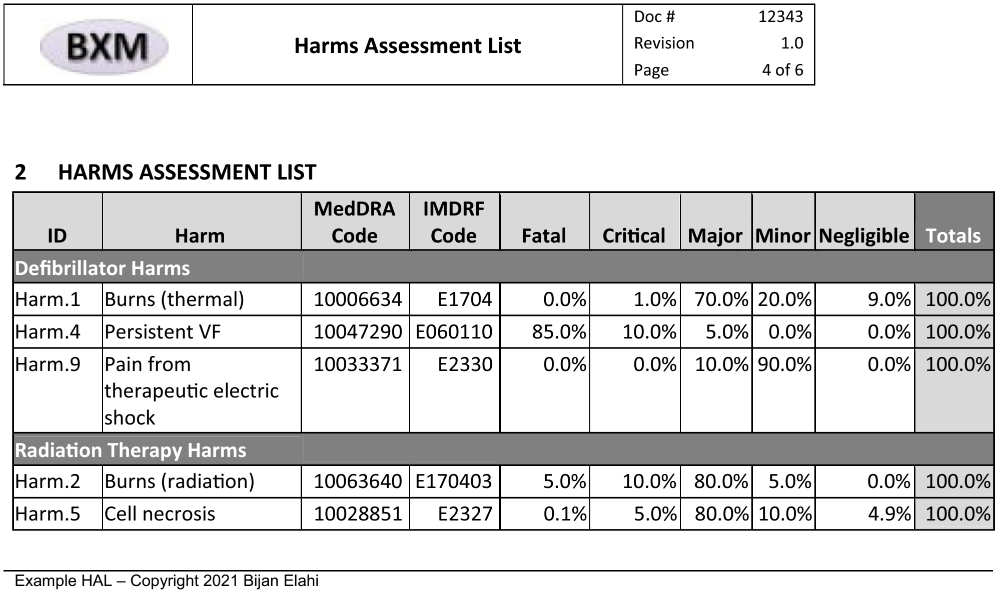
The Harm ID's are assigned as unique and permanent numbers. There is no special order in which the harms are cited in the HAL.

1.4 Definitions & Abbreviation

See [GLOSSARY] for a list of definitions and abbreviations.

1.5 References

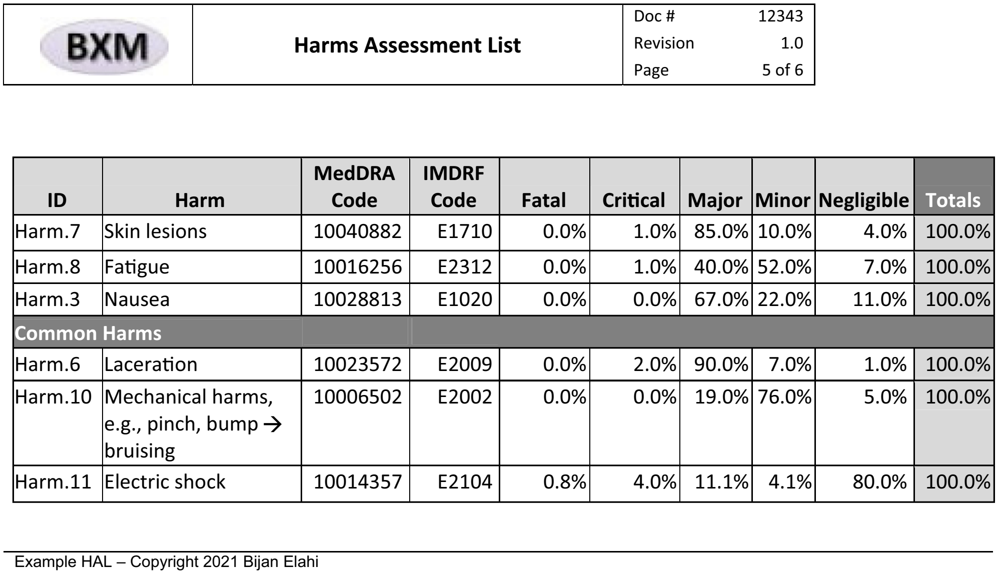
Reference	Identification	Title / additional remarks
[GLOSSARY]	xxxxxx	QMS Glossary for "Company"



BXM	Harms Assessment List	Doc # 12343 Revision 1.0 Page 4 of 6

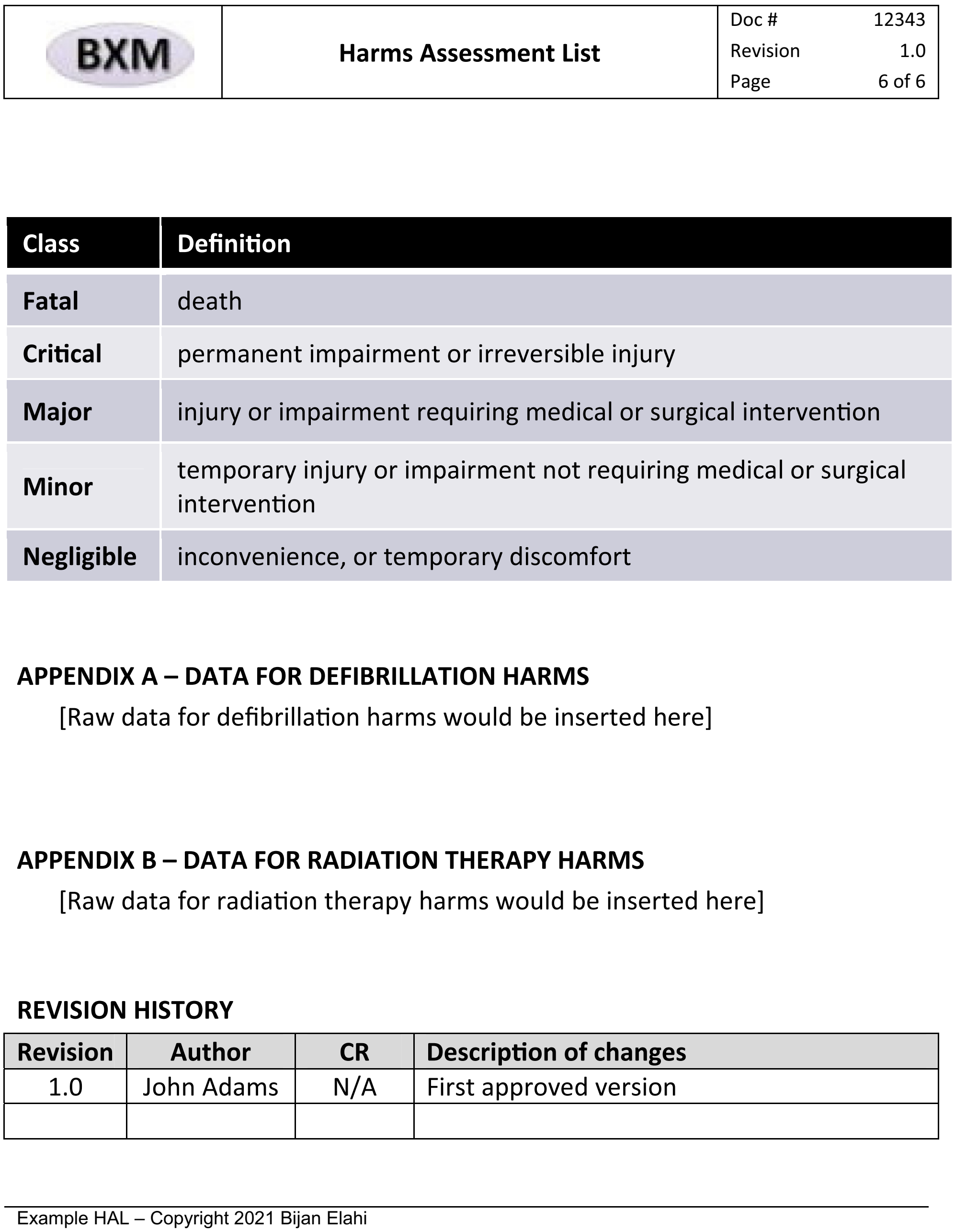
2 HARMS ASSESSMENT LIST

ID	Harm	MedDRA Code	IMDRF Code	Fatal	Critical	Major	Minor	Negligible	Totals
Defibrillator Harms									
Harm.1	Burns (thermal)	10006634	E1704	0.0%	1.0%	70.0%	20.0%	9.0%	100.0%
Harm.4	Persistent VF	10047290	E060110	85.0%	10.0%	5.0%	0.0%	0.0%	100.0%
Harm.9	Pain from therapeutic electric shock	10033371	E2330	0.0%	0.0%	10.0%	90.0%	0.0%	100.0%
Radiation Therapy Harms									
Harm.2	Burns (radiation)	10063640	E170403	5.0%	10.0%	80.0%	5.0%	0.0%	100.0%
Harm.5	Cell necrosis	10028851	E2327	0.1%	5.0%	80.0%	10.0%	4.9%	100.0%



BXM	Harms Assessment List	Doc # 12343 Revision 1.0 Page 5 of 6

ID	Harm	MedDRA Code	IMDRF Code	Fatal	Critical	Major	Minor	Negligible	Totals
Harm.7	Skin lesions	10040882	E1710	0.0%	1.0%	85.0%	10.0%	4.0%	100.0%
Harm.8	Fatigue	10016256	E2312	0.0%	1.0%	40.0%	52.0%	7.0%	100.0%
Harm.3	Nausea	10028813	E1020	0.0%	0.0%	67.0%	22.0%	11.0%	100.0%
Common Harms									
Harm.6	Laceration	10023572	E2009	0.0%	2.0%	90.0%	7.0%	1.0%	100.0%
Harm.10	Mechanical harms, e.g., pinch, bump → bruising	10006502	E2002	0.0%	0.0%	19.0%	76.0%	5.0%	100.0%
Harm.11	Electric shock	10014357	E2104	0.8%	4.0%	11.1%	4.1%	80.0%	100.0%



BXM	Harms Assessment List	Doc #	12343
		Revision	1.0
		Page	6 of 6

Class	Definition
Fatal	death
Critical	permanent impairment or irreversible injury
Major	injury or impairment requiring medical or surgical intervention
Minor	temporary injury or impairment not requiring medical or surgical intervention
Negligible	inconvenience, or temporary discomfort

APPENDIX A – DATA FOR DEFIBRILLATION HARMS

[Raw data for defibrillation harms would be inserted here]

APPENDIX B – DATA FOR RADIATION THERAPY HARMS

[Raw data for radiation therapy harms would be inserted here]

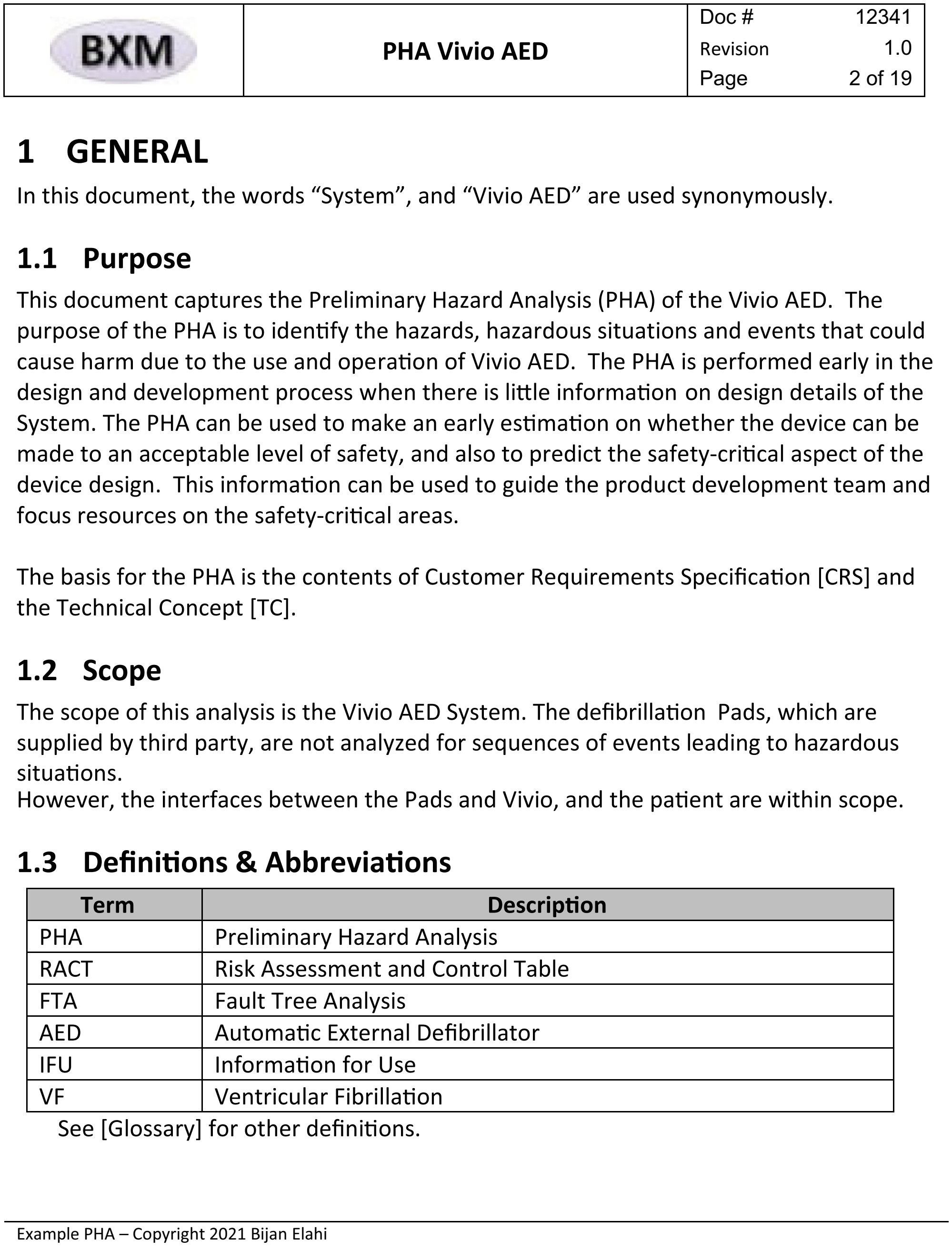
REVISION HISTORY

Revision	Author	CR	Description of changes
1.0	John Adams	N/A	First approved version

C.7 PRELIMINARY HAZARD ANALYSIS

BXM	**PHA Vivio AED**	Doc #	12341
		Revision	1.0
		Page	1 of 19

Table of Contents



BXM	PHA Vivio AED	Doc # 12341 Revision 1.0 Page 2 of 19

1 GENERAL

In this document, the words “System”, and “Vivio AED” are used synonymously.

1.1 Purpose

This document captures the Preliminary Hazard Analysis (PHA) of the Vivio AED. The purpose of the PHA is to identify the hazards, hazardous situations and events that could cause harm due to the use and operation of Vivio AED. The PHA is performed early in the design and development process when there is little information on design details of the System. The PHA can be used to make an early estimation on whether the device can be made to an acceptable level of safety, and also to predict the safety-critical aspect of the device design. This information can be used to guide the product development team and focus resources on the safety-critical areas.

The basis for the PHA is the contents of Customer Requirements Specification [CRS] and the Technical Concept [TC].

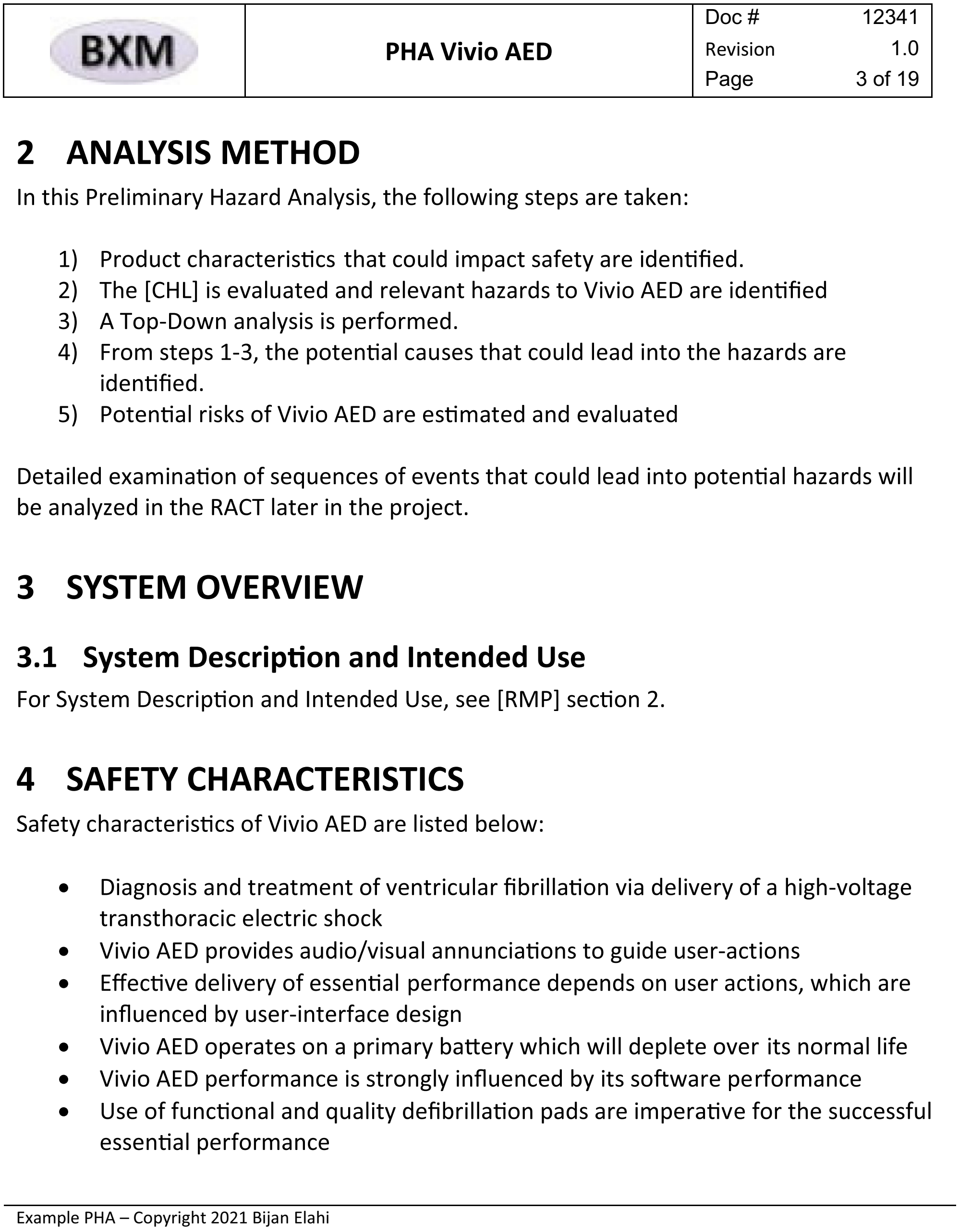
1.2 Scope

The scope of this analysis is the Vivio AED System. The defibrillation Pads, which are supplied by third party, are not analyzed for sequences of events leading to hazardous situations.
However, the interfaces between the Pads and Vivio, and the patient are within scope.

1.3 Definitions & Abbreviations

Term	Description
PHA	Preliminary Hazard Analysis
RACT	Risk Assessment and Control Table
FTA	Fault Tree Analysis
AED	Automatic External Defibrillator
IFU	Information for Use
VF	Ventricular Fibrillation

See [Glossary] for other definitions.



BXM	**PHA Vivio AED**	Doc #	12341
		Revision	1.0
		Page	3 of 19

2 ANALYSIS METHOD

In this Preliminary Hazard Analysis, the following steps are taken:

1) Product characteristics that could impact safety are identified.
2) The [CHL] is evaluated and relevant hazards to Vivio AED are identified
3) A Top-Down analysis is performed.
4) From steps 1-3, the potential causes that could lead into the hazards are identified.
5) Potential risks of Vivio AED are estimated and evaluated

Detailed examination of sequences of events that could lead into potential hazards will be analyzed in the RACT later in the project.

3 SYSTEM OVERVIEW

3.1 System Description and Intended Use

For System Description and Intended Use, see [RMP] section 2.

4 SAFETY CHARACTERISTICS

Safety characteristics of Vivio AED are listed below:

- Diagnosis and treatment of ventricular fibrillation via delivery of a high-voltage transthoracic electric shock
- Vivio AED provides audio/visual annunciations to guide user-actions
- Effective delivery of essential performance depends on user actions, which are influenced by user-interface design
- Vivio AED operates on a primary battery which will deplete over its normal life
- Vivio AED performance is strongly influenced by its software performance
- Use of functional and quality defibrillation pads are imperative for the successful essential performance

5 APPLICABLE HAZARDS FROM THE CLINICAL HAZARD LIST

The Clinical Hazards List [CHL] is a list of all known and foreseeable hazards that are related to the devices made by “Company”. For each hazard in [CHL] an analysis was performed to assess whether or not that hazard is relevant for the Vivio AED System. The result of this analysis is given in the table below.

ID	Hazard	Applicable?	Rationale
Haz.01	No therapy	Yes	Vivio AED delivers life-saving therapy
Haz.02	Inadequate therapy	Yes	Vivio AED delivers life-saving therapy
Haz.03	Inappropriate shock	Yes	Vivio AED may misdiagnose the heart rhythm and deliver an inappropriate shock
Haz.04	Hot surfaces	Yes	Vivio AED has potential to cause thermal burns
Haz.05	Sparks (pad to skin)	Yes	Improperly attached Pads could cause current jumping the airgap between pad and skin and cause sparks
Haz.06	Ionizing radiation	No	Vivio AED does not generate ionizing radiation
Haz.07	Sharps	Yes	Vivio AED has potential to present sharps
Haz.08	Pinch points	No	Vivio AED does not have potential for pinch points
Haz.09	Current leakage	Yes	High voltage is present within Vivio
Haz.10	Vibration	No	Vivio AED does not have the potential to cause vibration hazards
Haz.11	Delayed therapy	Yes	Vivio AED delivers life-saving therapy

6 TOP-DOWN ANALYSIS

A fault tree analysis of Vivio AED was performed to identify the potential pathways to System hazards. The top undesired event in each fault tree is one of the applicable hazards of Vivio AED. In each fault tree, probability numbers were assigned to the basic events and thereby the probability of the top undesired event was derived. (Note – in this PHA the basic event probabilities are hypothetical, and assigned only as examples.)

Some of the basic events were not further developed. In some cases, it is because an element is out of scope, e.g., the Pads. In other cases, it is not possible to develop them further until more is known about the design. In the final hazard analysis, the bottom-up Failure Modes and Effects Analyses (FMEA) will provide additional details that will be captured in the RACT.

Figure 1 depicts the fault tree for the “No Therapy” hazard.

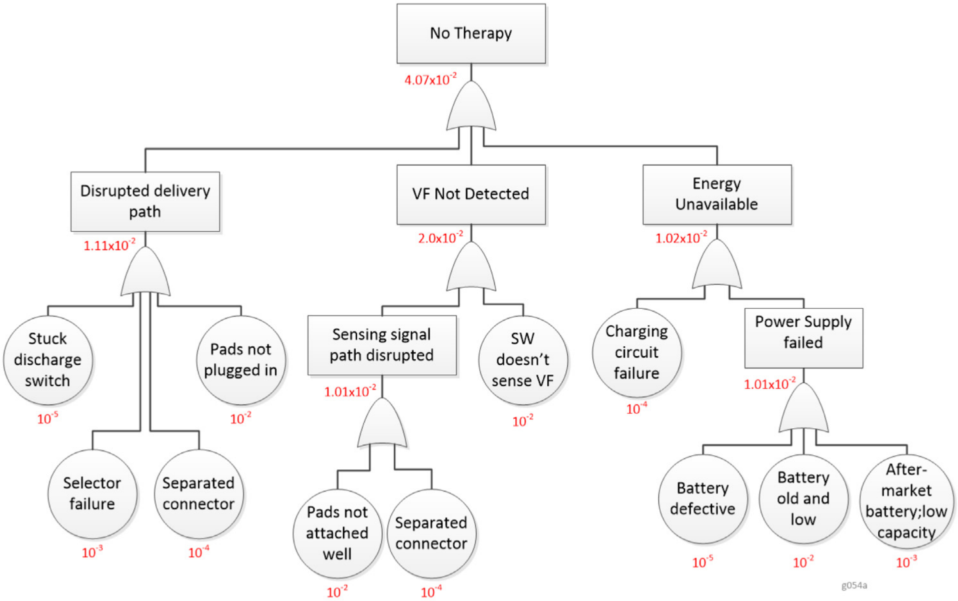


Figure 1- Vivio FTA - No Therapy

Figure 2 depicts the fault tree for the “Inadequate Therapy” hazard.

BXM	**PHA Vivio AED**	Doc #	12341
		Revision	1.0
		Page	6 of 19

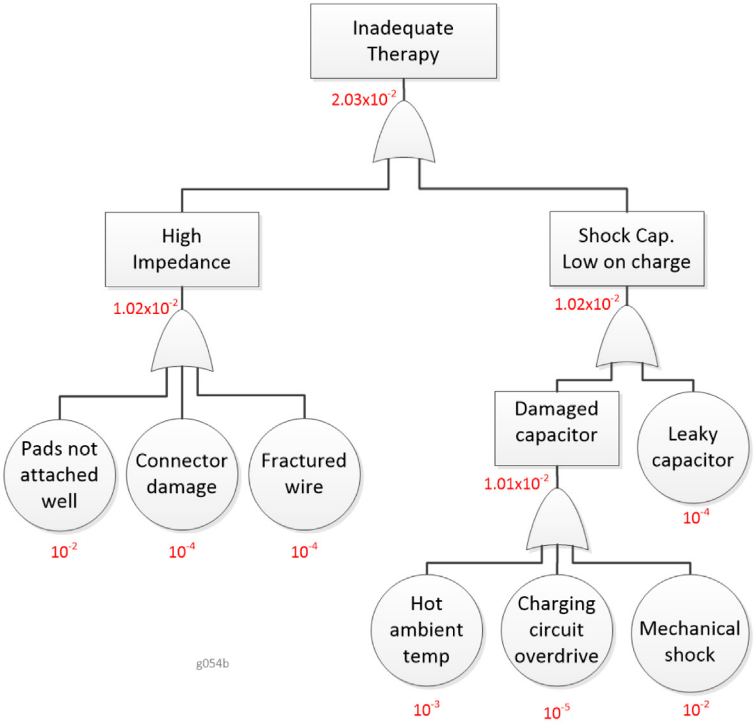


Figure 2- Vivio FTA - Inadequate Therapy

Figure 3 combines the two hazards of “Hot Surfaces” and “Sparks” into one fault tree.

BXM	**PHA Vivio AED**	Doc #	12341
		Revision	1.0
		Page	7 of 19

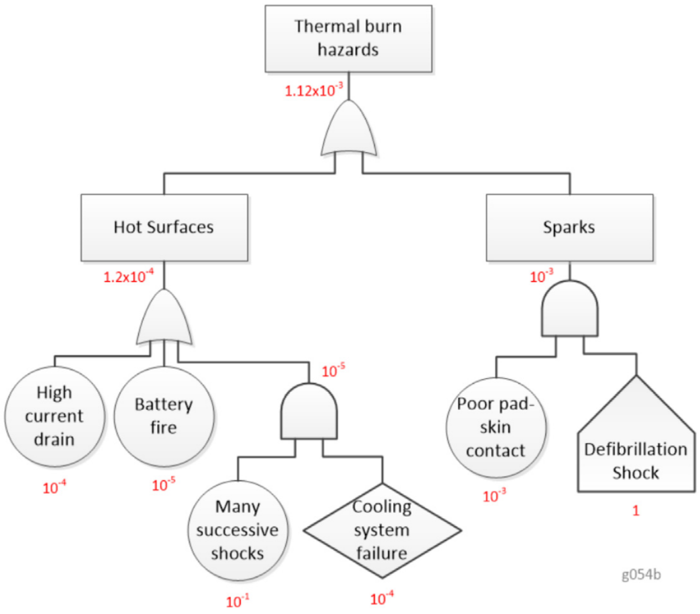


Figure 3 - Vivio FTA - Thermal Burn

BXM	**PHA Vivio AED**	Doc #	12341
		Revision	1.0
		Page	8 of 19

Figure 4 depicts the fault tree for “Sharps”.

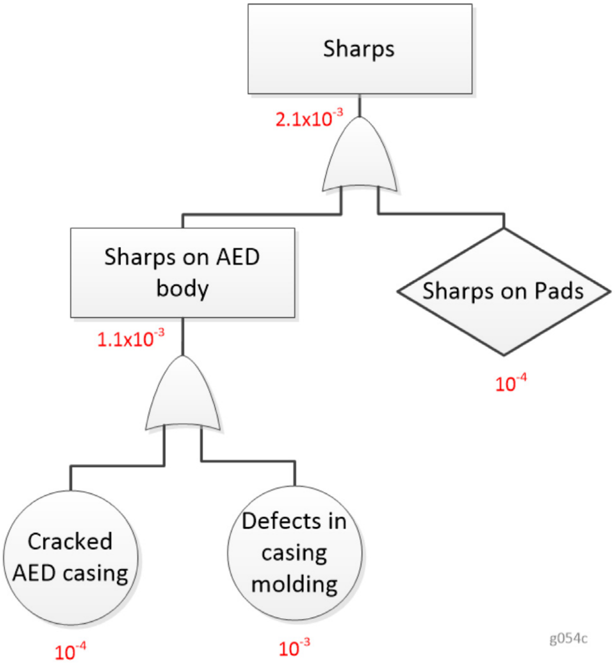


Figure 4 - Vivio FTA – Sharps

Figure 5 depicts the fault tree for “Inappropriate Shock” and **Figure 6** displays the fault tree for “Current Leakage”.

BXM	**PHA Vivio AED**	Doc #	12341
		Revision	1.0
		Page	9 of 19

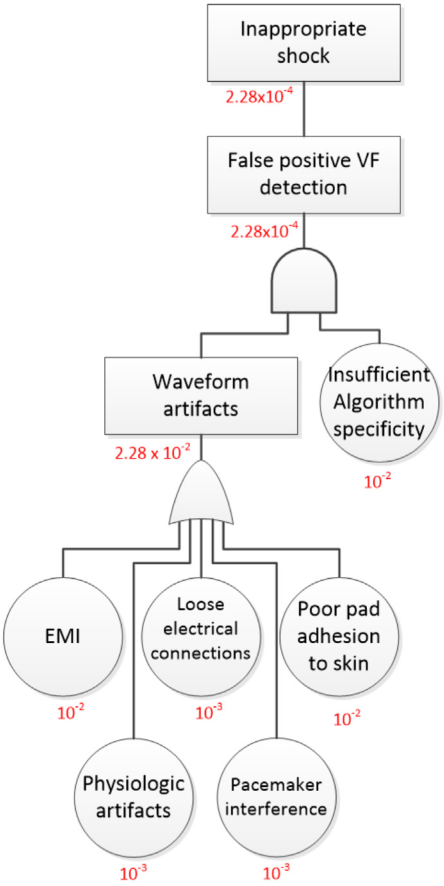


Figure 5 - Vivio FTA – Inappropriate shock

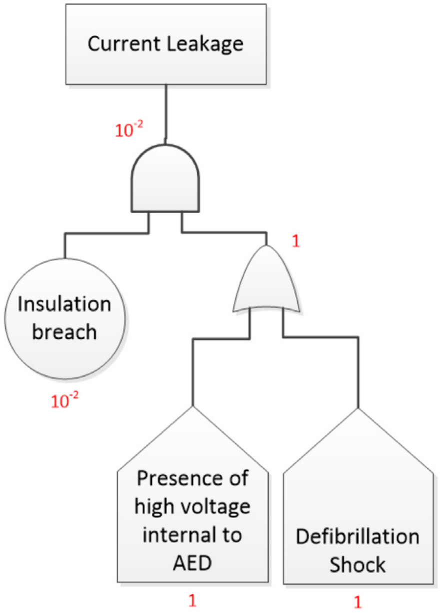


Figure 6 - Vivio FTA – Current Leakage

Figure 7 displays the fault tree for "Delayed Therapy"

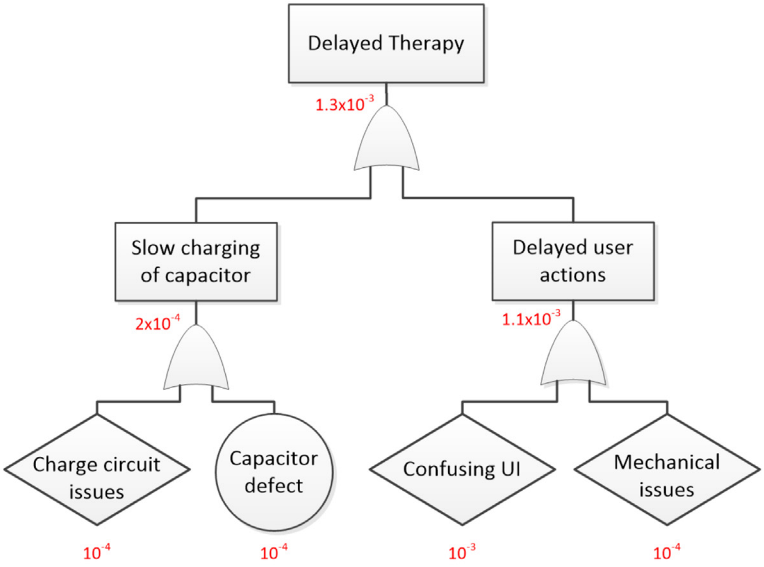


Figure 7 - Vivio FTA – Delayed Therapy

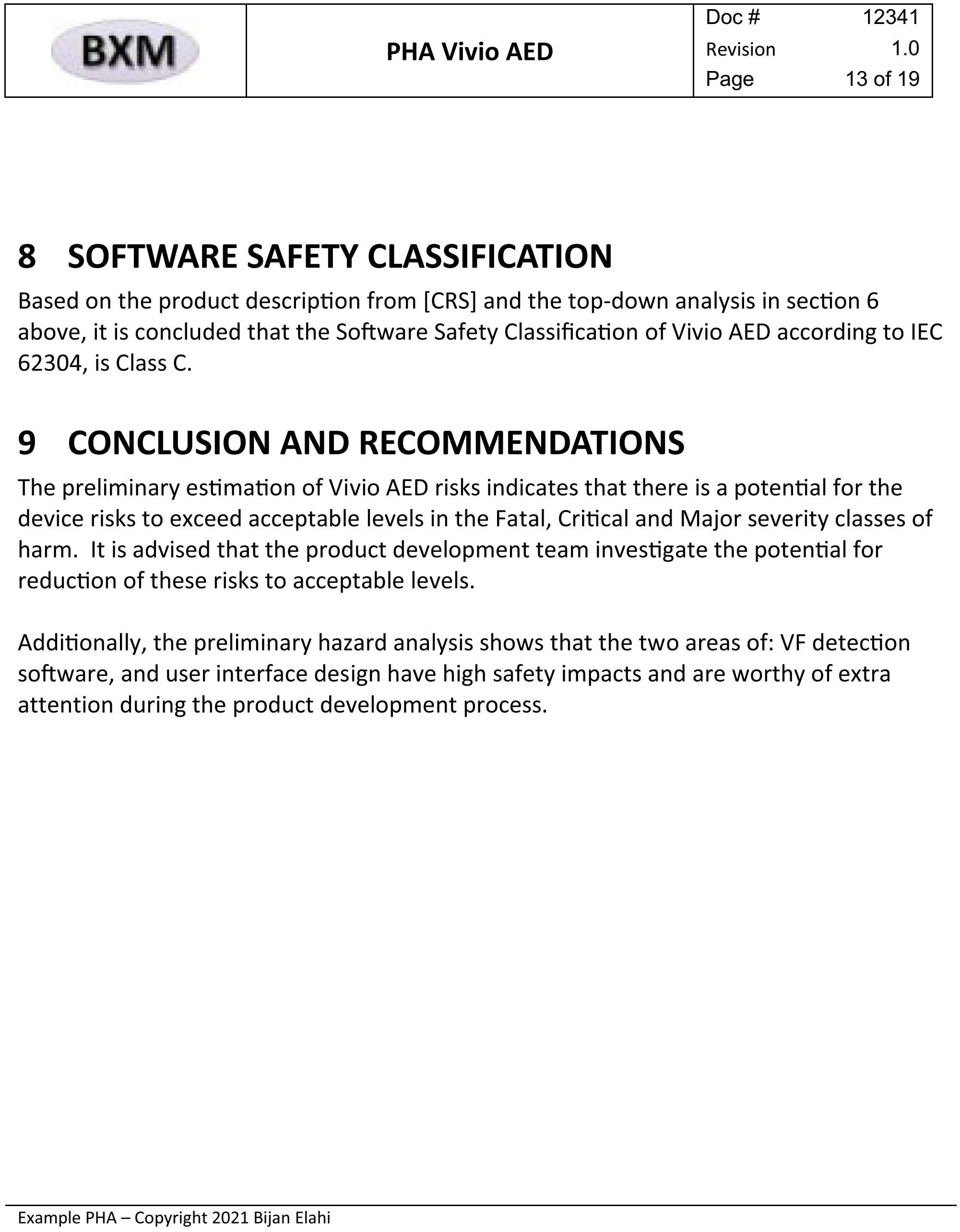
7 RISK ASSESSMENT AND CONTROL TABLE (RACT)

The PHA RACT captures the overall Vivio AED hazards, their predicted causes, their corresponding hazardous situations and harms. For each hazard, some risk controls are foreseen. At this early stage of product development, details of Vivio AED design are not yet available. This implies that the risk controls are not yet implemented. The P1 values are estimated to be inclusive of the foreseen risk controls. In other words, P1 is an estimate of the occurrence of the hazard, and exposure to that hazard while the foreseen risk controls are in place.

To calculate the risks, P2 numbers were looked up from the Harms Assessment List [HAL]. Each harm has five P2 estimates, one for each severity class of: Fatal, Critical, Major, Minor, and Negligible.

The residual risks for each Hazard, Hazardous Situation, and the overall residual risk for Vivio AED were computed. Risk acceptability criteria from the [RMP] were utilized to evaluate risks in each severity class.

These risk estimations will be updated in the final RACT and the Risk Management Report.



BXM	PHA Vivio AED	Doc # 12341 Revision 1.0 Page 13 of 19

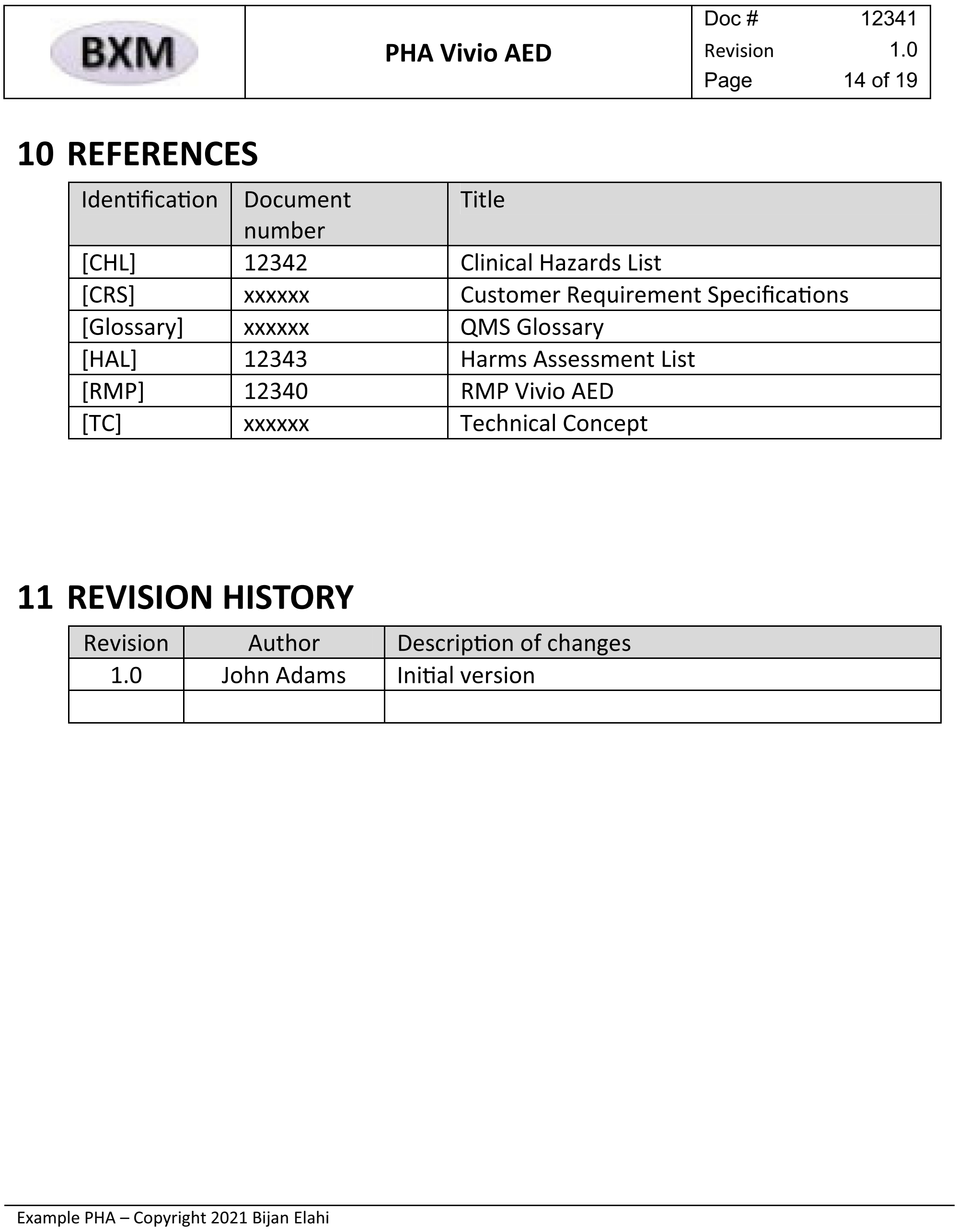
8 SOFTWARE SAFETY CLASSIFICATION

Based on the product description from [CRS] and the top-down analysis in section 6 above, it is concluded that the Software Safety Classification of Vivio AED according to IEC 62304, is Class C.

9 CONCLUSION AND RECOMMENDATIONS

The preliminary estimation of Vivio AED risks indicates that there is a potential for the device risks to exceed acceptable levels in the Fatal, Critical and Major severity classes of harm. It is advised that the product development team investigate the potential for reduction of these risks to acceptable levels.

Additionally, the preliminary hazard analysis shows that the two areas of: VF detection software, and user interface design have high safety impacts and are worthy of extra attention during the product development process.



BXM	**PHA Vivio AED**	Doc #	12341
		Revision	1.0
		Page	14 of 19

10 REFERENCES

Identification	Document number	Title
[CHL]	12342	Clinical Hazards List
[CRS]	xxxxxx	Customer Requirement Specifications
[Glossary]	xxxxxx	QMS Glossary
[HAL]	12343	Harms Assessment List
[RMP]	12340	RMP Vivio AED
[TC]	xxxxxx	Technical Concept

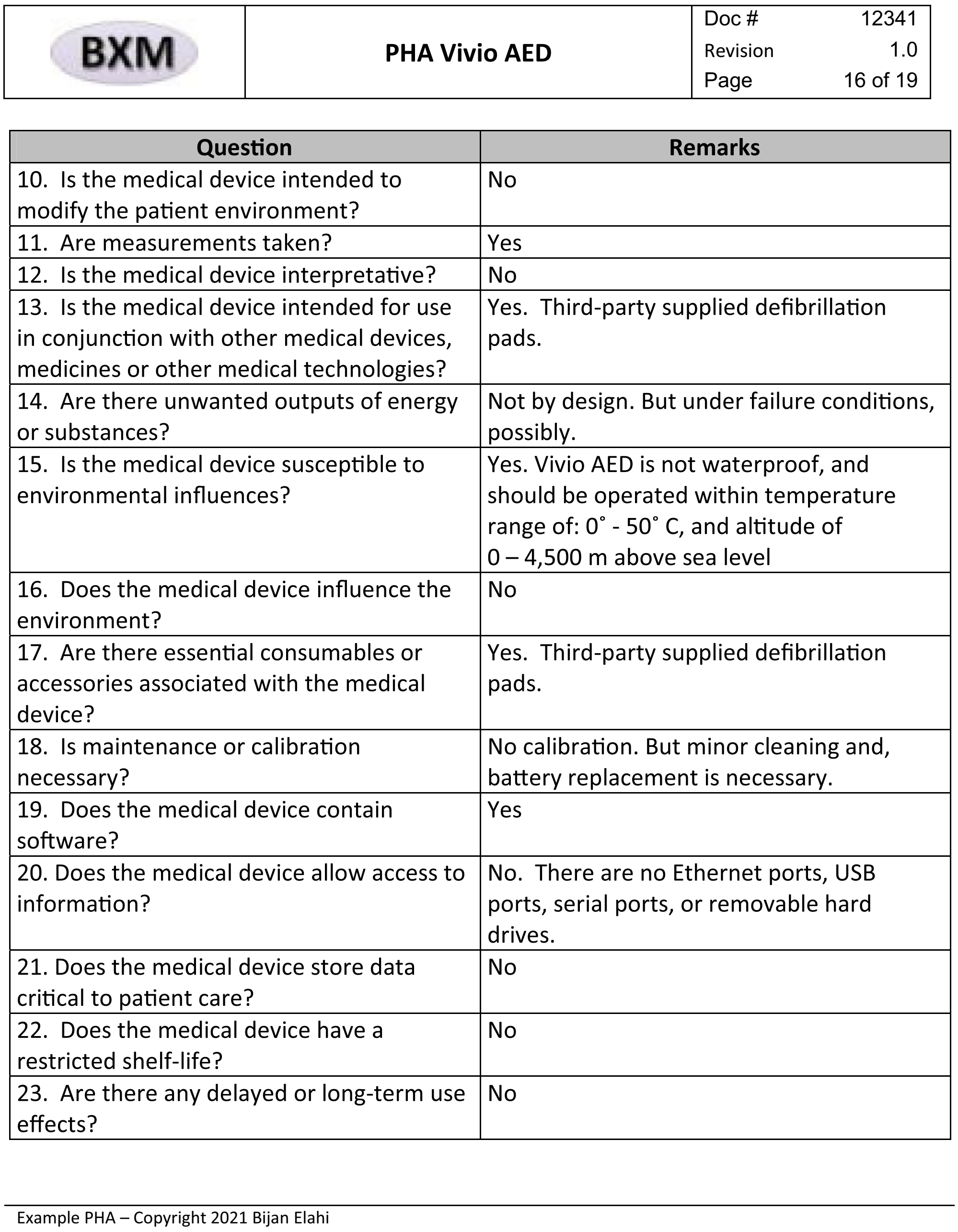
11 REVISION HISTORY

Revision	Author	Description of changes
1.0	John Adams	Initial version

APPENDIX A – PRODUCT CHARACTERIZATION

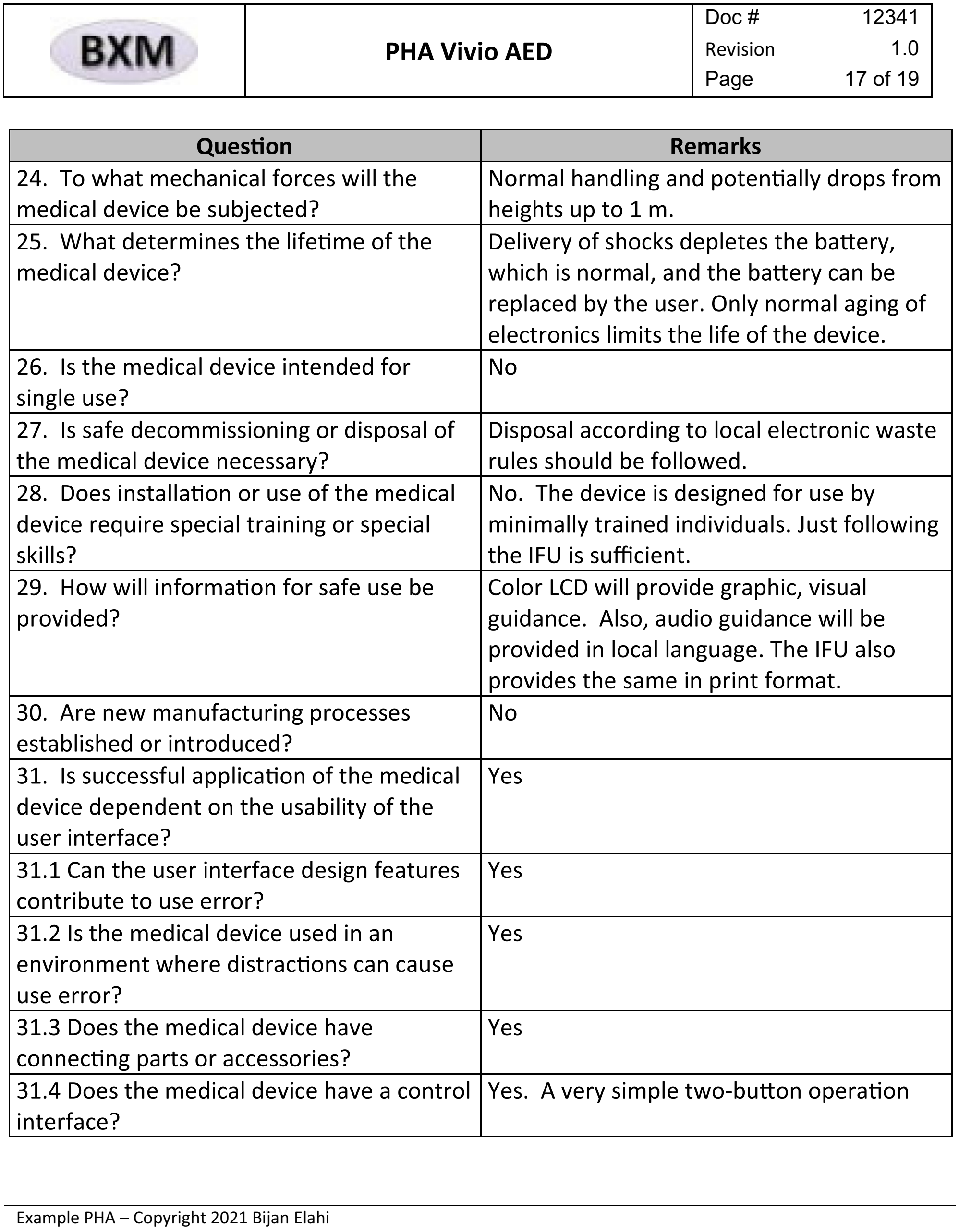
In this appendix, the results of evaluation of Vivio AED with respect to safety characteristics are captured. The questions in Annex A of ISO/TR 24971:2020 were used to guide this evaluation.

Question	Remarks
1. What is the intended use and how is the medical device to be used?	AED. Intended for use by minimally trained individuals on adults and children over 25 kg
2. Is the medical device intended to be implanted?	No
3. Is the medical device intended to be in contact with the patient or other persons?	The defibrillation pads of the Vivio AED system do contact the patient's skin surface
4. What materials or components are utilized in the medical device or are used with, or are in contact with, the medical device?	Vivio AED does not contact the patient. The user handles the AED and the pads. The pads contact the patient skin via medical grade conductive adhesive.
5. Is energy delivered to or extracted from the patient?	Yes
6. Are substances delivered to or extracted from the patient?	No
7. Are biological materials processed by the medical device for subsequent re-use, transfusion or transplantation?	No
8. Is the medical device supplied sterile or intended to be sterilized by the user, or are other microbiological controls applicable?	No
9. Is the medical device intended to be routinely cleaned and disinfected by the user?	Minor cleaning with damp cloth is sufficient



BXM	**PHA Vivio AED**	Doc #	12341
		Revision	1.0
		Page	16 of 19

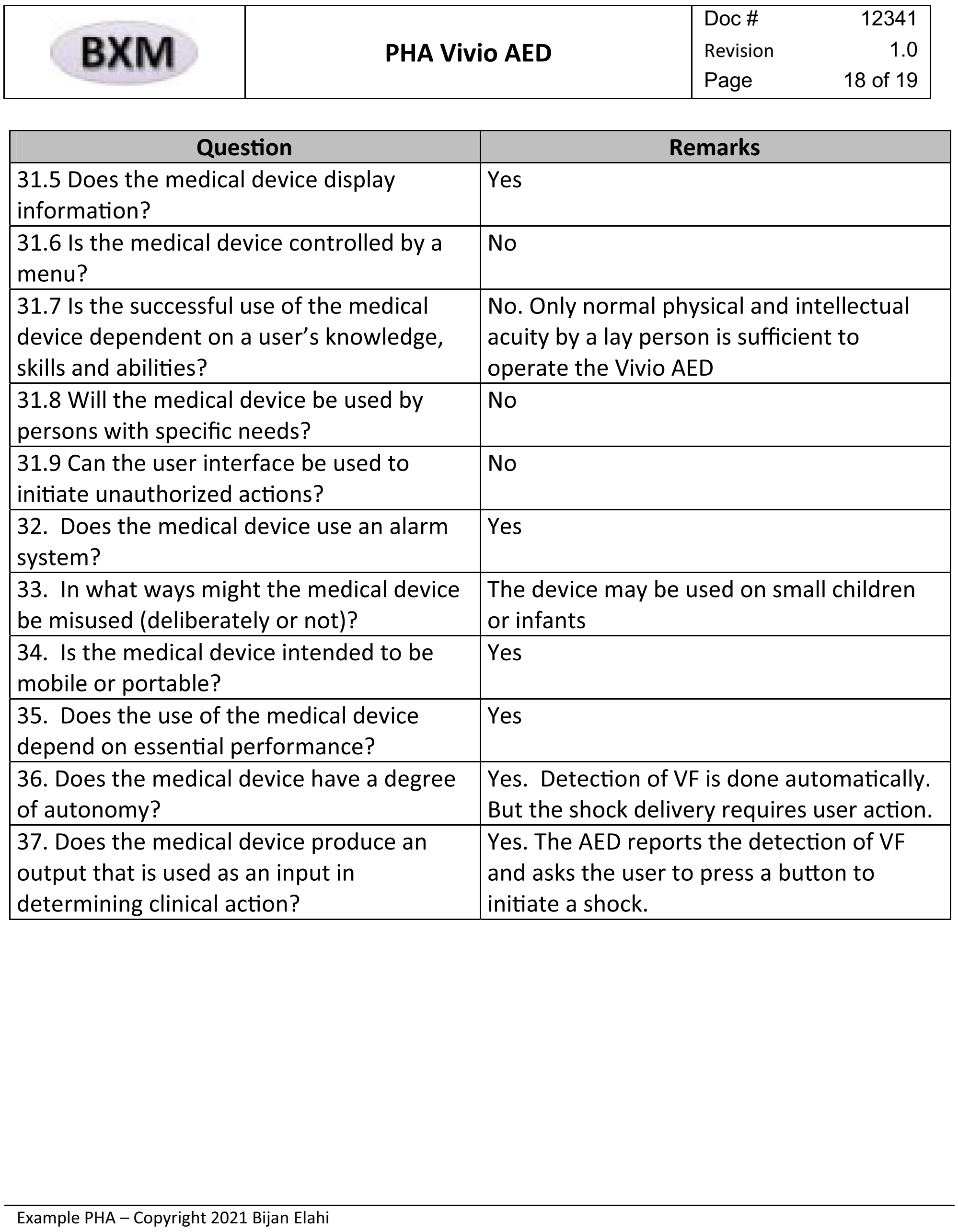
Question	Remarks
10. Is the medical device intended to modify the patient environment?	No
11. Are measurements taken?	Yes
12. Is the medical device interpretative?	No
13. Is the medical device intended for use in conjunction with other medical devices, medicines or other medical technologies?	Yes. Third-party supplied defibrillation pads.
14. Are there unwanted outputs of energy or substances?	Not by design. But under failure conditions, possibly.
15. Is the medical device susceptible to environmental influences?	Yes. Vivio AED is not waterproof, and should be operated within temperature range of: 0˚ - 50˚ C, and altitude of 0 – 4,500 m above sea level
16. Does the medical device influence the environment?	No
17. Are there essential consumables or accessories associated with the medical device?	Yes. Third-party supplied defibrillation pads.
18. Is maintenance or calibration necessary?	No calibration. But minor cleaning and, battery replacement is necessary.
19. Does the medical device contain software?	Yes
20. Does the medical device allow access to information?	No. There are no Ethernet ports, USB ports, serial ports, or removable hard drives.
21. Does the medical device store data critical to patient care?	No
22. Does the medical device have a restricted shelf-life?	No
23. Are there any delayed or long-term use effects?	No



BXM	**PHA Vivio AED**	Doc #	12341
		Revision	1.0
		Page	17 of 19

Question	Remarks
24. To what mechanical forces will the medical device be subjected?	Normal handling and potentially drops from heights up to 1 m.
25. What determines the lifetime of the medical device?	Delivery of shocks depletes the battery, which is normal, and the battery can be replaced by the user. Only normal aging of electronics limits the life of the device.
26. Is the medical device intended for single use?	No
27. Is safe decommissioning or disposal of the medical device necessary?	Disposal according to local electronic waste rules should be followed.
28. Does installation or use of the medical device require special training or special skills?	No. The device is designed for use by minimally trained individuals. Just following the IFU is sufficient.
29. How will information for safe use be provided?	Color LCD will provide graphic, visual guidance. Also, audio guidance will be provided in local language. The IFU also provides the same in print format.
30. Are new manufacturing processes established or introduced?	No
31. Is successful application of the medical device dependent on the usability of the user interface?	Yes
31.1 Can the user interface design features contribute to use error?	Yes
31.2 Is the medical device used in an environment where distractions can cause use error?	Yes
31.3 Does the medical device have connecting parts or accessories?	Yes
31.4 Does the medical device have a control interface?	Yes. A very simple two-button operation

Example PHA – Copyright 2021 Bijan Elahi



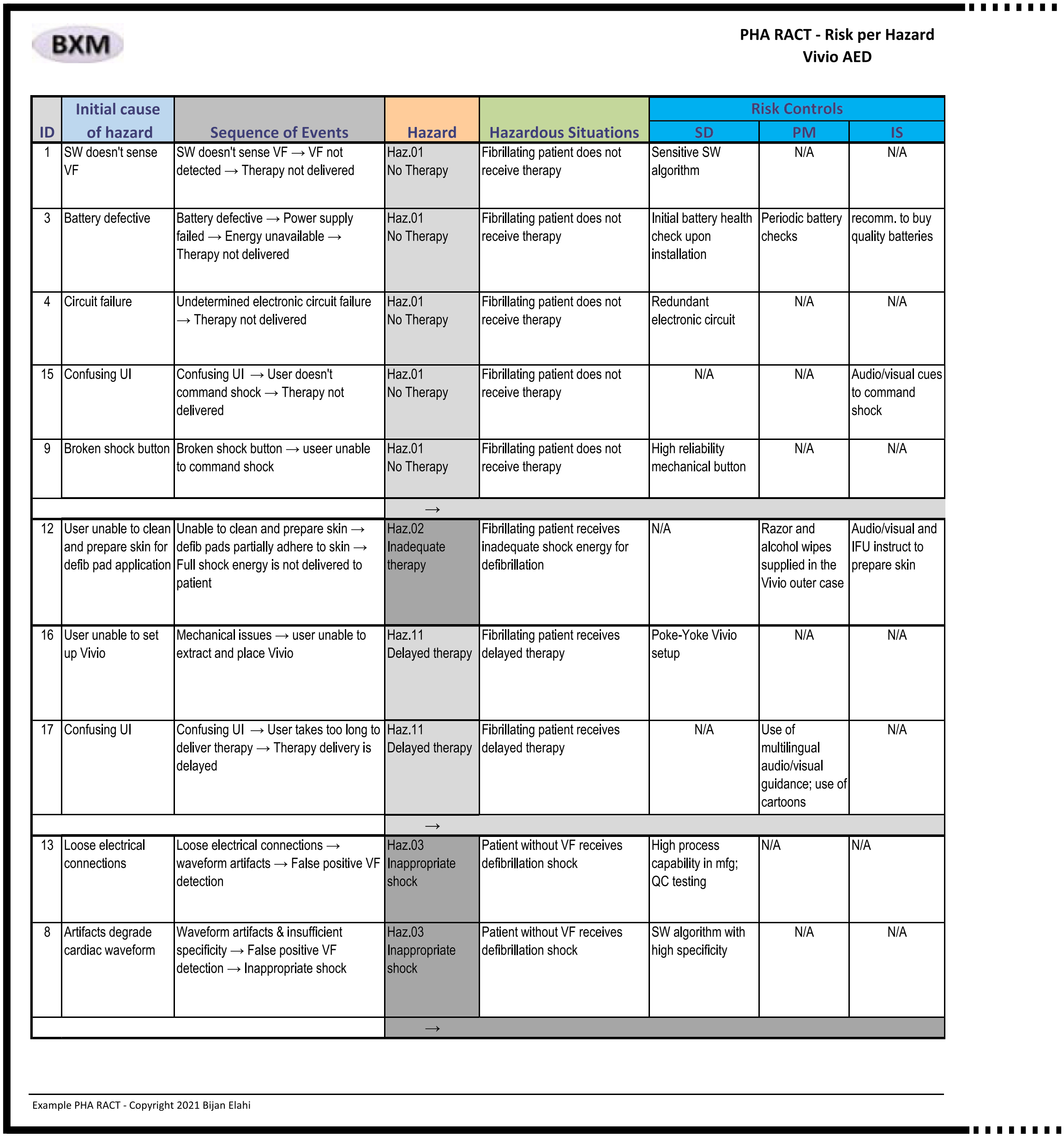
BXM	PHA Vivio AED	Doc #	12341
		Revision	1.0
		Page	18 of 19

Question	Remarks
31.5 Does the medical device display information?	Yes
31.6 Is the medical device controlled by a menu?	No
31.7 Is the successful use of the medical device dependent on a user's knowledge, skills and abilities?	No. Only normal physical and intellectual acuity by a lay person is sufficient to operate the Vivio AED
31.8 Will the medical device be used by persons with specific needs?	No
31.9 Can the user interface be used to initiate unauthorized actions?	No
32. Does the medical device use an alarm system?	Yes
33. In what ways might the medical device be misused (deliberately or not)?	The device may be used on small children or infants
34. Is the medical device intended to be mobile or portable?	Yes
35. Does the use of the medical device depend on essential performance?	Yes
36. Does the medical device have a degree of autonomy?	Yes. Detection of VF is done automatically. But the shock delivery requires user action.
37. Does the medical device produce an output that is used as an input in determining clinical action?	Yes. The AED reports the detection of VF and asks the user to press a button to initiate a shock.

BXM	**PHA Vivio AED**	Doc #	12341
		Revision	1.0
		Page	19 of 19

APPENDIX B – PHA RACT

For the purposes of this example PHA, a partial RACT is presented in the following pages.

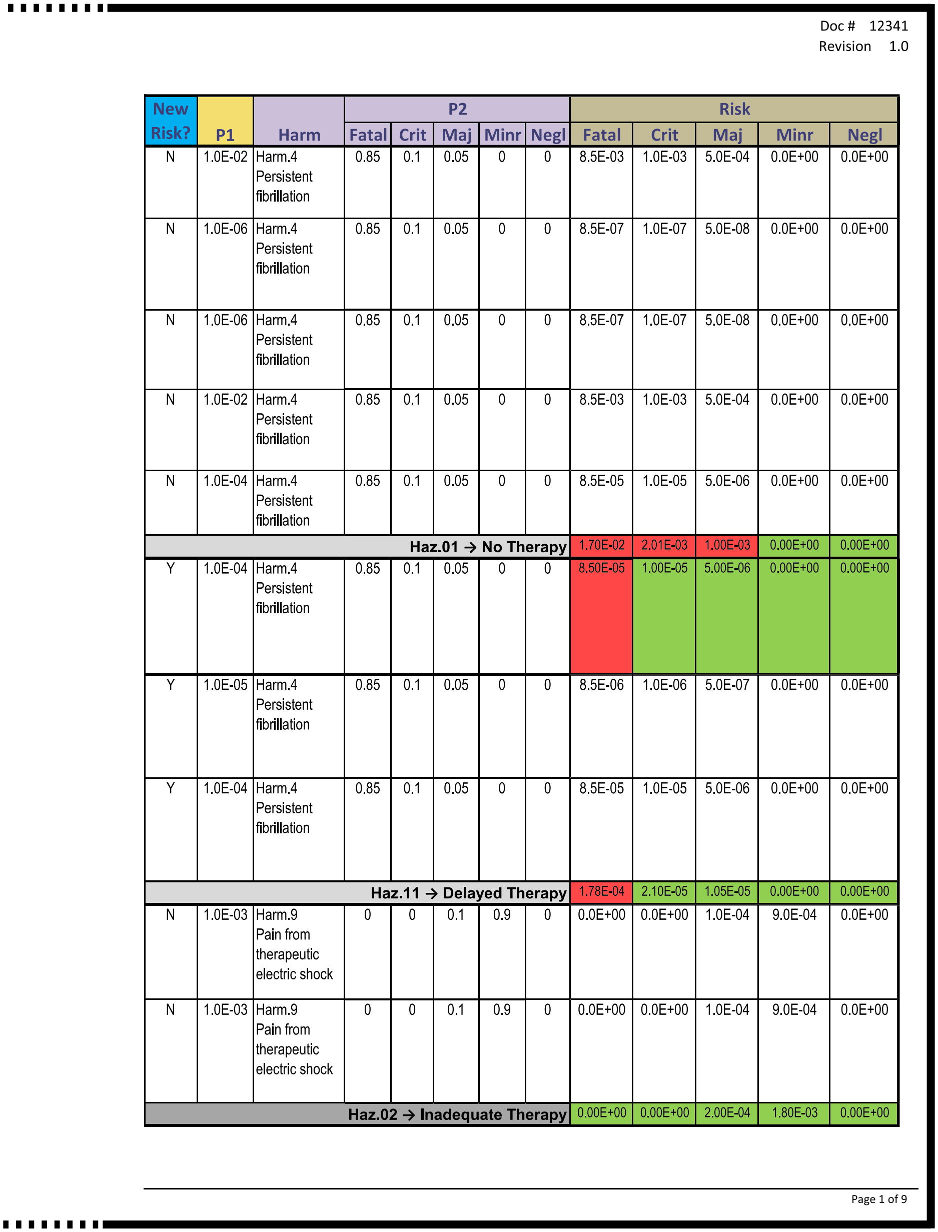


BXM

PHA RACT - Risk per Hazard
Vivio AED

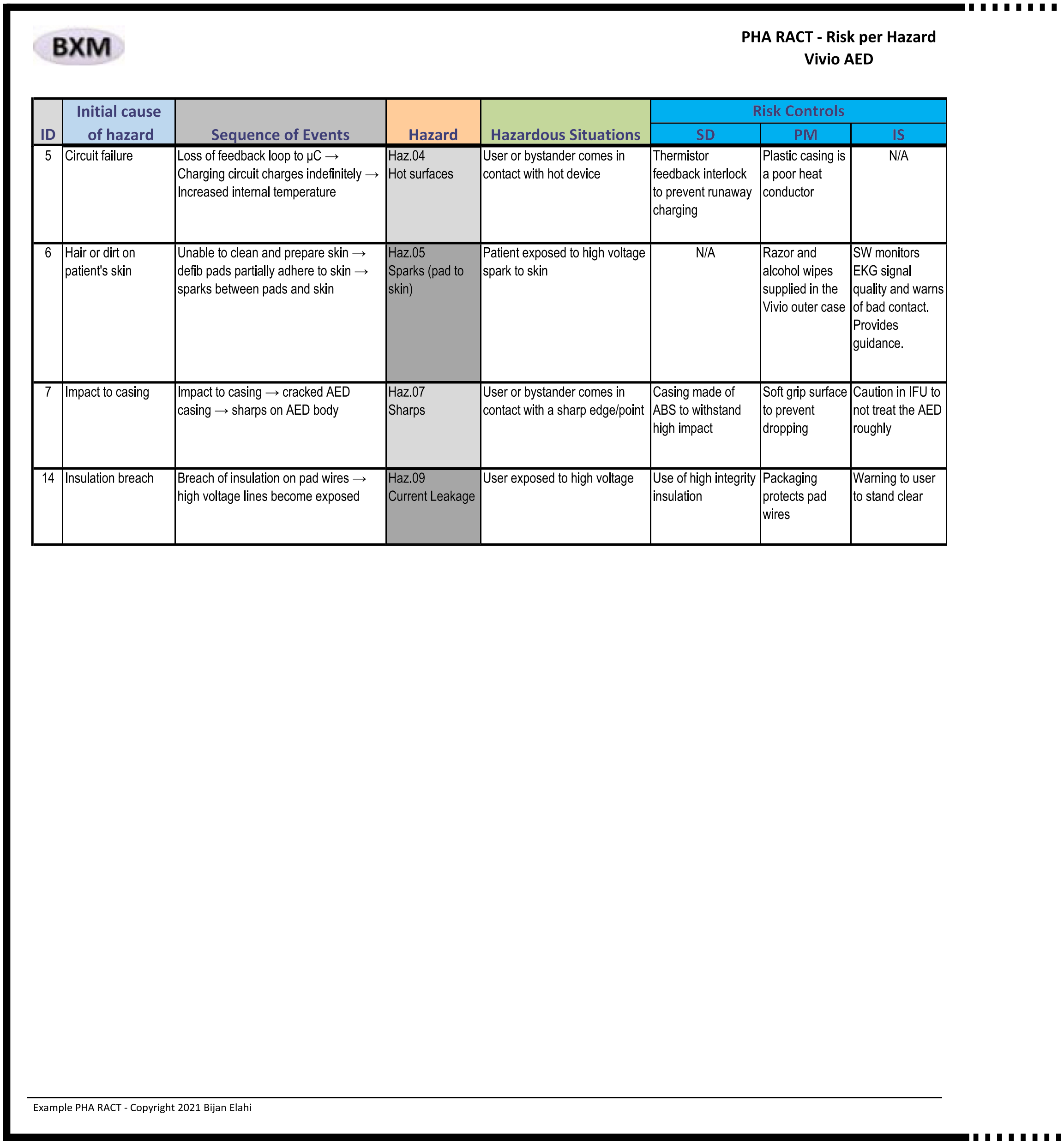
	Initial cause				Risk Controls		
ID	of hazard	Sequence of Events	Hazard	Hazardous Situations	SD	PM	IS
1	SW doesn't sense VF	SW doesn't sense VF → VF not detected → Therapy not delivered	Haz.01 No Therapy	Fibrillating patient does not receive therapy	Sensitive SW algorithm	N/A	N/A
3	Battery defective	Battery defective → Power supply failed → Energy unavailable → Therapy not delivered	Haz.01 No Therapy	Fibrillating patient does not receive therapy	Initial battery health check upon installation	Periodic battery checks	recomm. to buy quality batteries
4	Circuit failure	Undetermined electronic circuit failure → Therapy not delivered	Haz.01 No Therapy	Fibrillating patient does not receive therapy	Redundant electronic circuit	N/A	N/A
15	Confusing UI	Confusing UI → User doesn't command shock → Therapy not delivered	Haz.01 No Therapy	Fibrillating patient does not receive therapy	N/A	N/A	Audio/visual cues to command shock
9	Broken shock button	Broken shock button → useer unable to command shock	Haz.01 No Therapy	Fibrillating patient does not receive therapy	High reliability mechanical button	N/A	N/A
			→				
12	User unable to clean and prepare skin for defib pad application	Unable to clean and prepare skin → defib pads partially adhere to skin → Full shock energy is not delivered to patient	Haz.02 Inadequate therapy	Fibrillating patient receives inadequate shock energy for defibrillation	N/A	Razor and alcohol wipes supplied in the Vivio outer case	Audio/visual and IFU instruct to prepare skin
16	User unable to set up Vivio	Mechanical issues → user unable to extract and place Vivio	Haz.11 Delayed therapy	Fibrillating patient receives delayed therapy	Poke-Yoke Vivio setup	N/A	N/A
17	Confusing UI	Confusing UI → User takes too long to deliver therapy → Therapy delivery is delayed	Haz.11 Delayed therapy	Fibrillating patient receives delayed therapy	N/A	Use of multilingual audio/visual guidance; use of cartoons	N/A
			→				
13	Loose electrical connections	Loose electrical connections → waveform artifacts → False positive VF detection	Haz.03 Inappropriate shock	Patient without VF receives defibrillation shock	High process capability in mfg; QC testing	N/A	N/A
8	Artifacts degrade cardiac waveform	Waveform artifacts & insufficient specificity → False positive VF detection → Inappropriate shock	Haz.03 Inappropriate shock	Patient without VF receives defibrillation shock	SW algorithm with high specificity	N/A	N/A
			→				

Example PHA RACT - Copyright 2021 Bijan Elahi



Doc # 12341
Revision 1.0

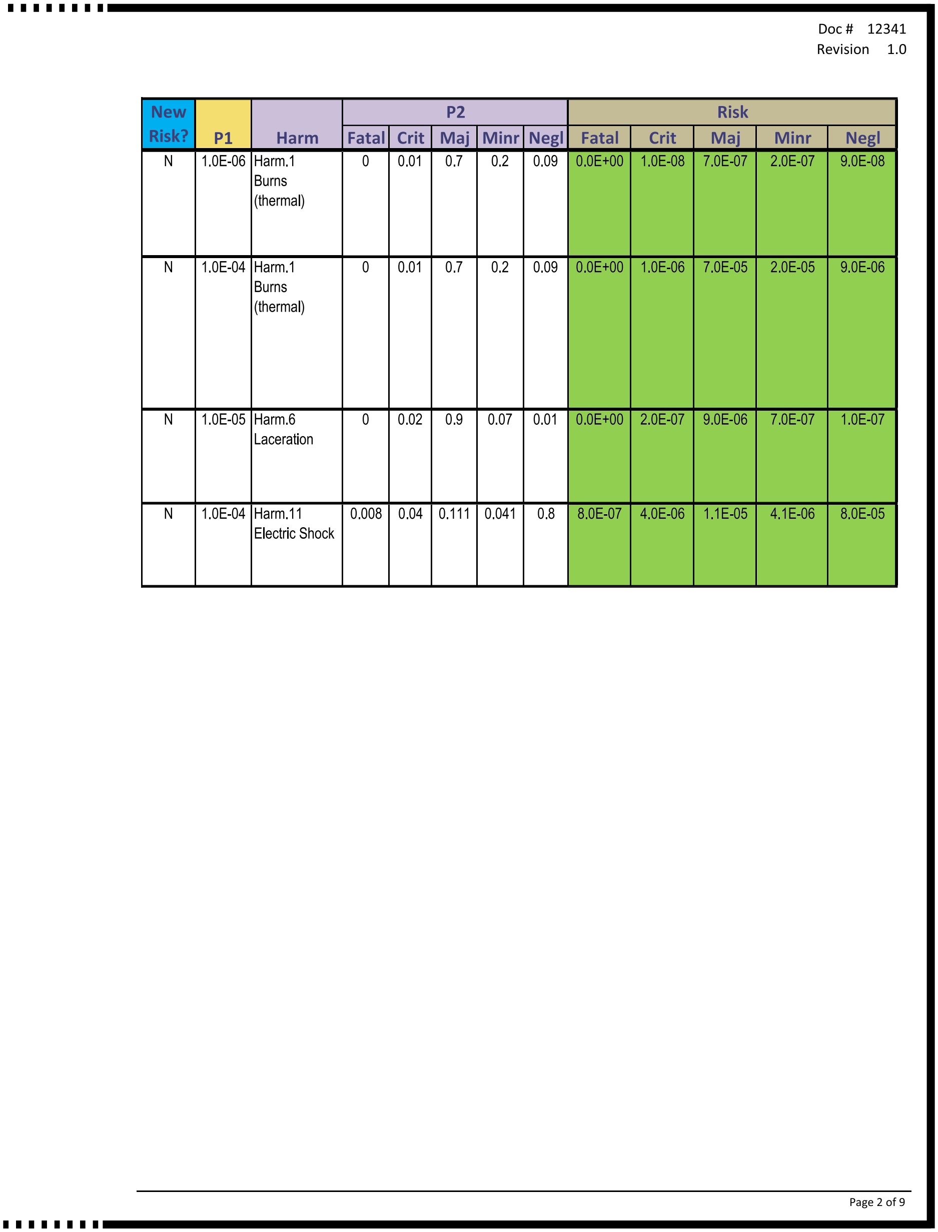
New Risk?	P1	Harm	P2					Risk				
			Fatal	Crit	Maj	Minr	Negl	Fatal	Crit	Maj	Minr	Negl
N	1.0E-02	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-03	1.0E-03	5.0E-04	0.0E+00	0.0E+00
N	1.0E-06	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-07	1.0E-07	5.0E-08	0.0E+00	0.0E+00
N	1.0E-06	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-07	1.0E-07	5.0E-08	0.0E+00	0.0E+00
N	1.0E-02	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-03	1.0E-03	5.0E-04	0.0E+00	0.0E+00
N	1.0E-04	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-05	1.0E-05	5.0E-06	0.0E+00	0.0E+00
Haz.01 → No Therapy								1.70E-02	2.01E-03	1.00E-03	0.00E+00	0.00E+00
Y	1.0E-04	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.50E-05	1.00E-05	5.00E-06	0.00E+00	0.00E+00
Y	1.0E-05	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-06	1.0E-06	5.0E-07	0.0E+00	0.0E+00
Y	1.0E-04	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-05	1.0E-05	5.0E-06	0.0E+00	0.0E+00
Haz.11 → Delayed Therapy								1.78E-04	2.10E-05	1.05E-05	0.00E+00	0.00E+00
N	1.0E-03	Harm.9 Pain from therapeutic electric shock	0	0	0.1	0.9	0	0.0E+00	0.0E+00	1.0E-04	9.0E-04	0.0E+00
N	1.0E-03	Harm.9 Pain from therapeutic electric shock	0	0	0.1	0.9	0	0.0E+00	0.0E+00	1.0E-04	9.0E-04	0.0E+00
Haz.02 → Inadequate Therapy								0.00E+00	0.00E+00	2.00E-04	1.80E-03	0.00E+00



BXM

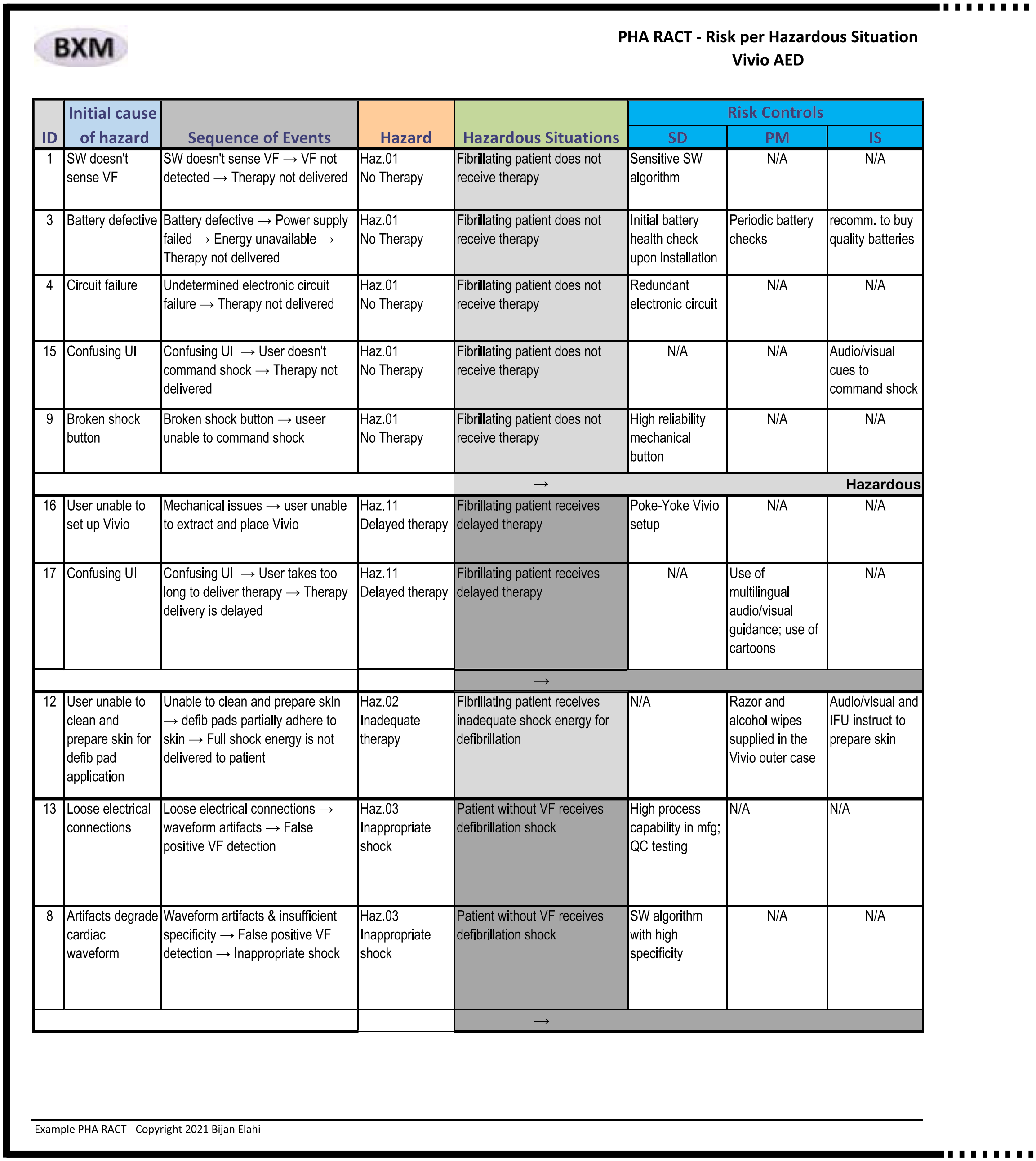
PHA RACT - Risk per Hazard
Vivio AED

ID	Initial cause of hazard	Sequence of Events	Hazard	Hazardous Situations	Risk Controls		
					SD	PM	IS
5	Circuit failure	Loss of feedback loop to μC → Charging circuit charges indefinitely → Increased internal temperature	Haz.04 Hot surfaces	User or bystander comes in contact with hot device	Thermistor feedback interlock to prevent runaway charging	Plastic casing is a poor heat conductor	N/A
6	Hair or dirt on patient's skin	Unable to clean and prepare skin → defib pads partially adhere to skin → sparks between pads and skin	Haz.05 Sparks (pad to skin)	Patient exposed to high voltage spark to skin	N/A	Razor and alcohol wipes supplied in the Vivio outer case	SW monitors EKG signal quality and warns of bad contact. Provides guidance.
7	Impact to casing	Impact to casing → cracked AED casing → sharps on AED body	Haz.07 Sharps	User or bystander comes in contact with a sharp edge/point	Casing made of ABS to withstand high impact	Soft grip surface to prevent dropping	Caution in IFU to not treat the AED roughly
14	Insulation breach	Breach of insulation on pad wires → high voltage lines become exposed	Haz.09 Current Leakage	User exposed to high voltage	Use of high integrity insulation	Packaging protects pad wires	Warning to user to stand clear



Doc # 12341
Revision 1.0

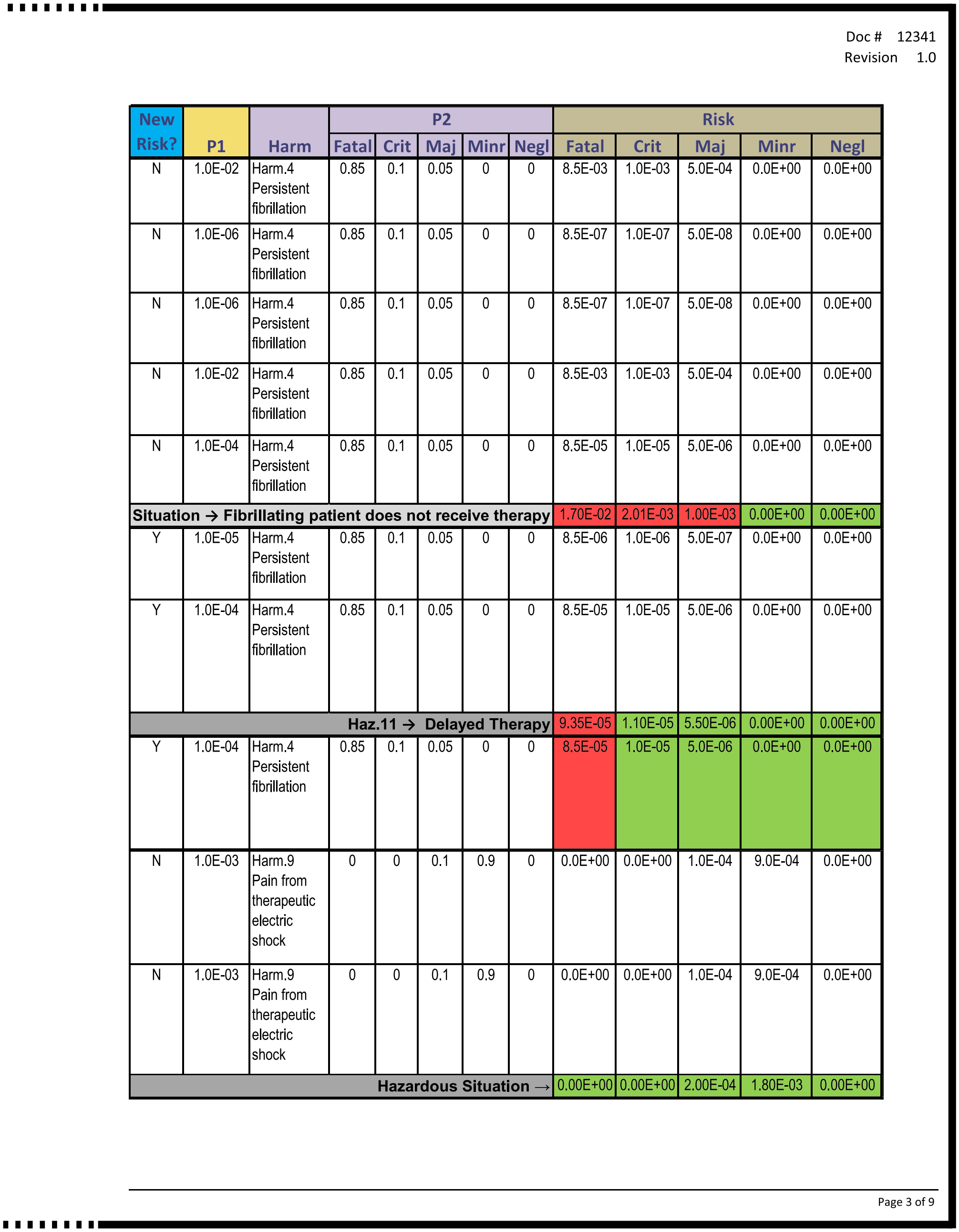
New Risk?	P1	Harm	P2					Risk				
			Fatal	Crit	Maj	Minr	Negl	Fatal	Crit	Maj	Minr	Negl
N	1.0E-06	Harm.1 Burns (thermal)	0	0.01	0.7	0.2	0.09	0.0E+00	1.0E-08	7.0E-07	2.0E-07	9.0E-08
N	1.0E-04	Harm.1 Burns (thermal)	0	0.01	0.7	0.2	0.09	0.0E+00	1.0E-06	7.0E-05	2.0E-05	9.0E-06
N	1.0E-05	Harm.6 Laceration	0	0.02	0.9	0.07	0.01	0.0E+00	2.0E-07	9.0E-06	7.0E-07	1.0E-07
N	1.0E-04	Harm.11 Electric Shock	0.008	0.04	0.111	0.041	0.8	8.0E-07	4.0E-06	1.1E-05	4.1E-06	8.0E-05



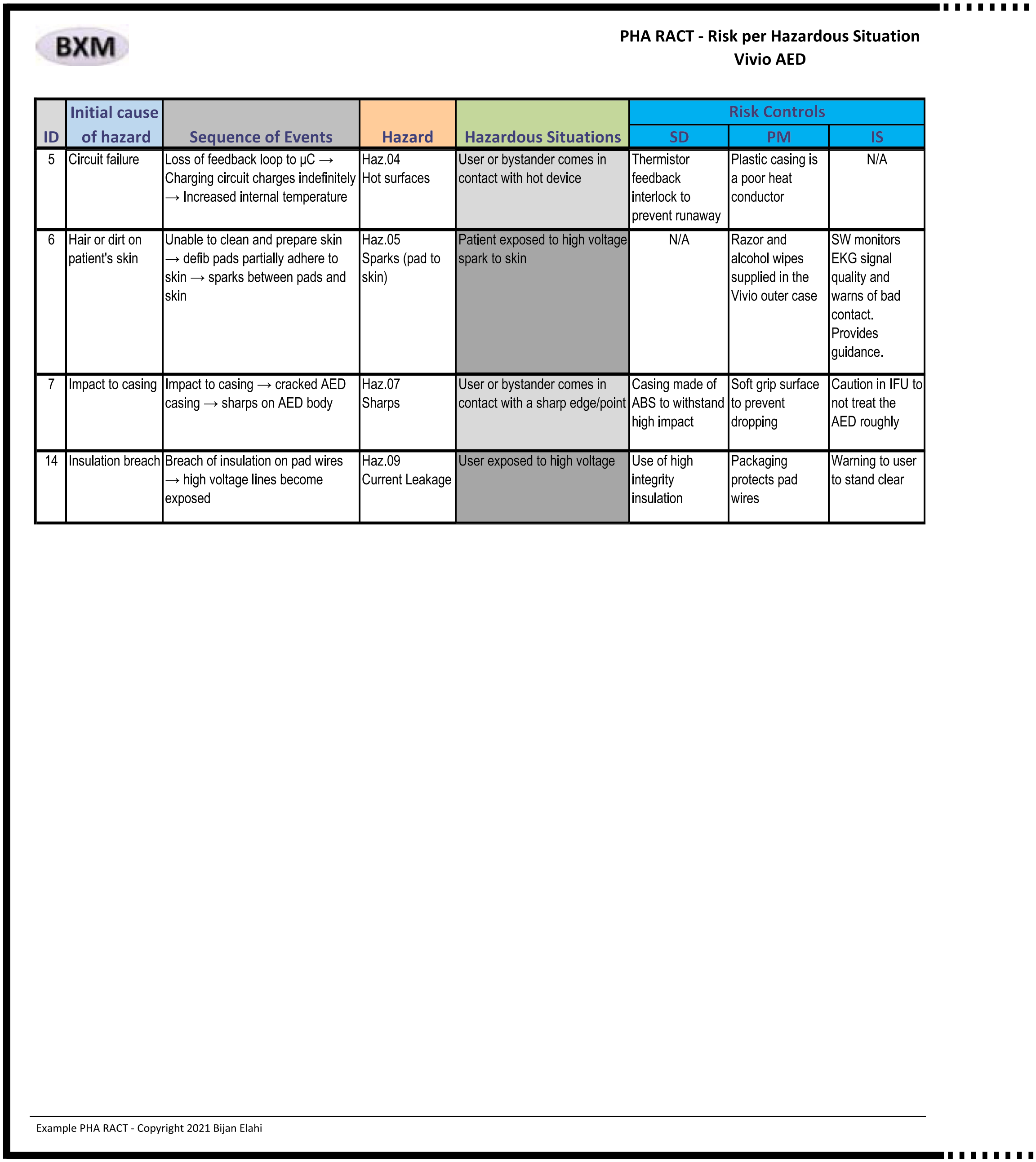
PHA RACT - Risk per Hazardous Situation
Vivio AED

ID	Initial cause of hazard	Sequence of Events	Hazard	Hazardous Situations	Risk Controls		
					SD	PM	IS
1	SW doesn't sense VF	SW doesn't sense VF → VF not detected → Therapy not delivered	Haz.01 No Therapy	Fibrillating patient does not receive therapy	Sensitive SW algorithm	N/A	N/A
3	Battery defective	Battery defective → Power supply failed → Energy unavailable → Therapy not delivered	Haz.01 No Therapy	Fibrillating patient does not receive therapy	Initial battery health check upon installation	Periodic battery checks	recomm. to buy quality batteries
4	Circuit failure	Undetermined electronic circuit failure → Therapy not delivered	Haz.01 No Therapy	Fibrillating patient does not receive therapy	Redundant electronic circuit	N/A	N/A
15	Confusing UI	Confusing UI → User doesn't command shock → Therapy not delivered	Haz.01 No Therapy	Fibrillating patient does not receive therapy	N/A	N/A	Audio/visual cues to command shock
9	Broken shock button	Broken shock button → useer unable to command shock	Haz.01 No Therapy	Fibrillating patient does not receive therapy	High reliability mechanical button	N/A	N/A
				→			Hazardous
16	User unable to set up Vivio	Mechanical issues → user unable to extract and place Vivio	Haz.11 Delayed therapy	Fibrillating patient receives delayed therapy	Poke-Yoke Vivio setup	N/A	N/A
17	Confusing UI	Confusing UI → User takes too long to deliver therapy → Therapy delivery is delayed	Haz.11 Delayed therapy	Fibrillating patient receives delayed therapy	N/A	Use of multilingual audio/visual guidance; use of cartoons	N/A
				→			
12	User unable to clean and prepare skin for defib pad application	Unable to clean and prepare skin → defib pads partially adhere to skin → Full shock energy is not delivered to patient	Haz.02 Inadequate therapy	Fibrillating patient receives inadequate shock energy for defibrillation	N/A	Razor and alcohol wipes supplied in the Vivio outer case	Audio/visual and IFU instruct to prepare skin
13	Loose electrical connections	Loose electrical connections → waveform artifacts → False positive VF detection	Haz.03 Inappropriate shock	Patient without VF receives defibrillation shock	High process capability in mfg; QC testing	N/A	N/A
8	Artifacts degrade cardiac waveform	Waveform artifacts & insufficient specificity → False positive VF detection → Inappropriate shock	Haz.03 Inappropriate shock	Patient without VF receives defibrillation shock	SW algorithm with high specificity	N/A	N/A
				→			

Example PHA RACT - Copyright 2021 Bijan Elahi



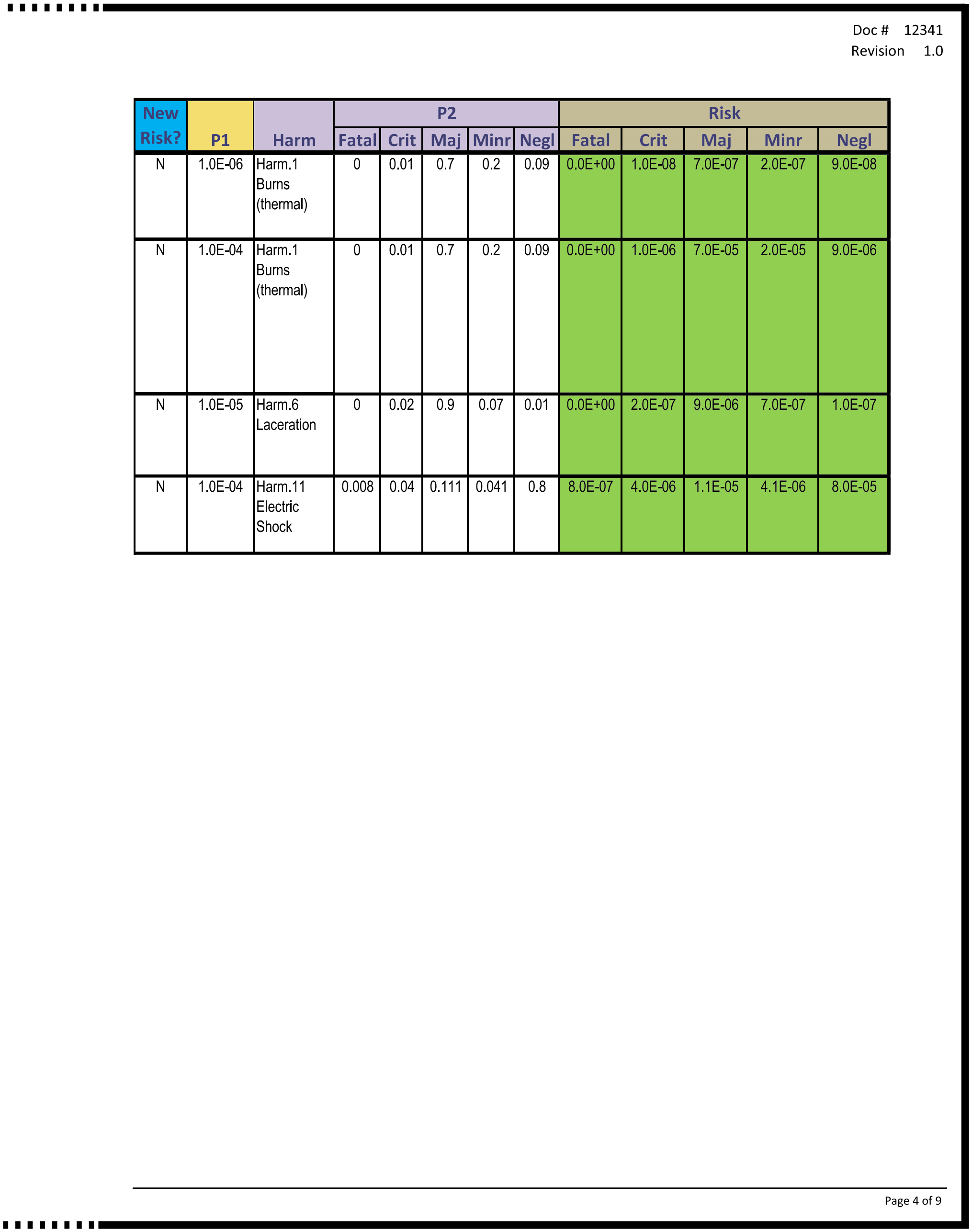
New Risk?			P2					Risk				
	P1	Harm	Fatal	Crit	Maj	Minr	Negl	Fatal	Crit	Maj	Minr	Negl
N	1.0E-02	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-03	1.0E-03	5.0E-04	0.0E+00	0.0E+00
N	1.0E-06	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-07	1.0E-07	5.0E-08	0.0E+00	0.0E+00
N	1.0E-06	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-07	1.0E-07	5.0E-08	0.0E+00	0.0E+00
N	1.0E-02	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-03	1.0E-03	5.0E-04	0.0E+00	0.0E+00
N	1.0E-04	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-05	1.0E-05	5.0E-06	0.0E+00	0.0E+00
Situation → Fibrillating patient does not receive therapy								1.70E-02	2.01E-03	1.00E-03	0.00E+00	0.00E+00
Y	1.0E-05	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-06	1.0E-06	5.0E-07	0.0E+00	0.0E+00
Y	1.0E-04	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-05	1.0E-05	5.0E-06	0.0E+00	0.0E+00
Haz.11 → Delayed Therapy								9.35E-05	1.10E-05	5.50E-06	0.00E+00	0.00E+00
Y	1.0E-04	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-05	1.0E-05	5.0E-06	0.0E+00	0.0E+00
N	1.0E-03	Harm.9 Pain from therapeutic electric shock	0	0	0.1	0.9	0	0.0E+00	0.0E+00	1.0E-04	9.0E-04	0.0E+00
N	1.0E-03	Harm.9 Pain from therapeutic electric shock	0	0	0.1	0.9	0	0.0E+00	0.0E+00	1.0E-04	9.0E-04	0.0E+00
Hazardous Situation →								0.00E+00	0.00E+00	2.00E-04	1.80E-03	0.00E+00



BXM

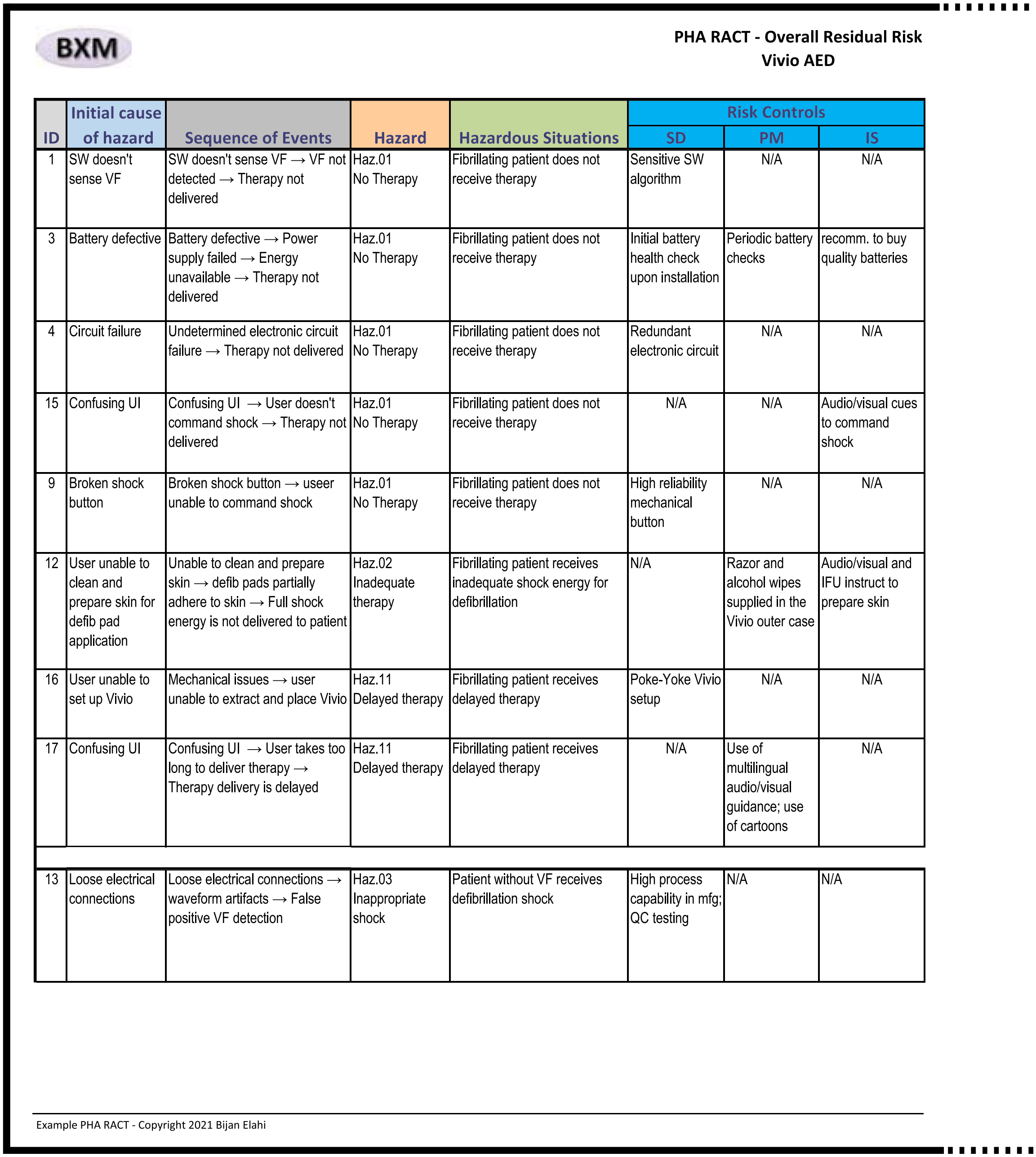
PHA RACT - Risk per Hazardous Situation
Vivio AED

ID	Initial cause of hazard	Sequence of Events	Hazard	Hazardous Situations	Risk Controls		
					SD	PM	IS
5	Circuit failure	Loss of feedback loop to µC → Charging circuit charges indefinitely → Increased internal temperature	Haz.04 Hot surfaces	User or bystander comes in contact with hot device	Thermistor feedback interlock to prevent runaway	Plastic casing is a poor heat conductor	N/A
6	Hair or dirt on patient's skin	Unable to clean and prepare skin → defib pads partially adhere to skin → sparks between pads and skin	Haz.05 Sparks (pad to skin)	Patient exposed to high voltage spark to skin	N/A	Razor and alcohol wipes supplied in the Vivio outer case	SW monitors EKG signal quality and warns of bad contact. Provides guidance.
7	Impact to casing	Impact to casing → cracked AED casing → sharps on AED body	Haz.07 Sharps	User or bystander comes in contact with a sharp edge/point	Casing made of ABS to withstand high impact	Soft grip surface to prevent dropping	Caution in IFU to not treat the AED roughly
14	Insulation breach	Breach of insulation on pad wires → high voltage lines become exposed	Haz.09 Current Leakage	User exposed to high voltage	Use of high integrity insulation	Packaging protects pad wires	Warning to user to stand clear



Doc # 12341
Revision 1.0

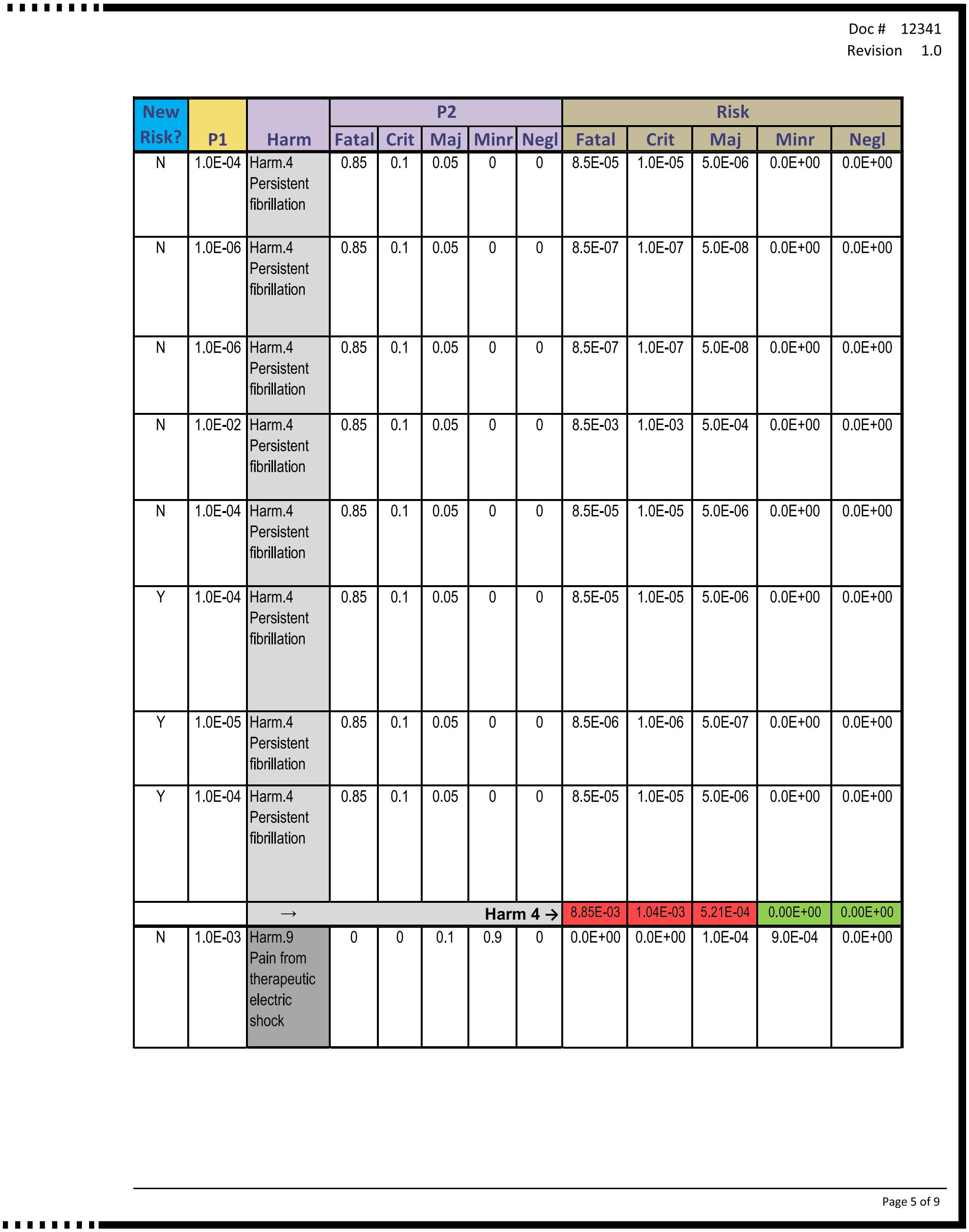
New Risk?	P1	Harm	P2					Risk				
			Fatal	Crit	Maj	Minr	Negl	Fatal	Crit	Maj	Minr	Negl
N	1.0E-06	Harm.1 Burns (thermal)	0	0.01	0.7	0.2	0.09	0.0E+00	1.0E-08	7.0E-07	2.0E-07	9.0E-08
N	1.0E-04	Harm.1 Burns (thermal)	0	0.01	0.7	0.2	0.09	0.0E+00	1.0E-06	7.0E-05	2.0E-05	9.0E-06
N	1.0E-05	Harm.6 Laceration	0	0.02	0.9	0.07	0.01	0.0E+00	2.0E-07	9.0E-06	7.0E-07	1.0E-07
N	1.0E-04	Harm.11 Electric Shock	0.008	0.04	0.111	0.041	0.8	8.0E-07	4.0E-06	1.1E-05	4.1E-06	8.0E-05



PHA RACT - Overall Residual Risk
Vivio AED

ID	Initial cause of hazard	Sequence of Events	Hazard	Hazardous Situations	Risk Controls		
					SD	PM	IS
1	SW doesn't sense VF	SW doesn't sense VF → VF not detected → Therapy not delivered	Haz.01 No Therapy	Fibrillating patient does not receive therapy	Sensitive SW algorithm	N/A	N/A
3	Battery defective	Battery defective → Power supply failed → Energy unavailable → Therapy not delivered	Haz.01 No Therapy	Fibrillating patient does not receive therapy	Initial battery health check upon installation	Periodic battery checks	recomm. to buy quality batteries
4	Circuit failure	Undetermined electronic circuit failure → Therapy not delivered	Haz.01 No Therapy	Fibrillating patient does not receive therapy	Redundant electronic circuit	N/A	N/A
15	Confusing UI	Confusing UI → User doesn't command shock → Therapy not delivered	Haz.01 No Therapy	Fibrillating patient does not receive therapy	N/A	N/A	Audio/visual cues to command shock
9	Broken shock button	Broken shock button → useer unable to command shock	Haz.01 No Therapy	Fibrillating patient does not receive therapy	High reliability mechanical button	N/A	N/A
12	User unable to clean and prepare skin for defib pad application	Unable to clean and prepare skin → defib pads partially adhere to skin → Full shock energy is not delivered to patient	Haz.02 Inadequate therapy	Fibrillating patient receives inadequate shock energy for defibrillation	N/A	Razor and alcohol wipes supplied in the Vivio outer case	Audio/visual and IFU instruct to prepare skin
16	User unable to set up Vivio	Mechanical issues → user unable to extract and place Vivio	Haz.11 Delayed therapy	Fibrillating patient receives delayed therapy	Poke-Yoke Vivio setup	N/A	N/A
17	Confusing UI	Confusing UI → User takes too long to deliver therapy → Therapy delivery is delayed	Haz.11 Delayed therapy	Fibrillating patient receives delayed therapy	N/A	Use of multilingual audio/visual guidance; use of cartoons	N/A
13	Loose electrical connections	Loose electrical connections → waveform artifacts → False positive VF detection	Haz.03 Inappropriate shock	Patient without VF receives defibrillation shock	High process capability in mfg; QC testing	N/A	N/A

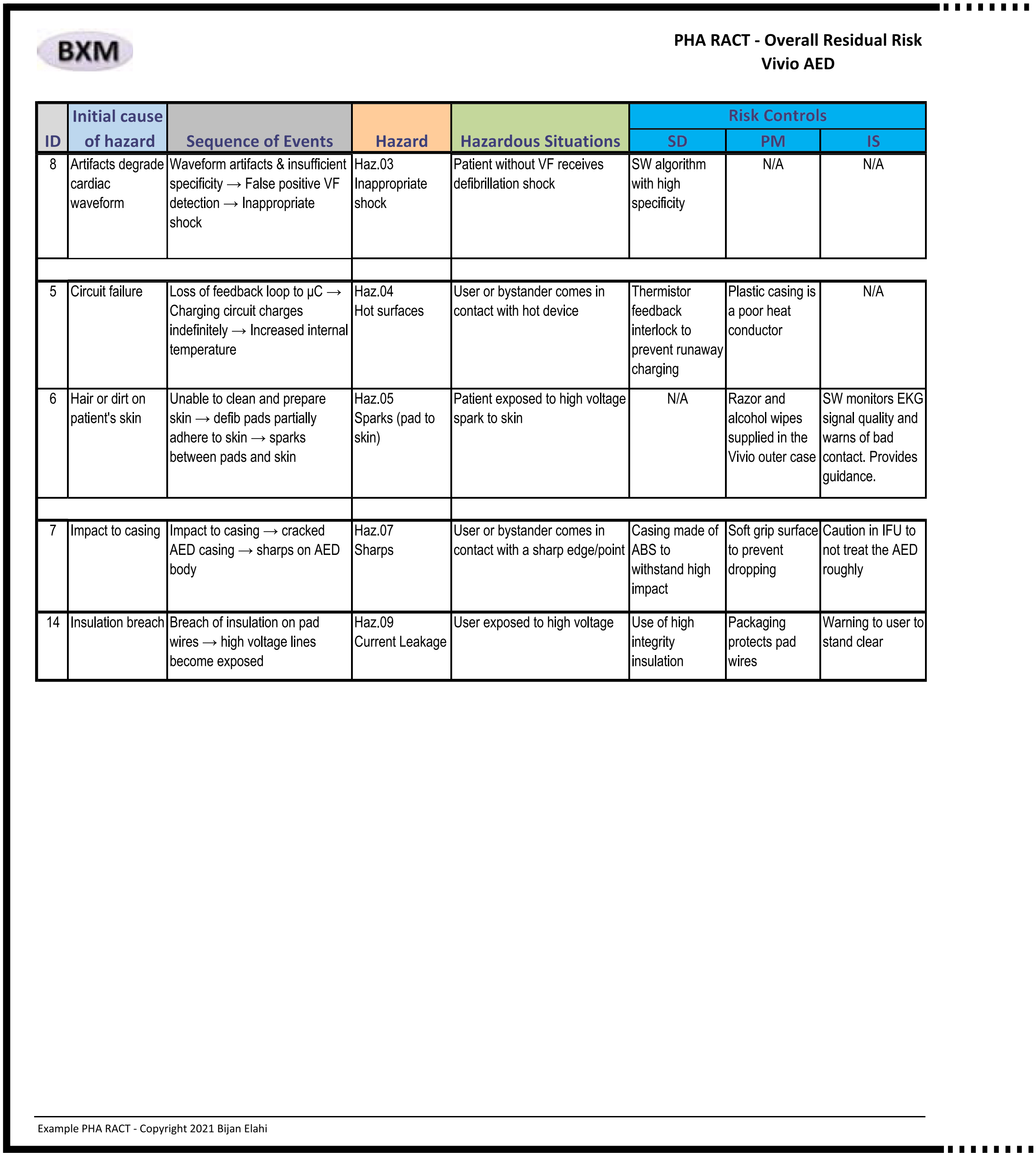
Example PHA RACT - Copyright 2021 Bijan Elahi



Doc # 12341
Revision 1.0

New Risk?	P1	Harm	P2 Fatal	P2 Crit	P2 Maj	P2 Minr	P2 Negl	Risk Fatal	Risk Crit	Risk Maj	Risk Minr	Risk Negl
N	1.0E-04	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-05	1.0E-05	5.0E-06	0.0E+00	0.0E+00
N	1.0E-06	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-07	1.0E-07	5.0E-08	0.0E+00	0.0E+00
N	1.0E-06	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-07	1.0E-07	5.0E-08	0.0E+00	0.0E+00
N	1.0E-02	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-03	1.0E-03	5.0E-04	0.0E+00	0.0E+00
N	1.0E-04	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-05	1.0E-05	5.0E-06	0.0E+00	0.0E+00
Y	1.0E-04	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-05	1.0E-05	5.0E-06	0.0E+00	0.0E+00
Y	1.0E-05	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-06	1.0E-06	5.0E-07	0.0E+00	0.0E+00
Y	1.0E-04	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-05	1.0E-05	5.0E-06	0.0E+00	0.0E+00
		→					Harm 4 →	8.85E-03	1.04E-03	5.21E-04	0.00E+00	0.00E+00
N	1.0E-03	Harm.9 Pain from therapeutic electric shock	0	0	0.1	0.9	0	0.0E+00	0.0E+00	1.0E-04	9.0E-04	0.0E+00

Page 5 of 9

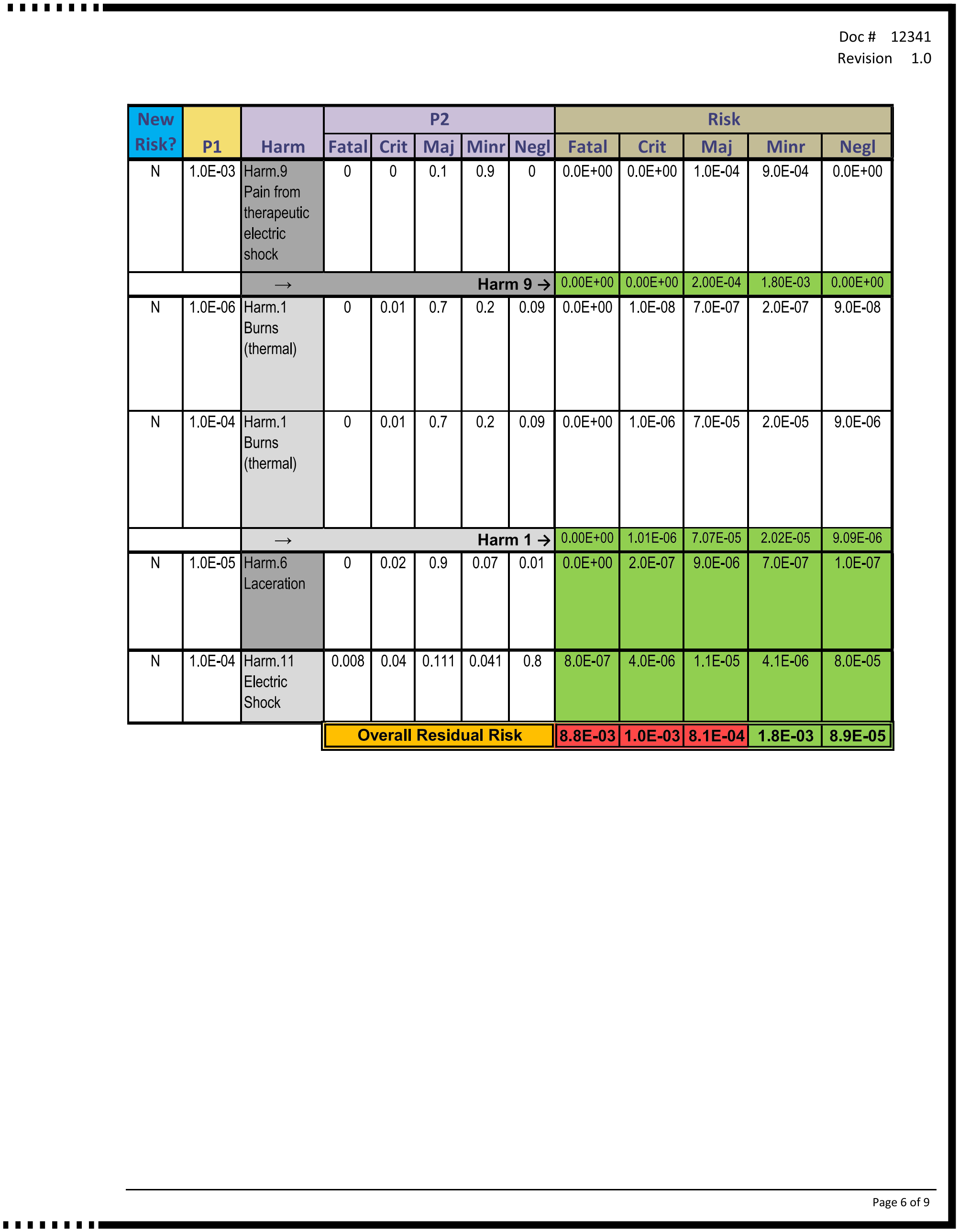


BXM

PHA RACT - Overall Residual Risk
Vivio AED

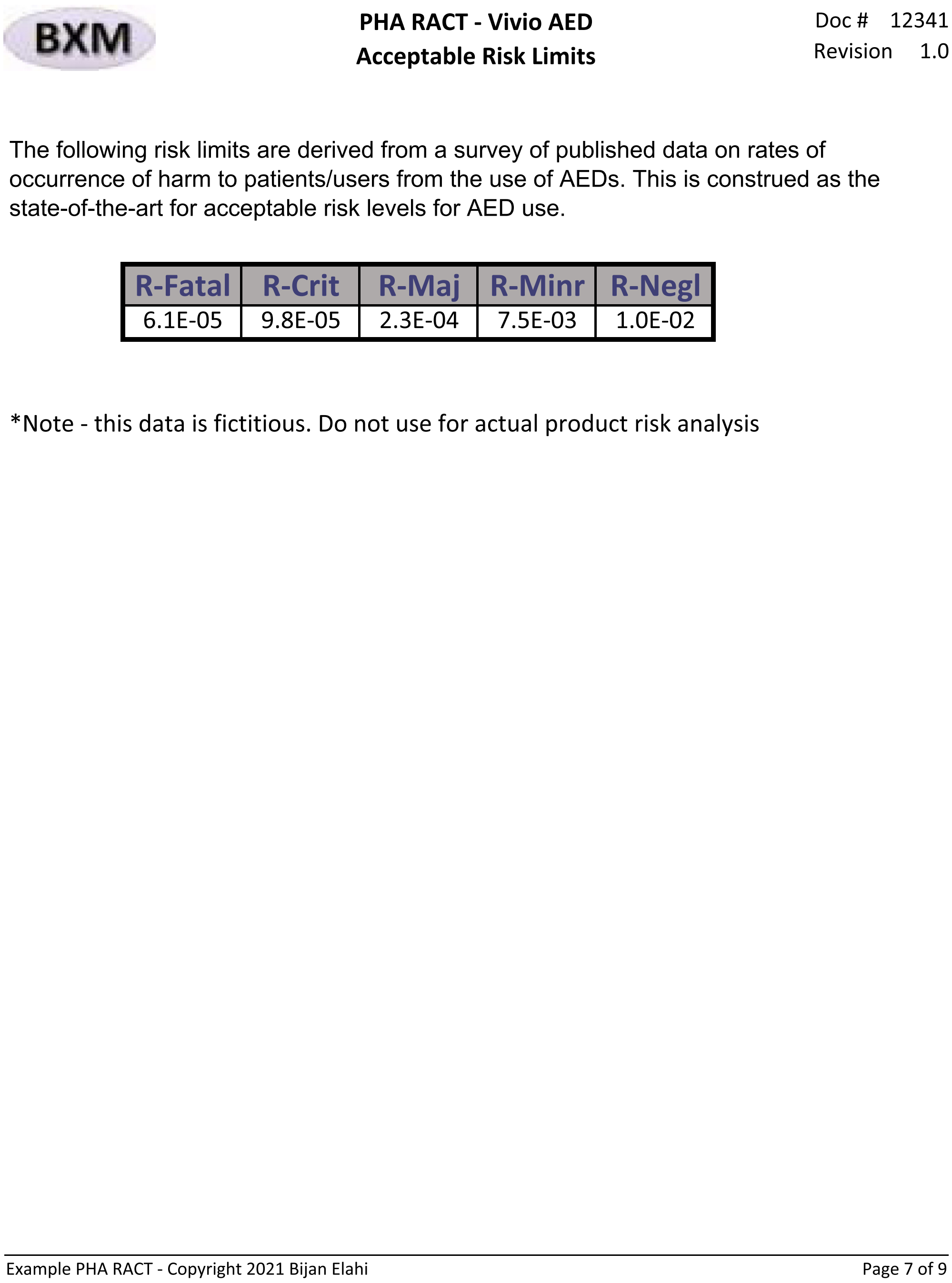
ID	Initial cause of hazard	Sequence of Events	Hazard	Hazardous Situations	Risk Controls		
					SD	PM	IS
8	Artifacts degrade cardiac waveform	Waveform artifacts & insufficient specificity → False positive VF detection → Inappropriate shock	Haz.03 Inappropriate shock	Patient without VF receives defibrillation shock	SW algorithm with high specificity	N/A	N/A
5	Circuit failure	Loss of feedback loop to μC → Charging circuit charges indefinitely → Increased internal temperature	Haz.04 Hot surfaces	User or bystander comes in contact with hot device	Thermistor feedback interlock to prevent runaway charging	Plastic casing is a poor heat conductor	N/A
6	Hair or dirt on patient's skin	Unable to clean and prepare skin → defib pads partially adhere to skin → sparks between pads and skin	Haz.05 Sparks (pad to skin)	Patient exposed to high voltage spark to skin	N/A	Razor and alcohol wipes supplied in the Vivio outer case	SW monitors EKG signal quality and warns of bad contact. Provides guidance.
7	Impact to casing	Impact to casing → cracked AED casing → sharps on AED body	Haz.07 Sharps	User or bystander comes in contact with a sharp edge/point	Casing made of ABS to withstand high impact	Soft grip surface to prevent dropping	Caution in IFU to not treat the AED roughly
14	Insulation breach	Breach of insulation on pad wires → high voltage lines become exposed	Haz.09 Current Leakage	User exposed to high voltage	Use of high integrity insulation	Packaging protects pad wires	Warning to user to stand clear

Example PHA RACT - Copyright 2021 Bijan Elahi



Doc # 12341
Revision 1.0

New Risk?	P1	Harm	P2					Risk				
			Fatal	Crit	Maj	Minr	Negl	Fatal	Crit	Maj	Minr	Negl
N	1.0E-03	Harm.9 Pain from therapeutic electric shock	0	0	0.1	0.9	0	0.0E+00	0.0E+00	1.0E-04	9.0E-04	0.0E+00
		→	Harm 9 →					0.00E+00	0.00E+00	2.00E-04	1.80E-03	0.00E+00
N	1.0E-06	Harm.1 Burns (thermal)	0	0.01	0.7	0.2	0.09	0.0E+00	1.0E-08	7.0E-07	2.0E-07	9.0E-08
N	1.0E-04	Harm.1 Burns (thermal)	0	0.01	0.7	0.2	0.09	0.0E+00	1.0E-06	7.0E-05	2.0E-05	9.0E-06
		→	Harm 1 →					0.00E+00	1.01E-06	7.07E-05	2.02E-05	9.09E-06
N	1.0E-05	Harm.6 Laceration	0	0.02	0.9	0.07	0.01	0.0E+00	2.0E-07	9.0E-06	7.0E-07	1.0E-07
N	1.0E-04	Harm.11 Electric Shock	0.008	0.04	0.111	0.041	0.8	8.0E-07	4.0E-06	1.1E-05	4.1E-06	8.0E-05
			Overall Residual Risk					**8.8E-03**	**1.0E-03**	**8.1E-04**	**1.8E-03**	**8.9E-05**



BXM

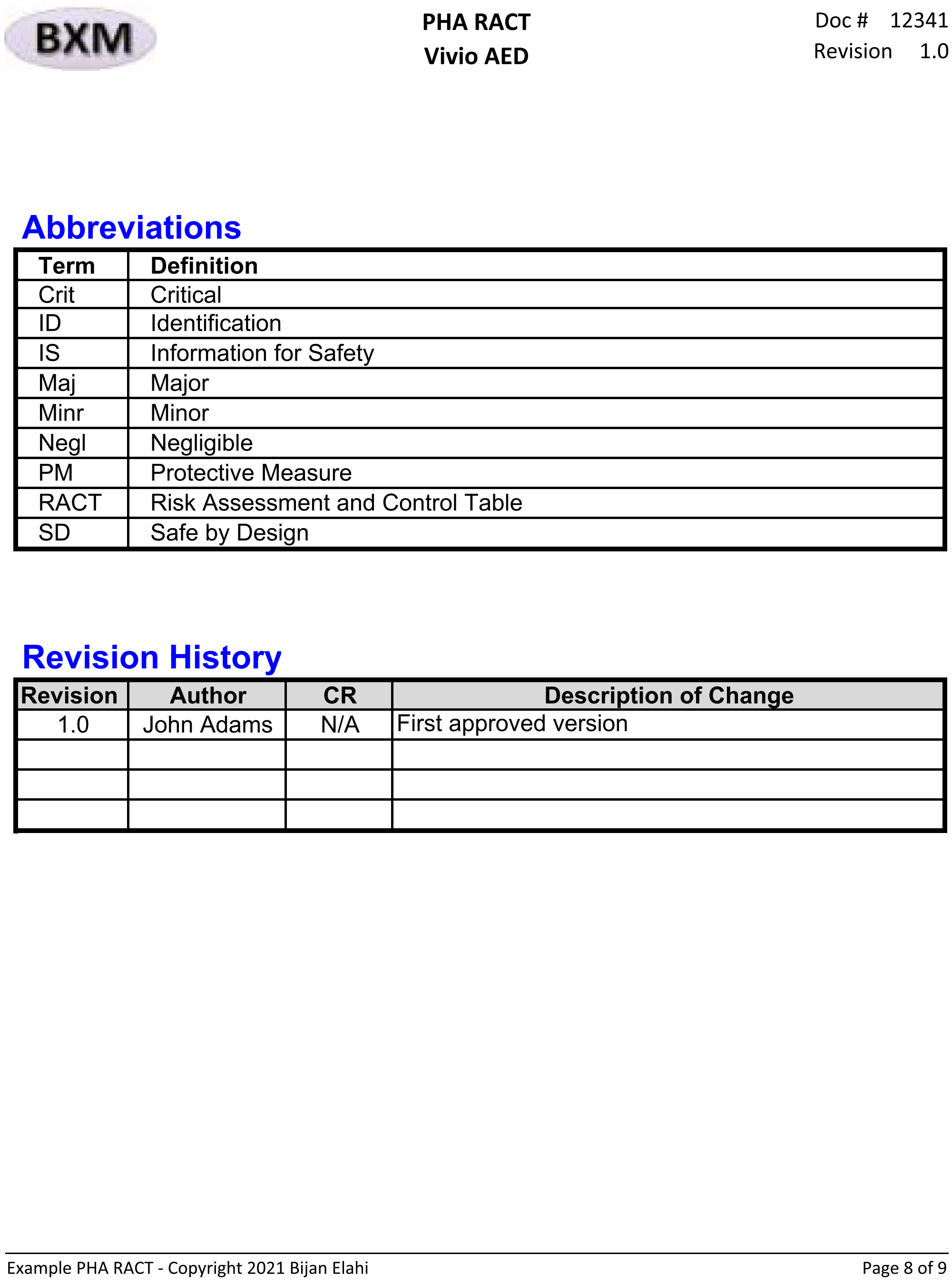
PHA RACT - Vivio AED
Acceptable Risk Limits

Doc # 12341
Revision 1.0

The following risk limits are derived from a survey of published data on rates of occurrence of harm to patients/users from the use of AEDs. This is construed as the state-of-the-art for acceptable risk levels for AED use.

R-Fatal	R-Crit	R-Maj	R-Minr	R-Negl
6.1E-05	9.8E-05	2.3E-04	7.5E-03	1.0E-02

*Note - this data is fictitious. Do not use for actual product risk analysis



PHA RACT
Vivio AED

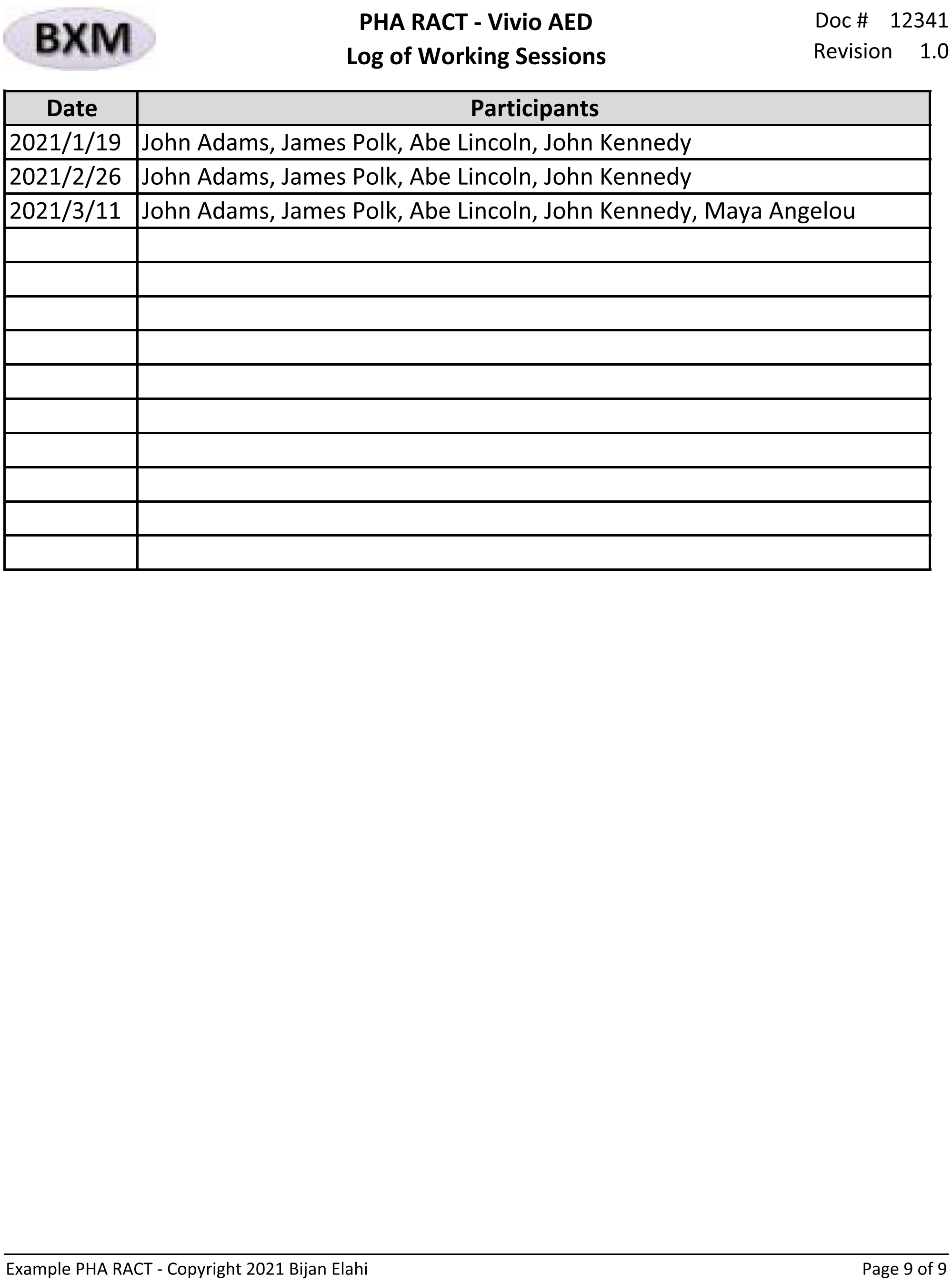
Doc # 12341
Revision 1.0

Abbreviations

Term	Definition
Crit	Critical
ID	Identification
IS	Information for Safety
Maj	Major
Minr	Minor
Negl	Negligible
PM	Protective Measure
RACT	Risk Assessment and Control Table
SD	Safe by Design

Revision History

Revision	Author	CR	Description of Change
1.0	John Adams	N/A	First approved version



BXM

PHA RACT - Vivio AED
Log of Working Sessions

Doc # 12341
Revision 1.0

Date	Participants
2021/1/19	John Adams, James Polk, Abe Lincoln, John Kennedy
2021/2/26	John Adams, James Polk, Abe Lincoln, John Kennedy
2021/3/11	John Adams, James Polk, Abe Lincoln, John Kennedy, Maya Angelou

Example PHA RACT - Copyright 2021 Bijan Elahi

Page 9 of 9

C.8 DESIGN FAILURE MODES AND EFFECTS ANALYSIS

BXM

DFMEA
Vivio AED

Doc # 12344
Revision 1.0

Scope

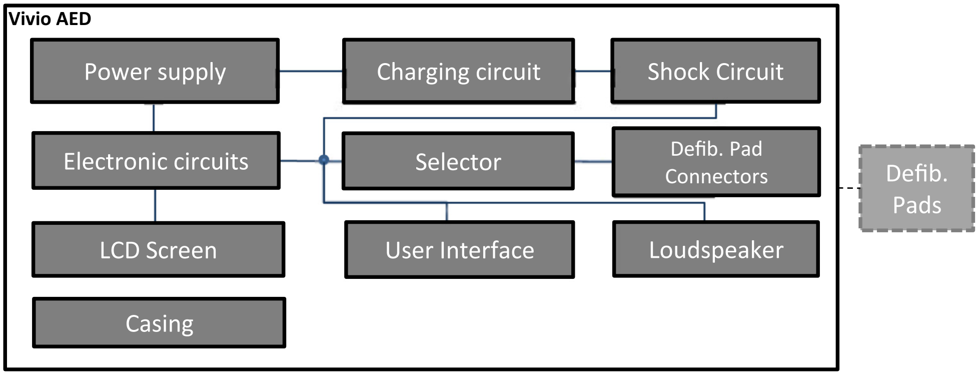
This DFMEA covers the Vivio AED design.

The scope of the analysis is bounded in the diagram below and encompases all the items within the analysis boundary.

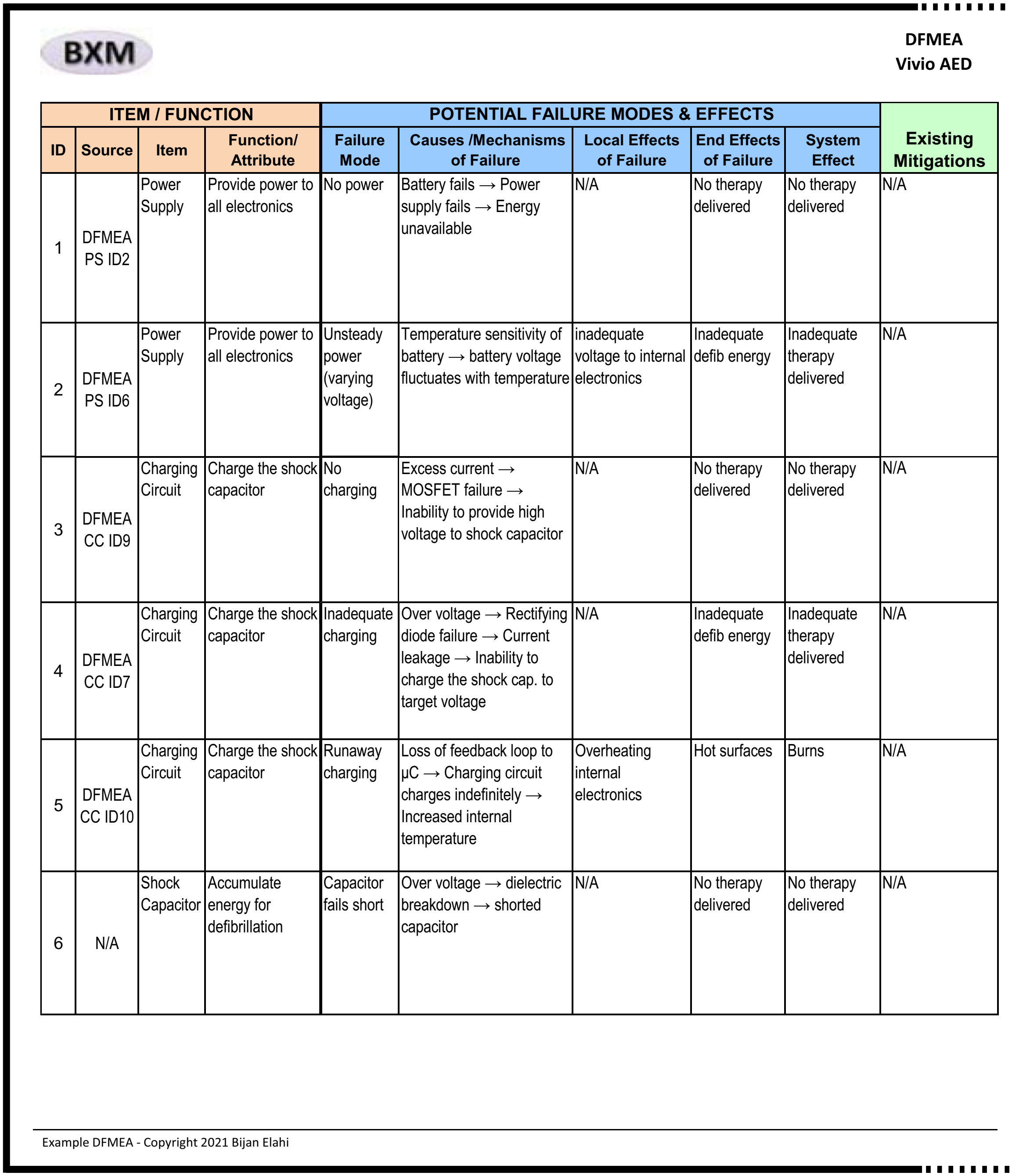
Item Under Analysis: Vivio AED model 1234, version 1.1

Primary functions: Detect VF and deliver therapeutic shock

Secondary Functions: Monitor AED health and report any abnormalities
Monitor the connections of the defibrillation pads, both to Vivio and to patient's skin



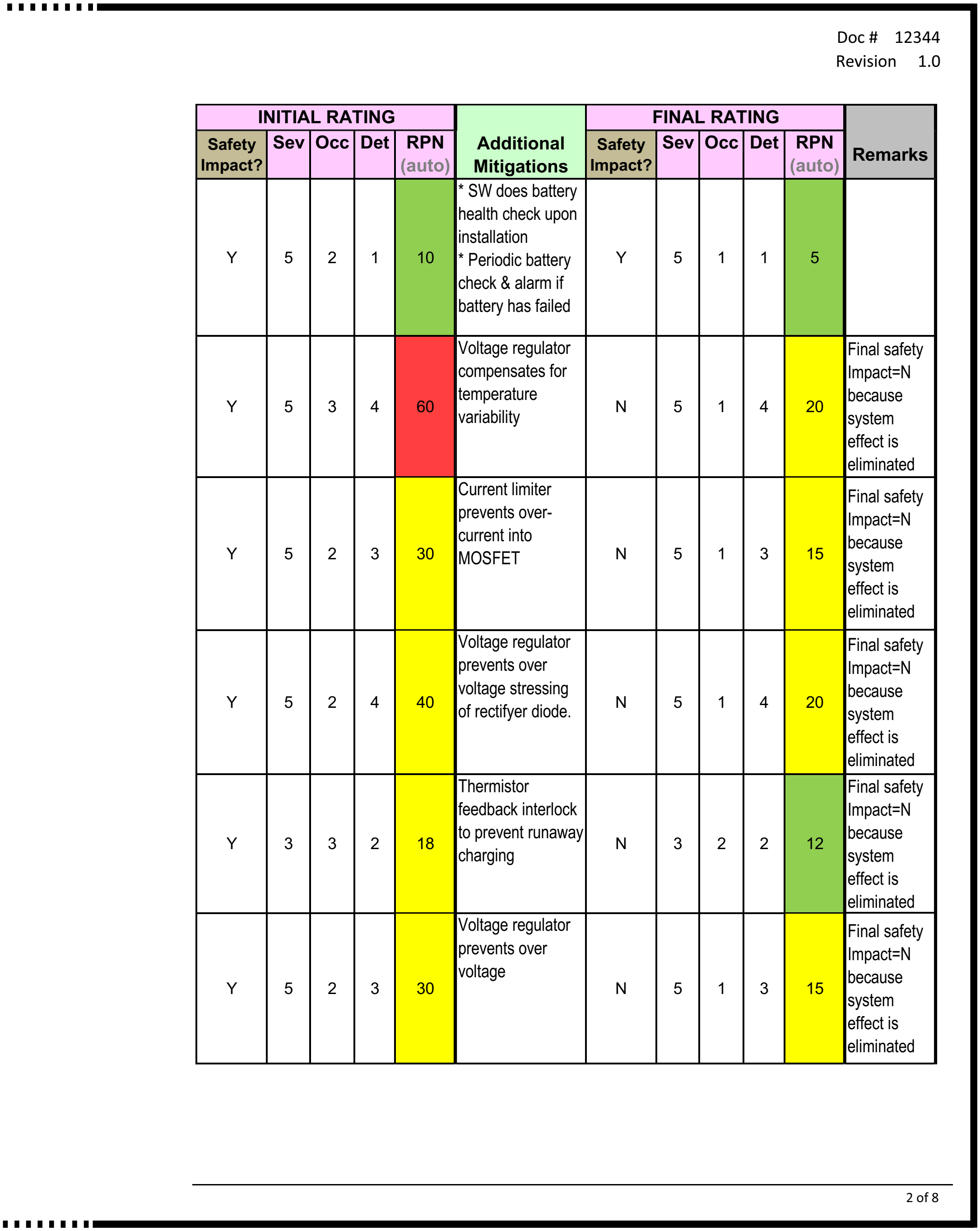
Note - This Example DFMEA is abbreviated and truncated due to page limitations in the book.



DFMEA
Vivio AED

ITEM / FUNCTION				POTENTIAL FAILURE MODES & EFFECTS					Existing Mitigations
ID	Source	Item	Function/ Attribute	Failure Mode	Causes /Mechanisms of Failure	Local Effects of Failure	End Effects of Failure	System Effect	
1	DFMEA PS ID2	Power Supply	Provide power to all electronics	No power	Battery fails → Power supply fails → Energy unavailable	N/A	No therapy delivered	No therapy delivered	N/A
2	DFMEA PS ID6	Power Supply	Provide power to all electronics	Unsteady power (varying voltage)	Temperature sensitivity of battery → battery voltage fluctuates with temperature	inadequate voltage to internal electronics	Inadequate defib energy	Inadequate therapy delivered	N/A
3	DFMEA CC ID9	Charging Circuit	Charge the shock capacitor	No charging	Excess current → MOSFET failure → Inability to provide high voltage to shock capacitor	N/A	No therapy delivered	No therapy delivered	N/A
4	DFMEA CC ID7	Charging Circuit	Charge the shock capacitor	Inadequate charging	Over voltage → Rectifying diode failure → Current leakage → Inability to charge the shock cap. to target voltage	N/A	Inadequate defib energy	Inadequate therapy delivered	N/A
5	DFMEA CC ID10	Charging Circuit	Charge the shock capacitor	Runaway charging	Loss of feedback loop to µC → Charging circuit charges indefinitely → Increased internal temperature	Overheating internal electronics	Hot surfaces	Burns	N/A
6	N/A	Shock Capacitor	Accumulate energy for defibrillation	Capacitor fails short	Over voltage → dielectric breakdown → shorted capacitor	N/A	No therapy delivered	No therapy delivered	N/A

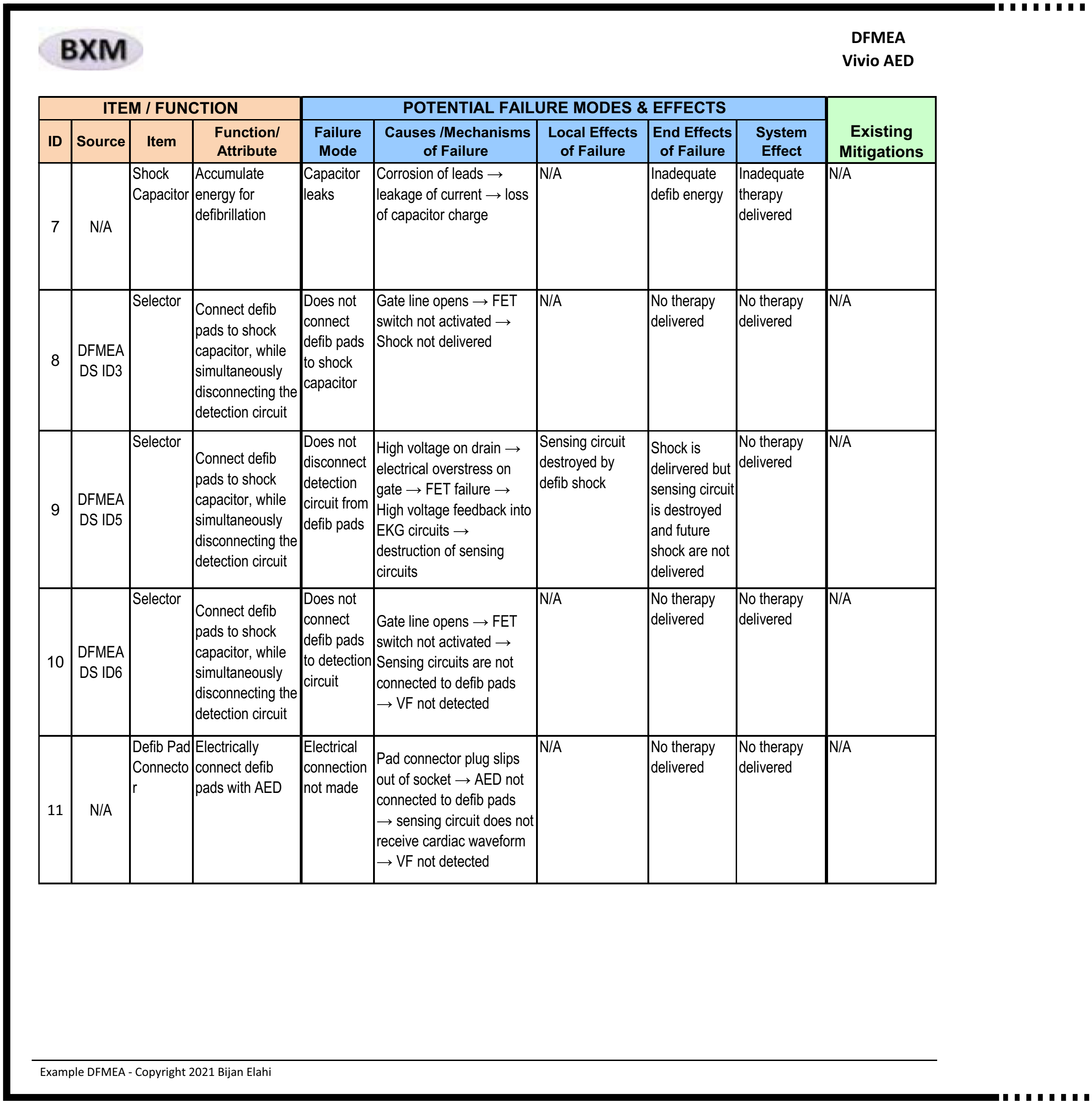
Example DFMEA - Copyright 2021 Bijan Elahi



Doc # 12344
Revision 1.0

INITIAL RATING					Additional Mitigations	FINAL RATING					Remarks
Safety Impact?	Sev	Occ	Det	RPN (auto)		Safety Impact?	Sev	Occ	Det	RPN (auto)	
Y	5	2	1	10	* SW does battery health check upon installation * Periodic battery check & alarm if battery has failed	Y	5	1	1	5	
Y	5	3	4	60	Voltage regulator compensates for temperature variability	N	5	1	4	20	Final safety Impact=N because system effect is eliminated
Y	5	2	3	30	Current limiter prevents over-current into MOSFET	N	5	1	3	15	Final safety Impact=N because system effect is eliminated
Y	5	2	4	40	Voltage regulator prevents over voltage stressing of rectifyer diode.	N	5	1	4	20	Final safety Impact=N because system effect is eliminated
Y	3	3	2	18	Thermistor feedback interlock to prevent runaway charging	N	3	2	2	12	Final safety Impact=N because system effect is eliminated
Y	5	2	3	30	Voltage regulator prevents over voltage	N	5	1	3	15	Final safety Impact=N because system effect is eliminated

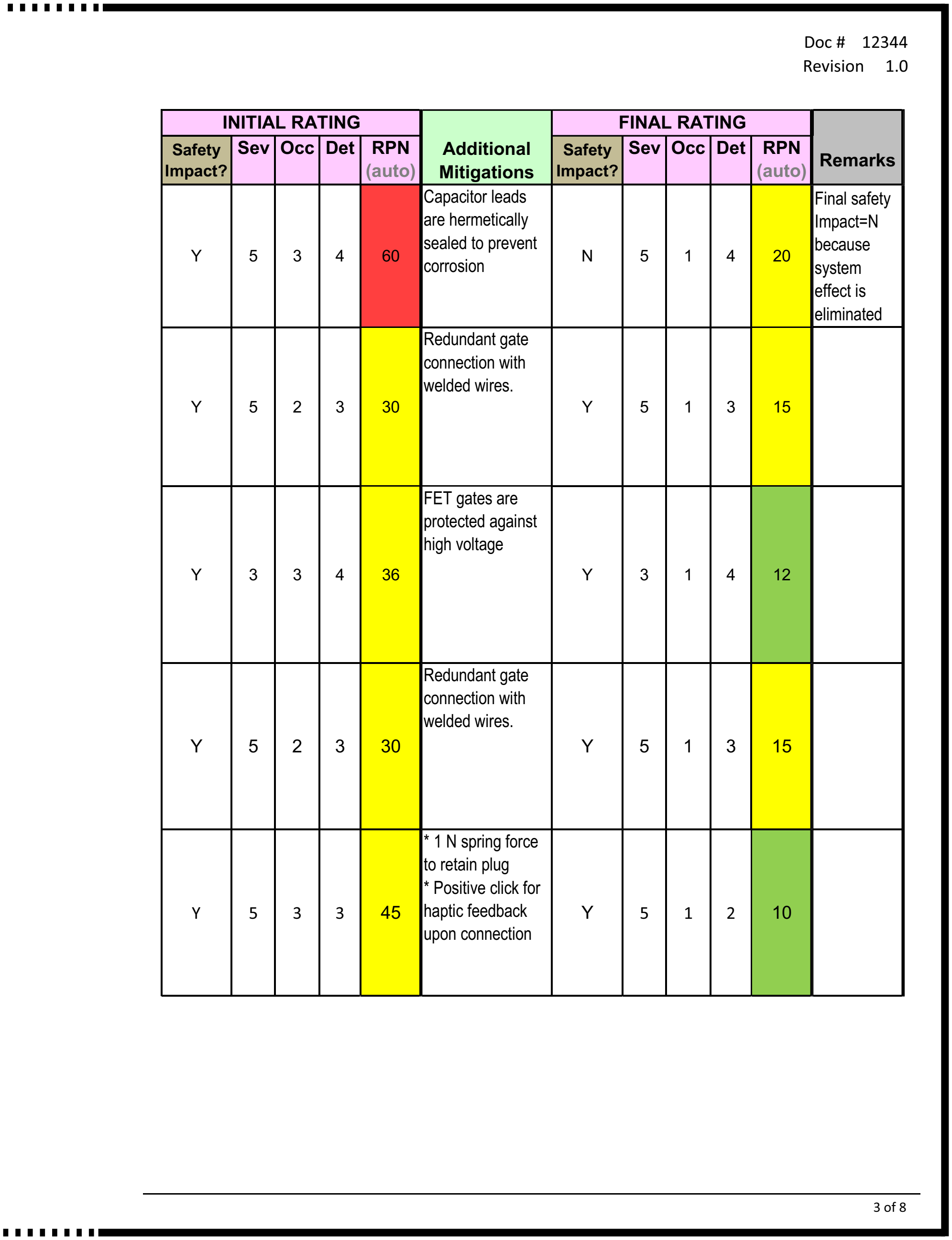
2 of 8



DFMEA
Vivio AED

ITEM / FUNCTION				POTENTIAL FAILURE MODES & EFFECTS					Existing Mitigations
ID	Source	Item	Function/ Attribute	Failure Mode	Causes /Mechanisms of Failure	Local Effects of Failure	End Effects of Failure	System Effect	
7	N/A	Shock Capacitor	Accumulate energy for defibrillation	Capacitor leaks	Corrosion of leads → leakage of current → loss of capacitor charge	N/A	Inadequate defib energy	Inadequate therapy delivered	N/A
8	DFMEA DS ID3	Selector	Connect defib pads to shock capacitor, while simultaneously disconnecting the detection circuit	Does not connect defib pads to shock capacitor	Gate line opens → FET switch not activated → Shock not delivered	N/A	No therapy delivered	No therapy delivered	N/A
9	DFMEA DS ID5	Selector	Connect defib pads to shock capacitor, while simultaneously disconnecting the detection circuit	Does not disconnect detection circuit from defib pads	High voltage on drain → electrical overstress on gate → FET failure → High voltage feedback into EKG circuits → destruction of sensing circuits	Sensing circuit destroyed by defib shock	Shock is delirvered but sensing circuit is destroyed and future shock are not delivered	No therapy delivered	N/A
10	DFMEA DS ID6	Selector	Connect defib pads to shock capacitor, while simultaneously disconnecting the detection circuit	Does not connect defib pads to detection circuit	Gate line opens → FET switch not activated → Sensing circuits are not connected to defib pads → VF not detected	N/A	No therapy delivered	No therapy delivered	N/A
11	N/A	Defib Pad Connector	Electrically connect defib pads with AED	Electrical connection not made	Pad connector plug slips out of socket → AED not connected to defib pads → sensing circuit does not receive cardiac waveform → VF not detected	N/A	No therapy delivered	No therapy delivered	N/A

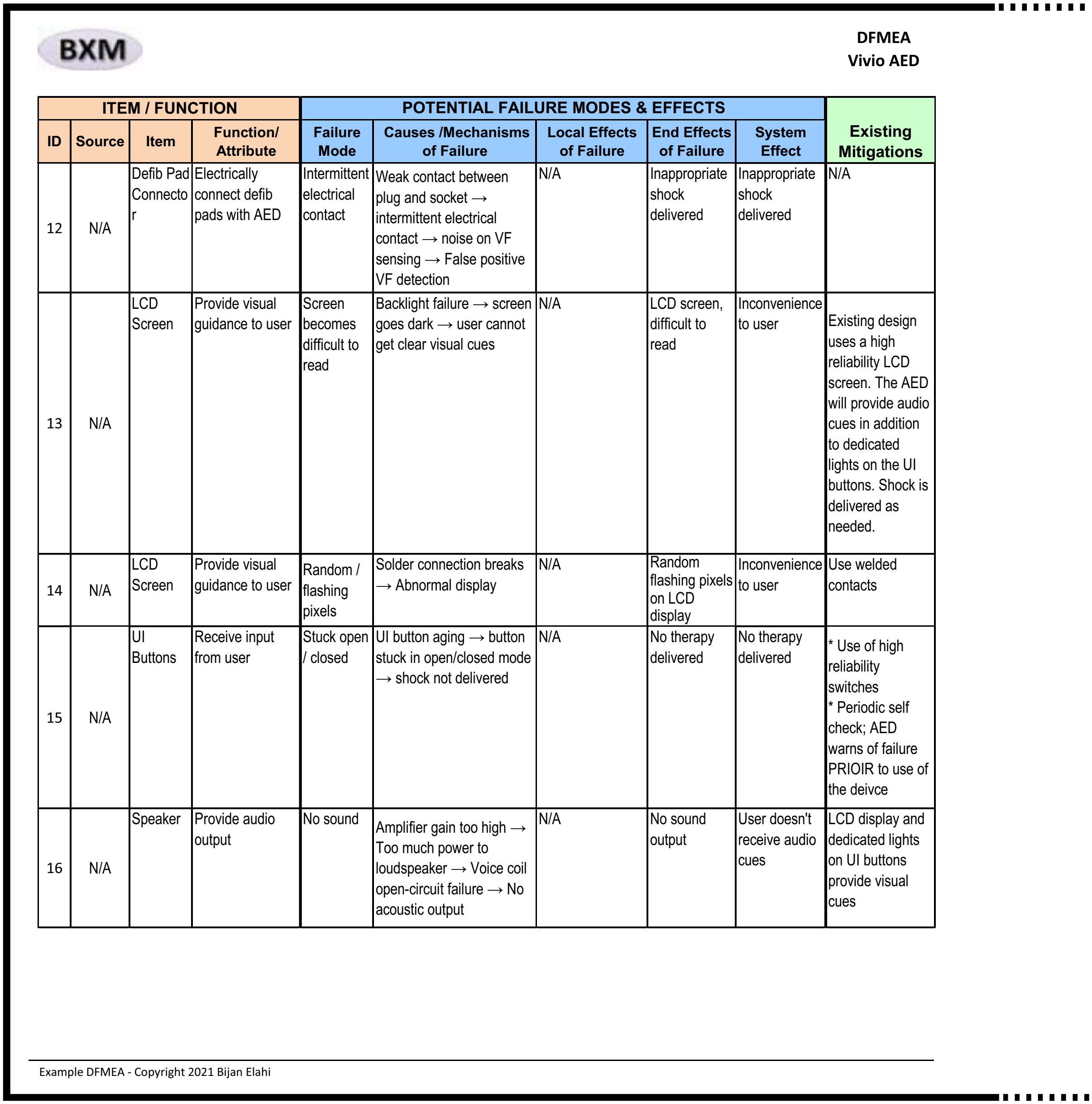
Example DFMEA - Copyright 2021 Bijan Elahi



Doc # 12344
Revision 1.0

INITIAL RATING					Additional Mitigations	FINAL RATING					Remarks
Safety Impact?	Sev	Occ	Det	RPN (auto)		Safety Impact?	Sev	Occ	Det	RPN (auto)	
Y	5	3	4	60	Capacitor leads are hermetically sealed to prevent corrosion	N	5	1	4	20	Final safety Impact=N because system effect is eliminated
Y	5	2	3	30	Redundant gate connection with welded wires.	Y	5	1	3	15	
Y	3	3	4	36	FET gates are protected against high voltage	Y	3	1	4	12	
Y	5	2	3	30	Redundant gate connection with welded wires.	Y	5	1	3	15	
Y	5	3	3	45	* 1 N spring force to retain plug * Positive click for haptic feedback upon connection	Y	5	1	2	10	

3 of 8

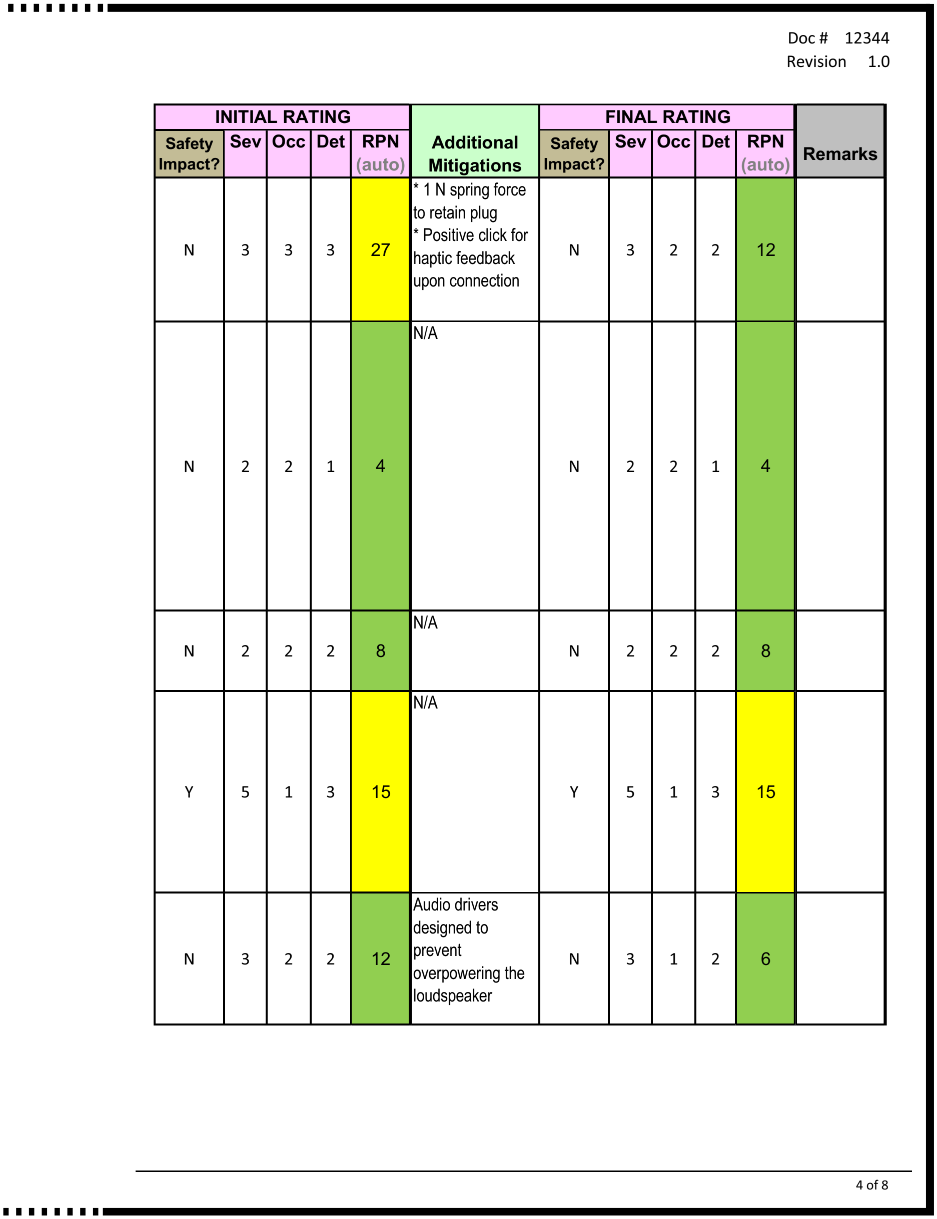


BXM

DFMEA
Vivio AED

ITEM / FUNCTION				POTENTIAL FAILURE MODES & EFFECTS					Existing Mitigations
ID	Source	Item	Function/ Attribute	Failure Mode	Causes /Mechanisms of Failure	Local Effects of Failure	End Effects of Failure	System Effect	
12	N/A	Defib Pad Connector	Electrically connect defib pads with AED	Intermittent electrical contact	Weak contact between plug and socket → intermittent electrical contact → noise on VF sensing → False positive VF detection	N/A	Inappropriate shock delivered	Inappropriate shock delivered	N/A
13	N/A	LCD Screen	Provide visual guidance to user	Screen becomes difficult to read	Backlight failure → screen goes dark → user cannot get clear visual cues	N/A	LCD screen, difficult to read	Inconvenience to user	Existing design uses a high reliability LCD screen. The AED will provide audio cues in addition to dedicated lights on the UI buttons. Shock is delivered as needed.
14	N/A	LCD Screen	Provide visual guidance to user	Random / flashing pixels	Solder connection breaks → Abnormal display	N/A	Random flashing pixels on LCD display	Inconvenience to user	Use welded contacts
15	N/A	UI Buttons	Receive input from user	Stuck open / closed	UI button aging → button stuck in open/closed mode → shock not delivered	N/A	No therapy delivered	No therapy delivered	* Use of high reliability switches * Periodic self check; AED warns of failure PRIOIR to use of the deivce
16	N/A	Speaker	Provide audio output	No sound	Amplifier gain too high → Too much power to loudspeaker → Voice coil open-circuit failure → No acoustic output	N/A	No sound output	User doesn't receive audio cues	LCD display and dedicated lights on UI buttons provide visual cues

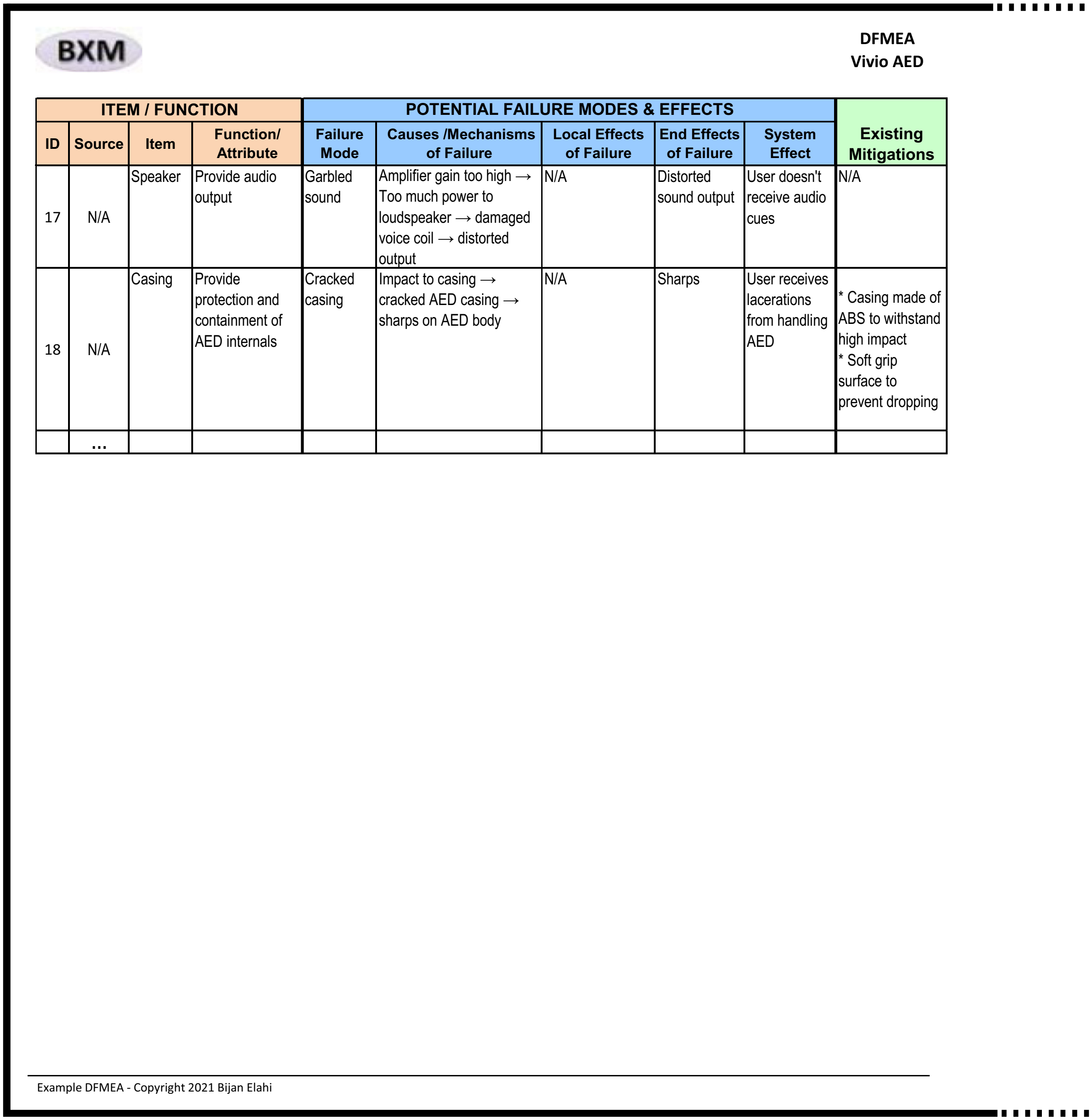
Example DFMEA - Copyright 2021 Bijan Elahi



Doc # 12344
Revision 1.0

INITIAL RATING						FINAL RATING					
Safety Impact?	Sev	Occ	Det	RPN (auto)	Additional Mitigations	Safety Impact?	Sev	Occ	Det	RPN (auto)	Remarks
N	3	3	3	27	* 1 N spring force to retain plug * Positive click for haptic feedback upon connection	N	3	2	2	12	
N	2	2	1	4	N/A	N	2	2	1	4	
N	2	2	2	8	N/A	N	2	2	2	8	
Y	5	1	3	15	N/A	Y	5	1	3	15	
N	3	2	2	12	Audio drivers designed to prevent overpowering the loudspeaker	N	3	1	2	6	

4 of 8

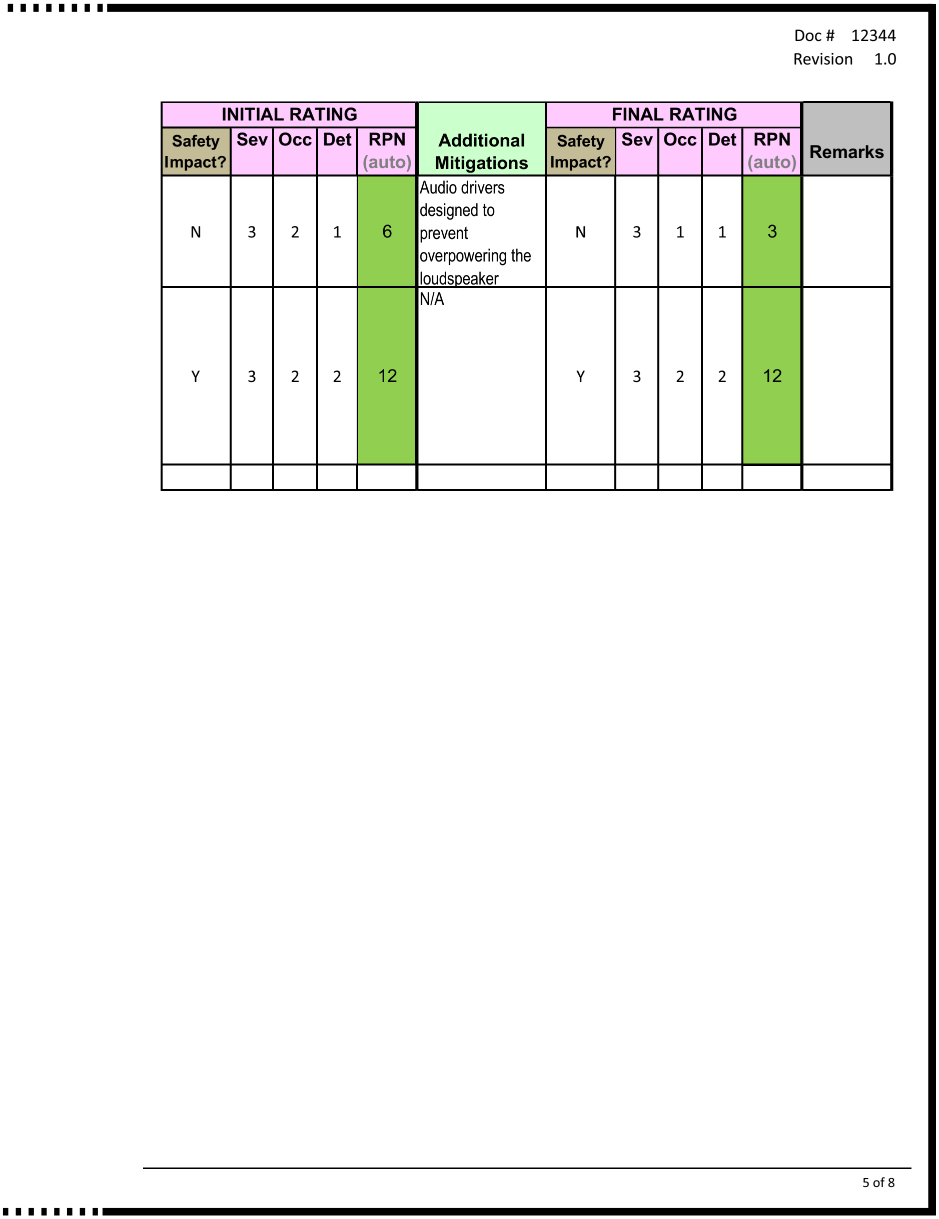


BXM

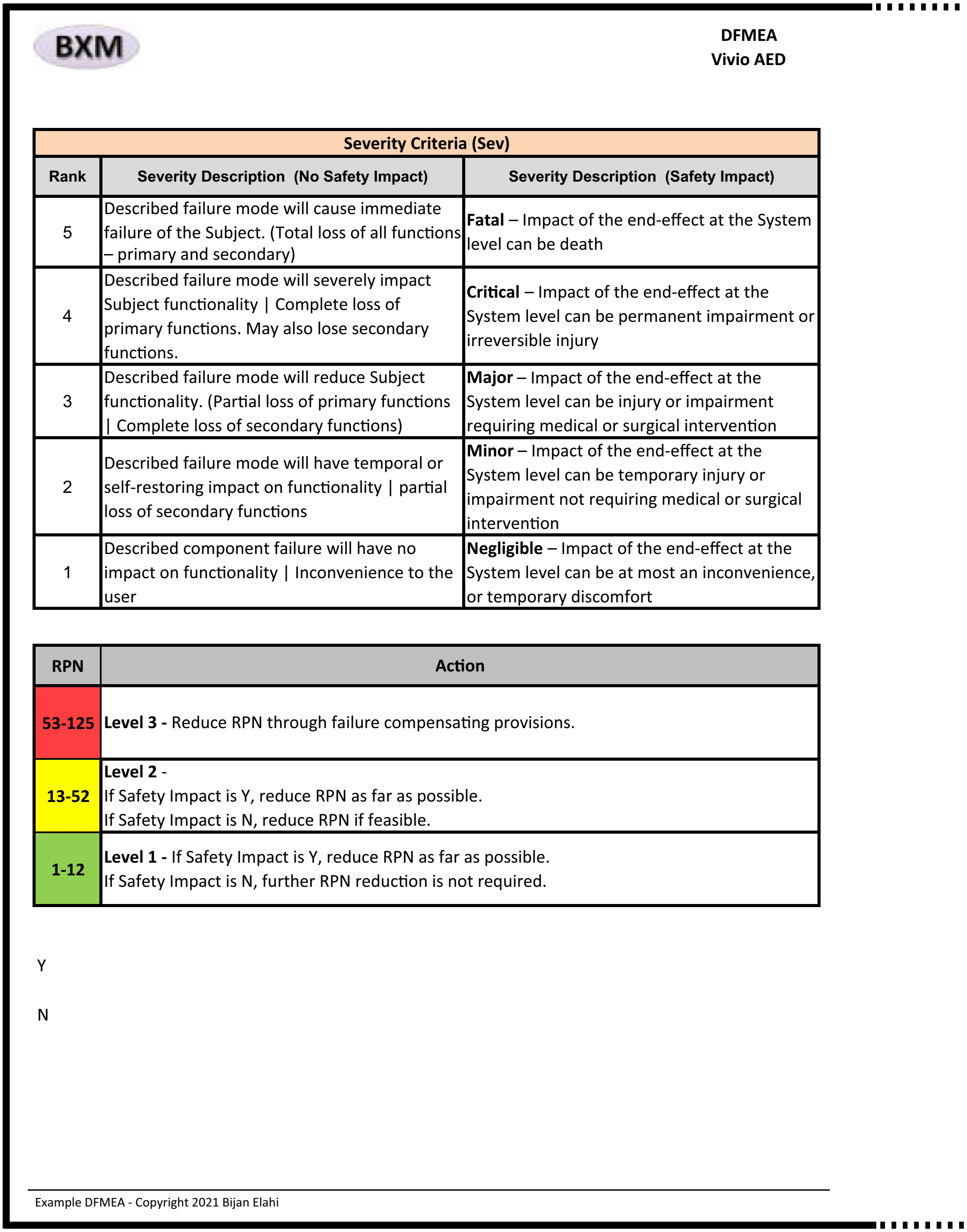
DFMEA
Vivio AED

ITEM / FUNCTION				POTENTIAL FAILURE MODES & EFFECTS					Existing Mitigations
ID	Source	Item	Function/ Attribute	Failure Mode	Causes /Mechanisms of Failure	Local Effects of Failure	End Effects of Failure	System Effect	
17	N/A	Speaker	Provide audio output	Garbled sound	Amplifier gain too high → Too much power to loudspeaker → damaged voice coil → distorted output	N/A	Distorted sound output	User doesn't receive audio cues	N/A
18	N/A	Casing	Provide protection and containment of AED internals	Cracked casing	Impact to casing → cracked AED casing → sharps on AED body	N/A	Sharps	User receives lacerations from handling AED	* Casing made of ABS to withstand high impact * Soft grip surface to prevent dropping
	...								

Example DFMEA - Copyright 2021 Bijan Elahi



INITIAL RATING					Additional Mitigations	FINAL RATING					Remarks
Safety Impact?	Sev	Occ	Det	RPN (auto)		Safety Impact?	Sev	Occ	Det	RPN (auto)	
N	3	2	1	6	Audio drivers designed to prevent overpowering the loudspeaker	N	3	1	1	3	
Y	3	2	2	12	N/A	Y	3	2	2	12	



BXM

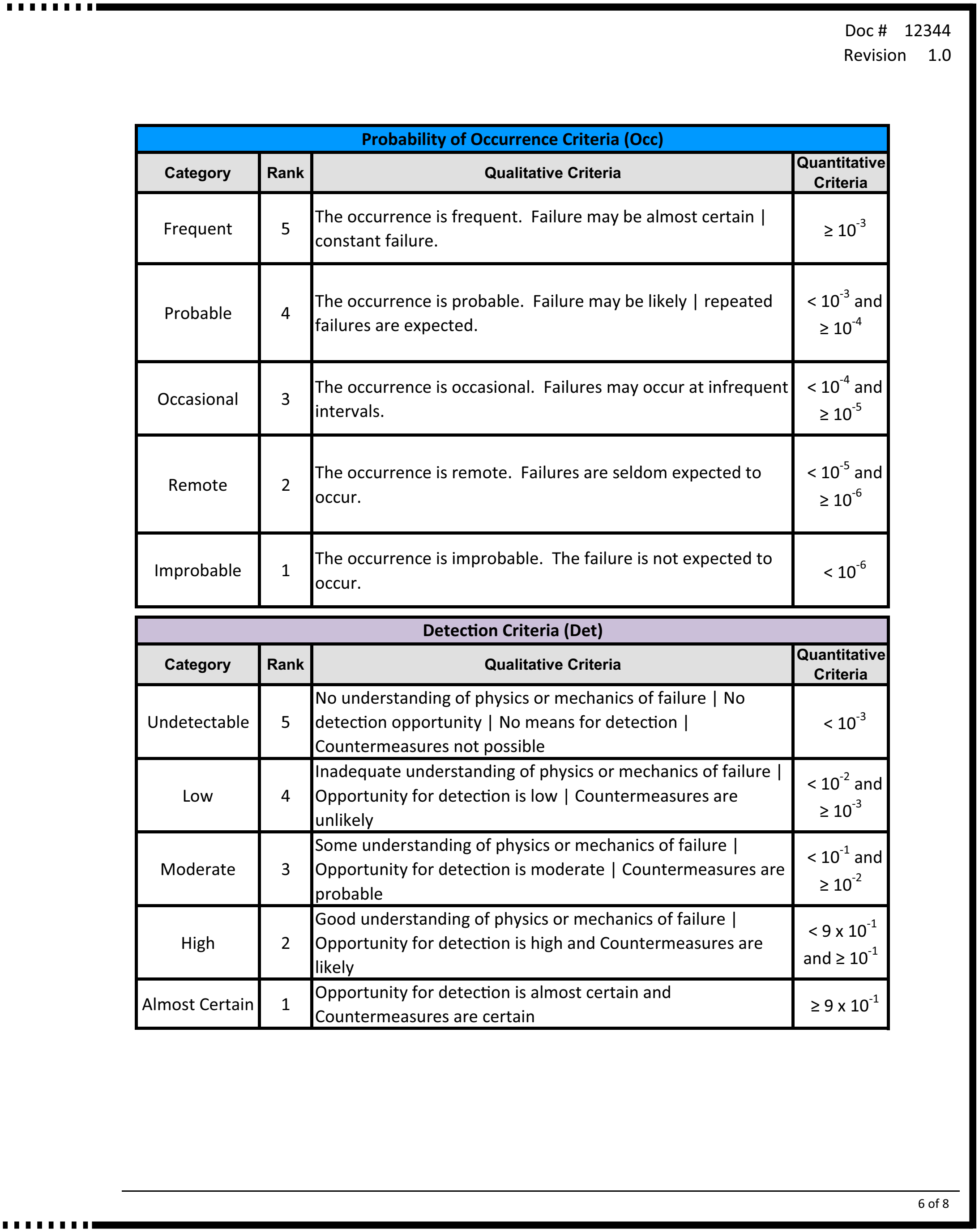
DFMEA
Vivio AED

Severity Criteria (Sev)		
Rank	**Severity Description (No Safety Impact)**	**Severity Description (Safety Impact)**
5	Described failure mode will cause immediate failure of the Subject. (Total loss of all functions – primary and secondary)	**Fatal** – Impact of the end-effect at the System level can be death
4	Described failure mode will severely impact Subject functionality | Complete loss of primary functions. May also lose secondary functions.	**Critical** – Impact of the end-effect at the System level can be permanent impairment or irreversible injury
3	Described failure mode will reduce Subject functionality. (Partial loss of primary functions | Complete loss of secondary functions)	**Major** – Impact of the end-effect at the System level can be injury or impairment requiring medical or surgical intervention
2	Described failure mode will have temporal or self-restoring impact on functionality | partial loss of secondary functions	**Minor** – Impact of the end-effect at the System level can be temporary injury or impairment not requiring medical or surgical intervention
1	Described component failure will have no impact on functionality | Inconvenience to the user	**Negligible** – Impact of the end-effect at the System level can be at most an inconvenience, or temporary discomfort

RPN	Action
53-125	**Level 3 -** Reduce RPN through failure compensating provisions.
13-52	**Level 2** - If Safety Impact is Y, reduce RPN as far as possible. If Safety Impact is N, reduce RPN if feasible.
1-12	**Level 1 -** If Safety Impact is Y, reduce RPN as far as possible. If Safety Impact is N, further RPN reduction is not required.

Y

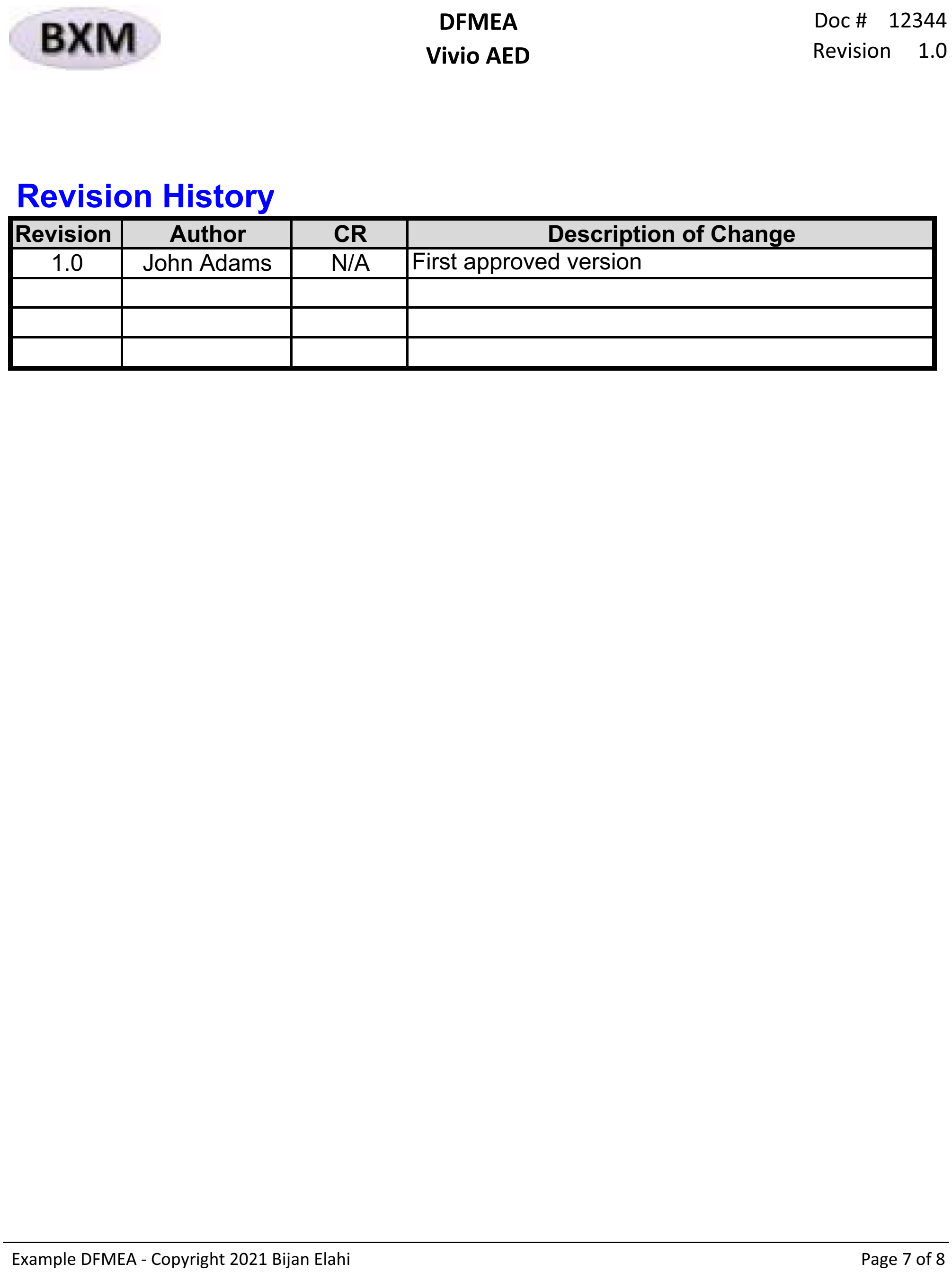
N



Doc # 12344
Revision 1.0

Probability of Occurrence Criteria (Occ)			
Category	Rank	Qualitative Criteria	Quantitative Criteria
Frequent	5	The occurrence is frequent. Failure may be almost certain | constant failure.	≥ 10^{-3}
Probable	4	The occurrence is probable. Failure may be likely | repeated failures are expected.	< 10^{-3} and ≥ 10^{-4}
Occasional	3	The occurrence is occasional. Failures may occur at infrequent intervals.	< 10^{-4} and ≥ 10^{-5}
Remote	2	The occurrence is remote. Failures are seldom expected to occur.	< 10^{-5} and ≥ 10^{-6}
Improbable	1	The occurrence is improbable. The failure is not expected to occur.	< 10^{-6}

Detection Criteria (Det)			
Category	Rank	Qualitative Criteria	Quantitative Criteria
Undetectable	5	No understanding of physics or mechanics of failure | No detection opportunity | No means for detection | Countermeasures not possible	< 10^{-3}
Low	4	Inadequate understanding of physics or mechanics of failure | Opportunity for detection is low | Countermeasures are unlikely	< 10^{-2} and ≥ 10^{-3}
Moderate	3	Some understanding of physics or mechanics of failure | Opportunity for detection is moderate | Countermeasures are probable	< 10^{-1} and ≥ 10^{-2}
High	2	Good understanding of physics or mechanics of failure | Opportunity for detection is high and Countermeasures are likely	< 9 x 10^{-1} and ≥ 10^{-1}
Almost Certain	1	Opportunity for detection is almost certain and Countermeasures are certain	≥ 9 x 10^{-1}



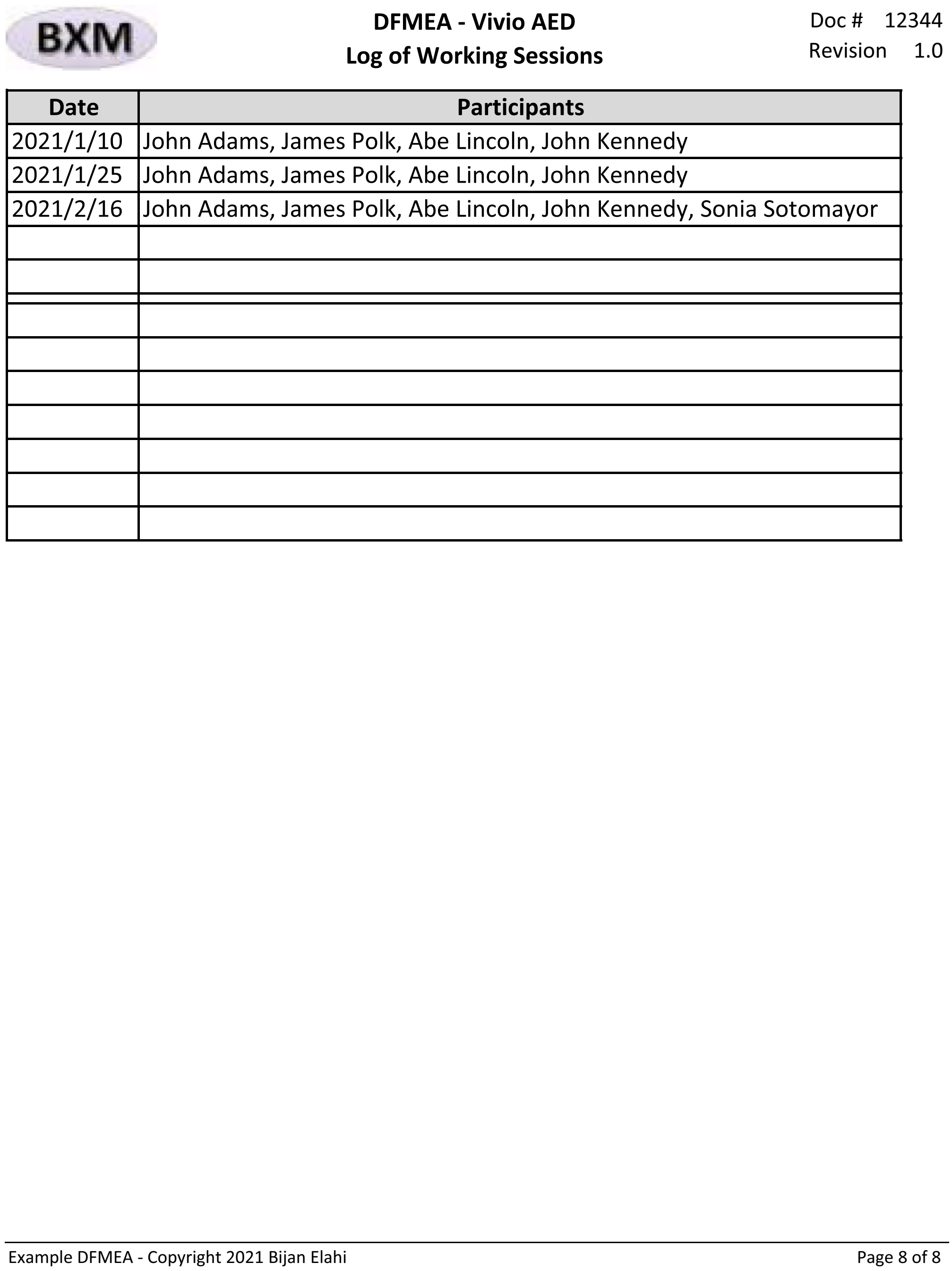
BXM

DFMEA
Vivio AED

Doc # 12344
Revision 1.0

Revision History

Revision	Author	CR	Description of Change
1.0	John Adams	N/A	First approved version



BXM

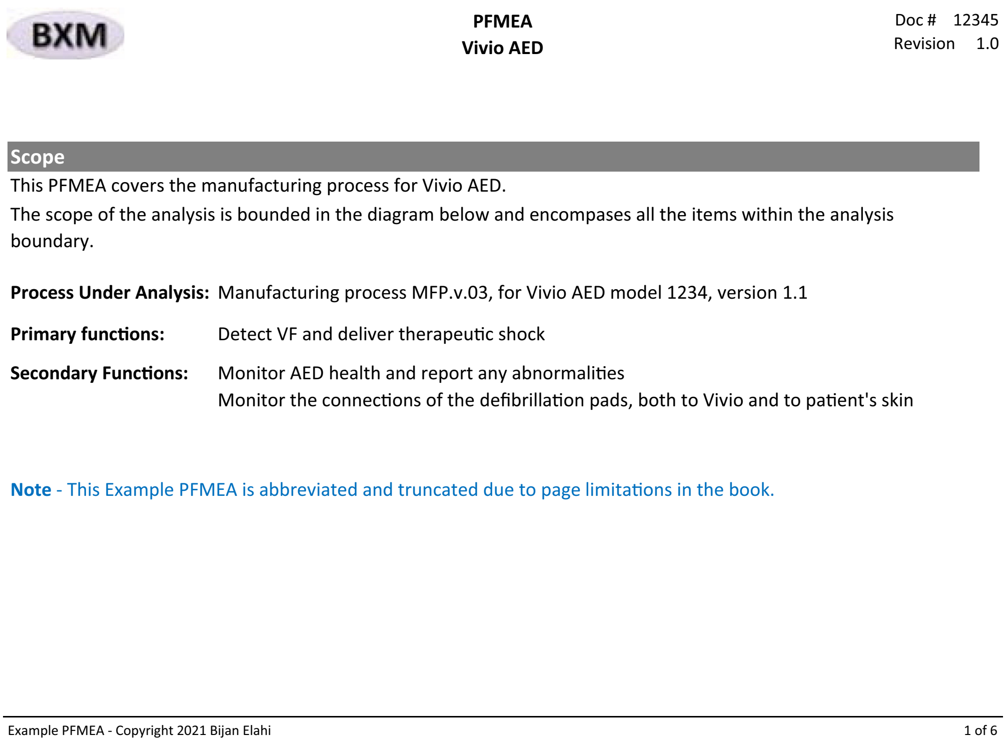
DFMEA - Vivio AED
Log of Working Sessions

Doc # 12344
Revision 1.0

Date	Participants
2021/1/10	John Adams, James Polk, Abe Lincoln, John Kennedy
2021/1/25	John Adams, James Polk, Abe Lincoln, John Kennedy
2021/2/16	John Adams, James Polk, Abe Lincoln, John Kennedy, Sonia Sotomayor

Example DFMEA - Copyright 2021 Bijan Elahi   Page 8 of 8

C.9 PROCESS FAILURE MODES AND EFFECT ANALYSIS



BXM

PFMEA
Vivio AED

Doc # 12345
Revision 1.0

Scope

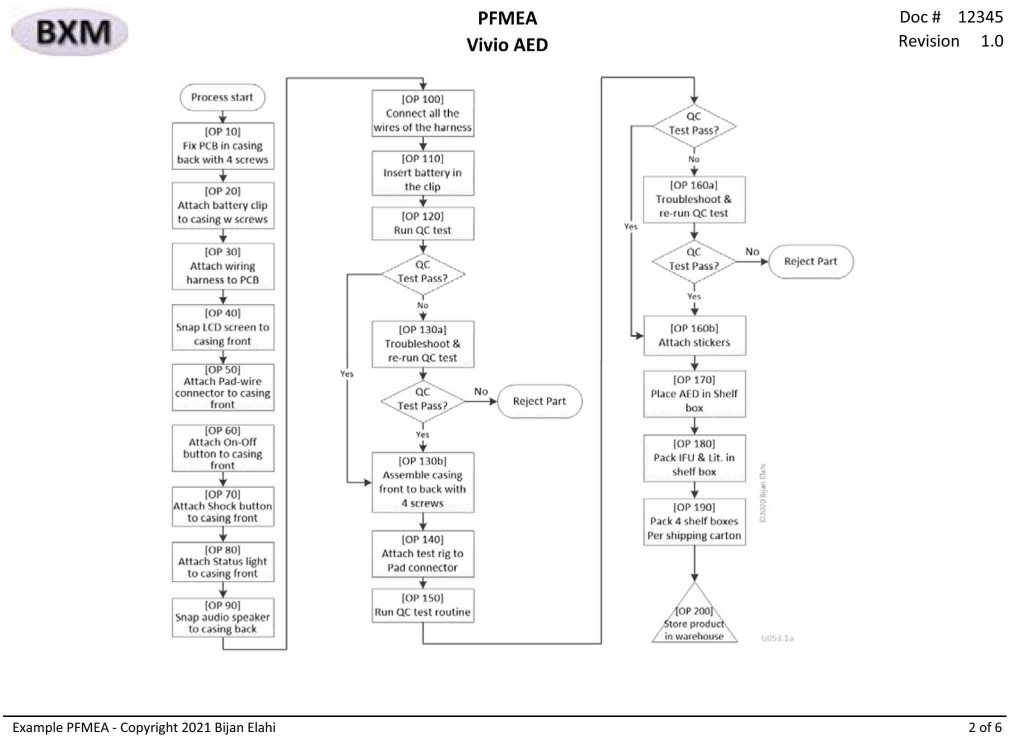
This PFMEA covers the manufacturing process for Vivio AED.

The scope of the analysis is bounded in the diagram below and encompases all the items within the analysis boundary.

Process Under Analysis:	Manufacturing process MFP.v.03, for Vivio AED model 1234, version 1.1
Primary functions:	Detect VF and deliver therapeutic shock
Secondary Functions:	Monitor AED health and report any abnormalities Monitor the connections of the defibrillation pads, both to Vivio and to patient's skin

Note - This Example PFMEA is abbreviated and truncated due to page limitations in the book.

Example PFMEA - Copyright 2021 Bijan Elahi 1 of 6



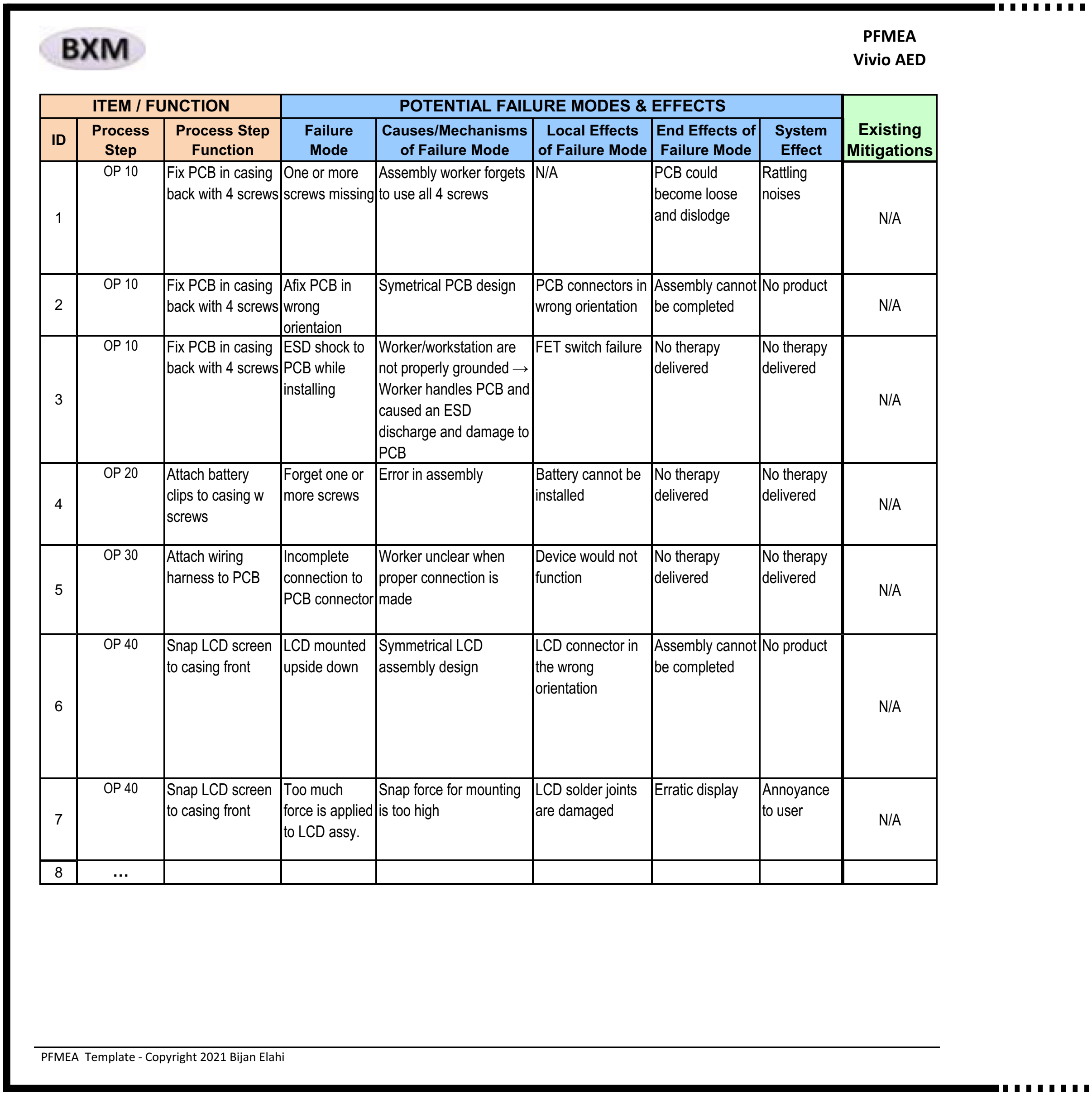
BXM

PFMEA
Vivio AED

Doc # 12345
Revision 1.0

Process start
[OP 10] Fix PCB in casing back with 4 screws
[OP 20] Attach battery clip to casing w screws
[OP 30] Attach wiring harness to PCB
[OP 40] Snap LCD screen to casing front
[OP 50] Attach Pad-wire connector to casing front
[OP 60] Attach On-Off button to casing front
[OP 70] Attach Shock button to casing front
[OP 80] Attach Status light to casing front
[OP 90] Snap audio speaker to casing back
[OP 100] Connect all the wires of the harness
[OP 110] Insert battery in the clip
[OP 120] Run QC test
QC Test Pass?
Yes
No
[OP 130a] Troubleshoot & re-run QC test
QC Test Pass?
No
Reject Part
Yes
[OP 130b] Assemble casing front to back with 4 screws
[OP 140] Attach test rig to Pad connector
[OP 150] Run QC test routine
QC Test Pass?
Yes
No
[OP 160a] Troubleshoot & re-run QC test
QC Test Pass?
No
Reject Part
Yes
[OP 160b] Attach stickers
[OP 170] Place AED in Shelf box
[OP 180] Pack IFU & Lit. in shelf box
[OP 190] Pack 4 shelf boxes Per shipping carton
[OP 200] Store product in warehouse
©2020 Bijan Elahi
G053.1a

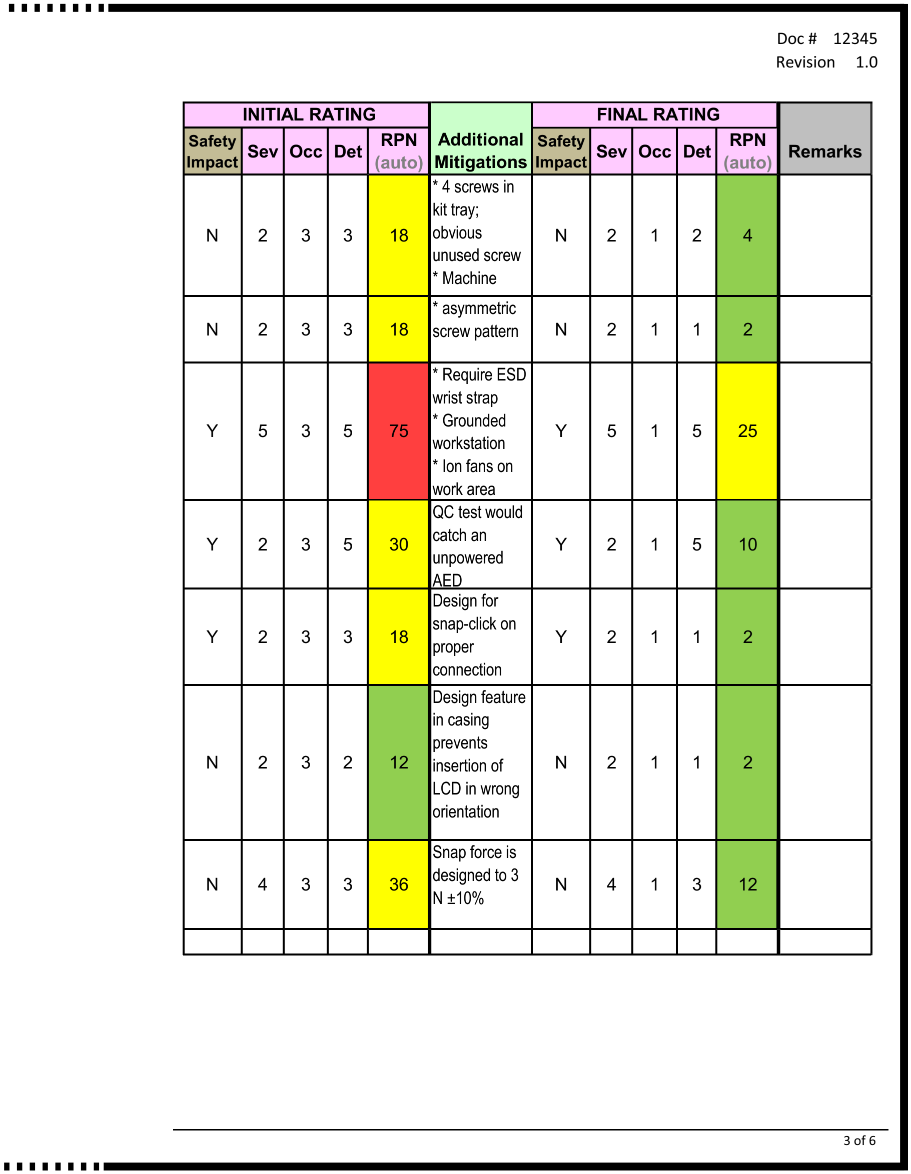
Example PFMEA - Copyright 2021 Bijan Elahi 2 of 6



PFMEA
Vivio AED

ITEM / FUNCTION			POTENTIAL FAILURE MODES & EFFECTS					
ID	Process Step	Process Step Function	Failure Mode	Causes/Mechanisms of Failure Mode	Local Effects of Failure Mode	End Effects of Failure Mode	System Effect	Existing Mitigations
1	OP 10	Fix PCB in casing back with 4 screws	One or more screws missing	Assembly worker forgets to use all 4 screws	N/A	PCB could become loose and dislodge	Rattling noises	N/A
2	OP 10	Fix PCB in casing back with 4 screws	Afix PCB in wrong orientaion	Symetrical PCB design	PCB connectors in wrong orientation	Assembly cannot be completed	No product	N/A
3	OP 10	Fix PCB in casing back with 4 screws	ESD shock to PCB while installing	Worker/workstation are not properly grounded → Worker handles PCB and caused an ESD discharge and damage to PCB	FET switch failure	No therapy delivered	No therapy delivered	N/A
4	OP 20	Attach battery clips to casing w screws	Forget one or more screws	Error in assembly	Battery cannot be installed	No therapy delivered	No therapy delivered	N/A
5	OP 30	Attach wiring harness to PCB	Incomplete connection to PCB connector	Worker unclear when proper connection is made	Device would not function	No therapy delivered	No therapy delivered	N/A
6	OP 40	Snap LCD screen to casing front	LCD mounted upside down	Symmetrical LCD assembly design	LCD connector in the wrong orientation	Assembly cannot be completed	No product	N/A
7	OP 40	Snap LCD screen to casing front	Too much force is applied to LCD assy.	Snap force for mounting is too high	LCD solder joints are damaged	Erratic display	Annoyance to user	N/A
8	...							

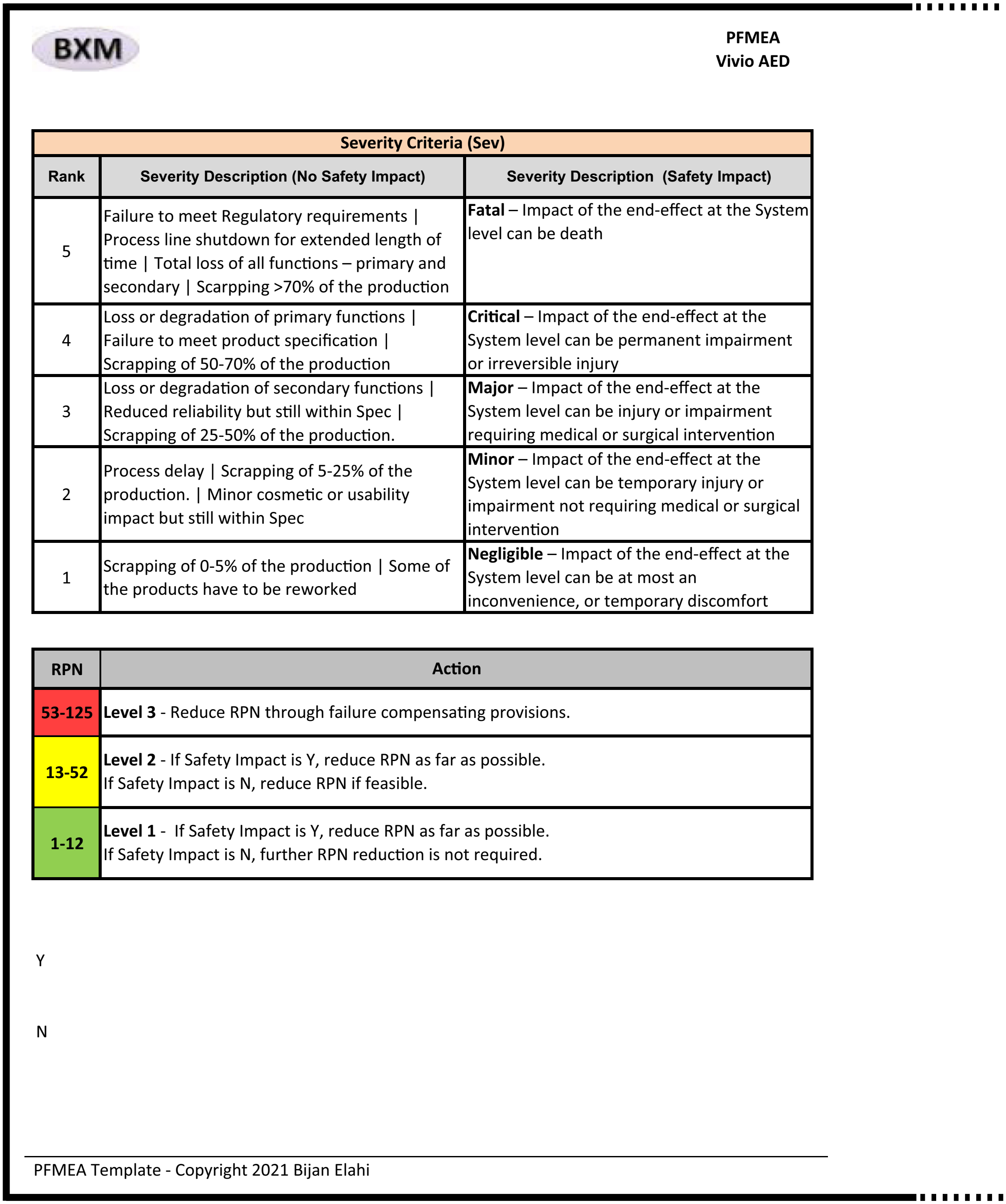
PFMEA Template - Copyright 2021 Bijan Elahi



Doc # 12345
Revision 1.0

INITIAL RATING						FINAL RATING					
Safety Impact	Sev	Occ	Det	RPN (auto)	Additional Mitigations	Safety Impact	Sev	Occ	Det	RPN (auto)	Remarks
N	2	3	3	18	* 4 screws in kit tray; obvious unused screw * Machine	N	2	1	2	4	
N	2	3	3	18	* asymmetric screw pattern	N	2	1	1	2	
Y	5	3	5	75	* Require ESD wrist strap * Grounded workstation * Ion fans on work area	Y	5	1	5	25	
Y	2	3	5	30	QC test would catch an unpowered AED	Y	2	1	5	10	
Y	2	3	3	18	Design for snap-click on proper connection	Y	2	1	1	2	
N	2	3	2	12	Design feature in casing prevents insertion of LCD in wrong orientation	N	2	1	1	2	
N	4	3	3	36	Snap force is designed to 3 N ±10%	N	4	1	3	12	

3 of 6



BXM

PFMEA
Vivio AED

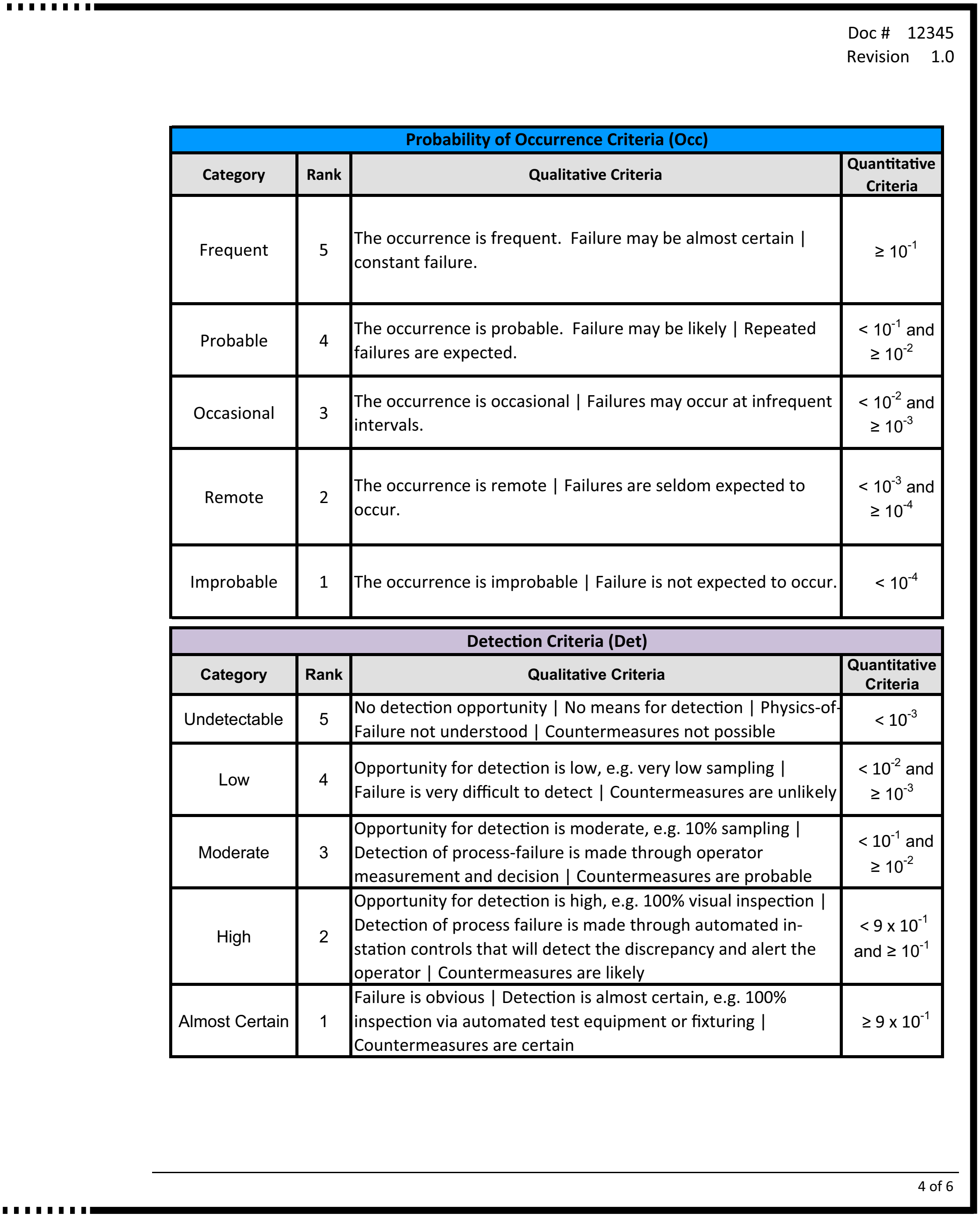
Severity Criteria (Sev)		
Rank	Severity Description (No Safety Impact)	Severity Description (Safety Impact)
5	Failure to meet Regulatory requirements | Process line shutdown for extended length of time | Total loss of all functions – primary and secondary | Scarpping >70% of the production	**Fatal** – Impact of the end-effect at the System level can be death
4	Loss or degradation of primary functions | Failure to meet product specification | Scrapping of 50-70% of the production	**Critical** – Impact of the end-effect at the System level can be permanent impairment or irreversible injury
3	Loss or degradation of secondary functions | Reduced reliability but still within Spec | Scrapping of 25-50% of the production.	**Major** – Impact of the end-effect at the System level can be injury or impairment requiring medical or surgical intervention
2	Process delay | Scrapping of 5-25% of the production. | Minor cosmetic or usability impact but still within Spec	**Minor** – Impact of the end-effect at the System level can be temporary injury or impairment not requiring medical or surgical intervention
1	Scrapping of 0-5% of the production | Some of the products have to be reworked	**Negligible** – Impact of the end-effect at the System level can be at most an inconvenience, or temporary discomfort

RPN	Action
53-125	**Level 3** - Reduce RPN through failure compensating provisions.
13-52	**Level 2** - If Safety Impact is Y, reduce RPN as far as possible. If Safety Impact is N, reduce RPN if feasible.
1-12	**Level 1** - If Safety Impact is Y, reduce RPN as far as possible. If Safety Impact is N, further RPN reduction is not required.

Y

N

PFMEA Template - Copyright 2021 Bijan Elahi



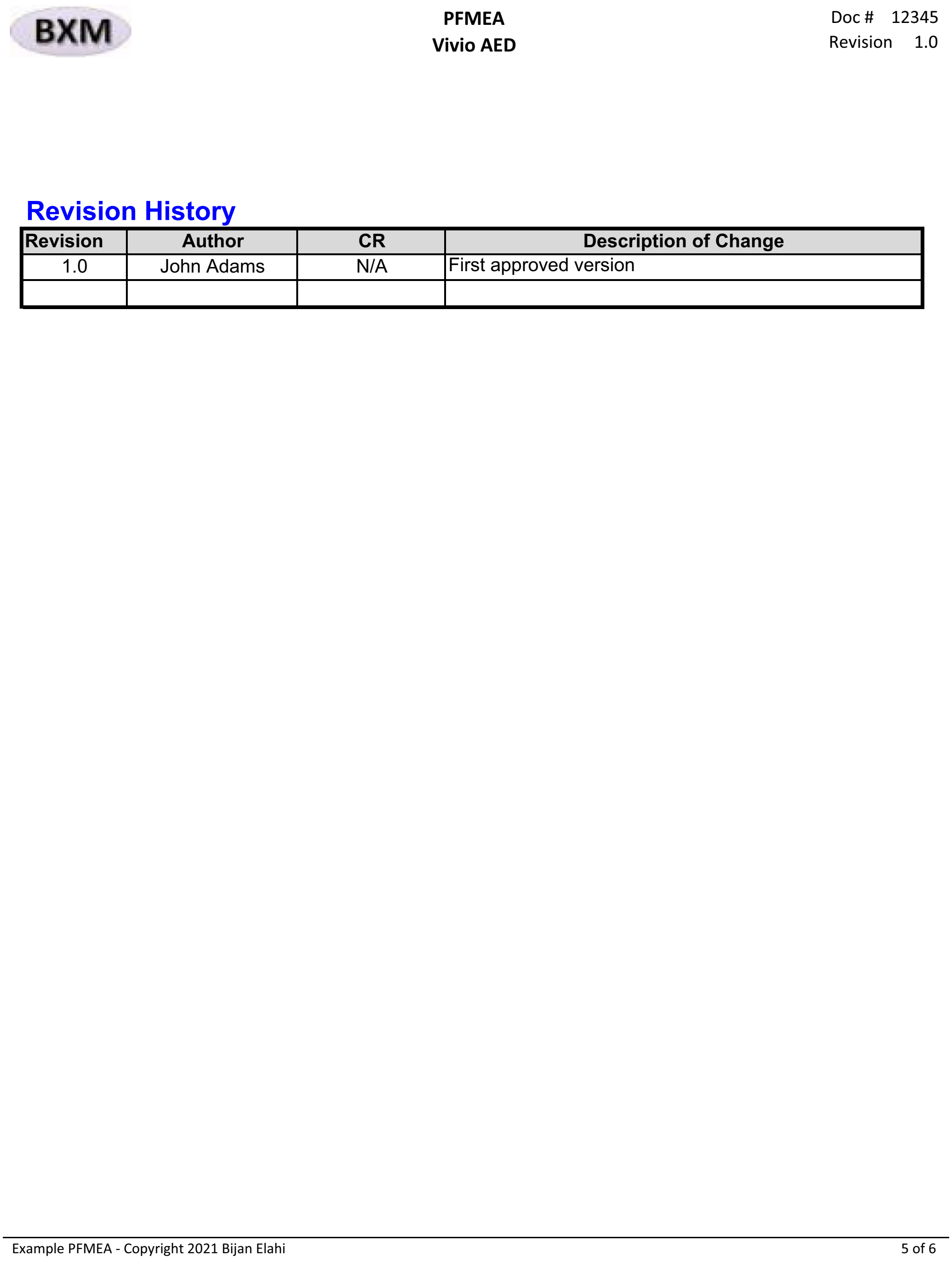
Doc # 12345
Revision 1.0

Probability of Occurrence Criteria (Occ)

Category	Rank	Qualitative Criteria	Quantitative Criteria
Frequent	5	The occurrence is frequent. Failure may be almost certain | constant failure.	≥ 10^{-1}
Probable	4	The occurrence is probable. Failure may be likely | Repeated failures are expected.	< 10^{-1} and ≥ 10^{-2}
Occasional	3	The occurrence is occasional | Failures may occur at infrequent intervals.	< 10^{-2} and ≥ 10^{-3}
Remote	2	The occurrence is remote | Failures are seldom expected to occur.	< 10^{-3} and ≥ 10^{-4}
Improbable	1	The occurrence is improbable | Failure is not expected to occur.	< 10^{-4}

Detection Criteria (Det)

Category	Rank	Qualitative Criteria	Quantitative Criteria
Undetectable	5	No detection opportunity | No means for detection | Physics-of-Failure not understood | Countermeasures not possible	< 10^{-3}
Low	4	Opportunity for detection is low, e.g. very low sampling | Failure is very difficult to detect | Countermeasures are unlikely	< 10^{-2} and ≥ 10^{-3}
Moderate	3	Opportunity for detection is moderate, e.g. 10% sampling | Detection of process-failure is made through operator measurement and decision | Countermeasures are probable	< 10^{-1} and ≥ 10^{-2}
High	2	Opportunity for detection is high, e.g. 100% visual inspection | Detection of process failure is made through automated in-station controls that will detect the discrepancy and alert the operator | Countermeasures are likely	< 9 x 10^{-1} and ≥ 10^{-1}
Almost Certain	1	Failure is obvious | Detection is almost certain, e.g. 100% inspection via automated test equipment or fixturing | Countermeasures are certain	≥ 9 x 10^{-1}



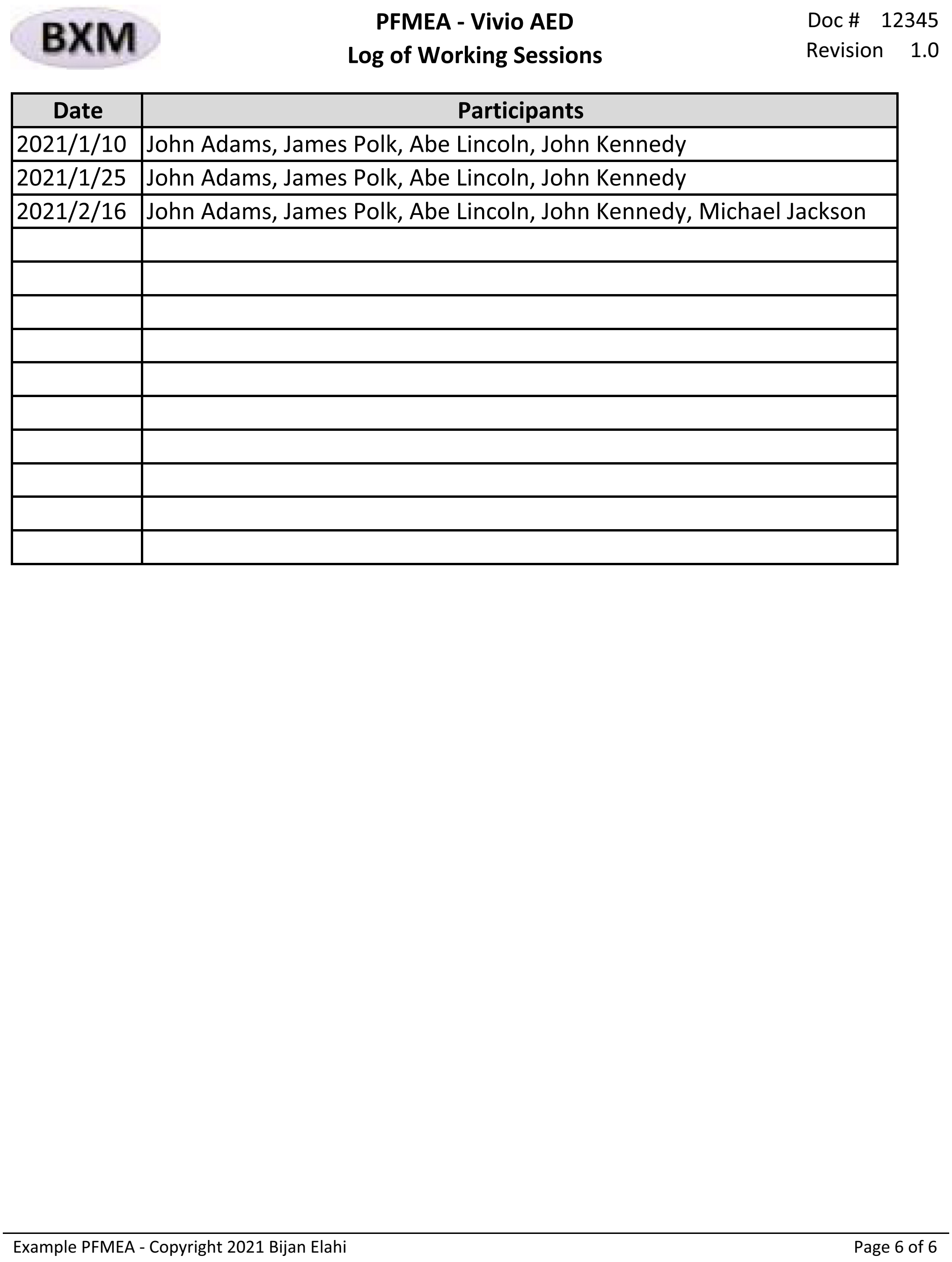
BXM

PFMEA
Vivio AED

Doc # 12345
Revision 1.0

Revision History

Revision	Author	CR	Description of Change
1.0	John Adams	N/A	First approved version



BXM

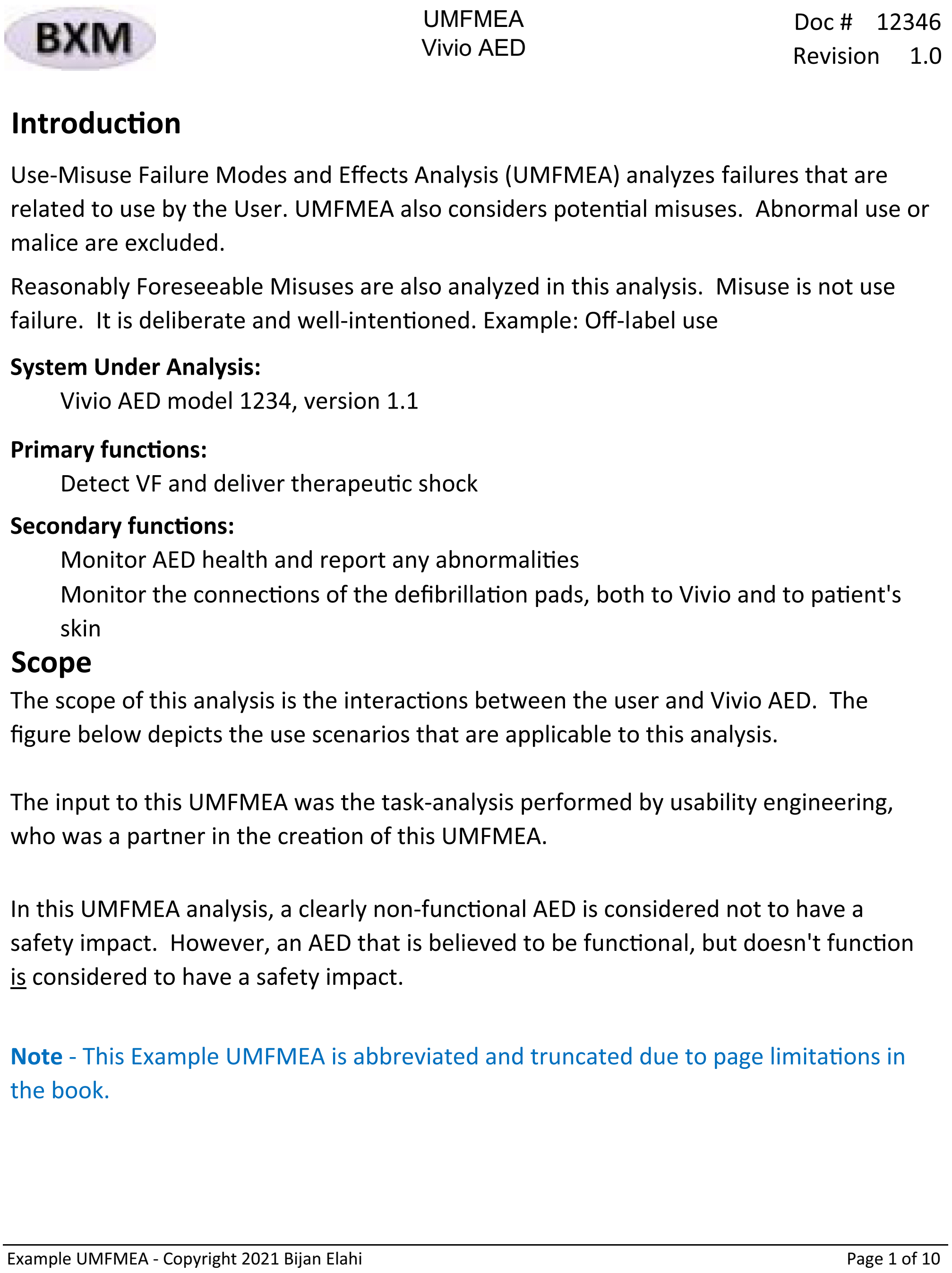
PFMEA - Vivio AED
Log of Working Sessions

Doc # 12345
Revision 1.0

Date	Participants
2021/1/10	John Adams, James Polk, Abe Lincoln, John Kennedy
2021/1/25	John Adams, James Polk, Abe Lincoln, John Kennedy
2021/2/16	John Adams, James Polk, Abe Lincoln, John Kennedy, Michael Jackson

Example PFMEA - Copyright 2021 Bijan Elahi Page 6 of 6

C.10 USE/MISUSE FAILURE MODES AND EFFECTS ANALYSIS



BXM

UMFMEA
Vivio AED

Doc # 12346
Revision 1.0

Introduction

Use-Misuse Failure Modes and Effects Analysis (UMFMEA) analyzes failures that are related to use by the User. UMFMEA also considers potential misuses. Abnormal use or malice are excluded.

Reasonably Foreseeable Misuses are also analyzed in this analysis. Misuse is not use failure. It is deliberate and well-intentioned. Example: Off-label use

System Under Analysis:

Vivio AED model 1234, version 1.1

Primary functions:

Detect VF and deliver therapeutic shock

Secondary functions:

Monitor AED health and report any abnormalities

Monitor the connections of the defibrillation pads, both to Vivio and to patient's skin

Scope

The scope of this analysis is the interactions between the user and Vivio AED. The figure below depicts the use scenarios that are applicable to this analysis.

The input to this UMFMEA was the task-analysis performed by usability engineering, who was a partner in the creation of this UMFMEA.

In this UMFMEA analysis, a clearly non-functional AED is considered not to have a safety impact. However, an AED that is believed to be functional, but doesn't function is considered to have a safety impact.

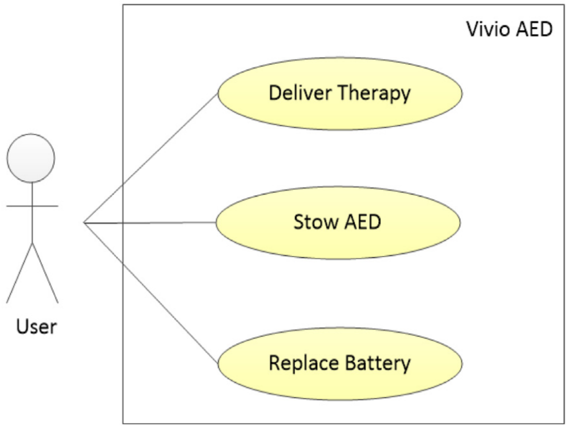
Note - This Example UMFMEA is abbreviated and truncated due to page limitations in the book.

Example UMFMEA - Copyright 2021 Bijan Elahi   Page 1 of 10

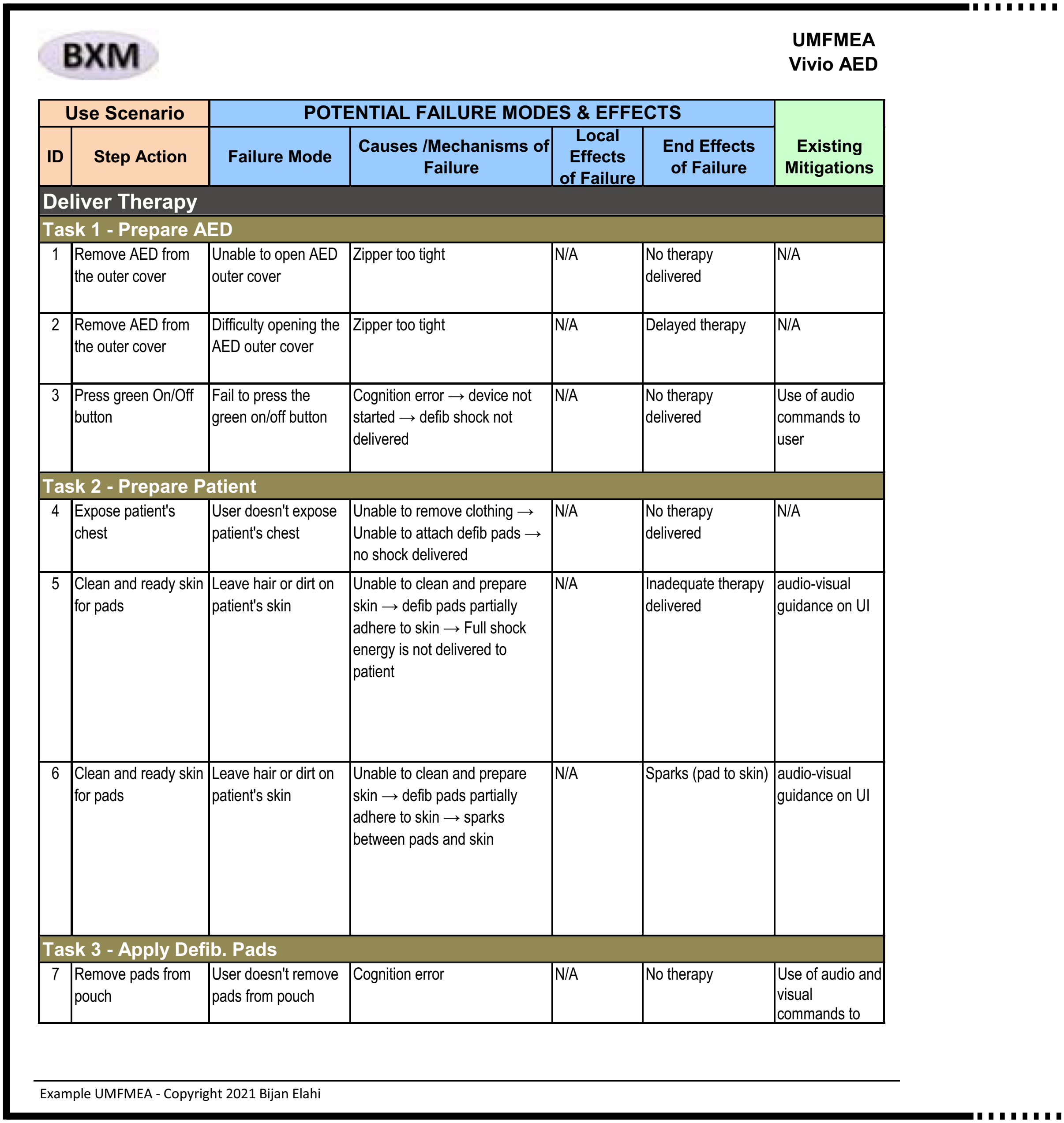
BXM

UMFMEA
Vivio AED

Doc # 12346
Revision 1.0



Vivio AED Use Scenarios

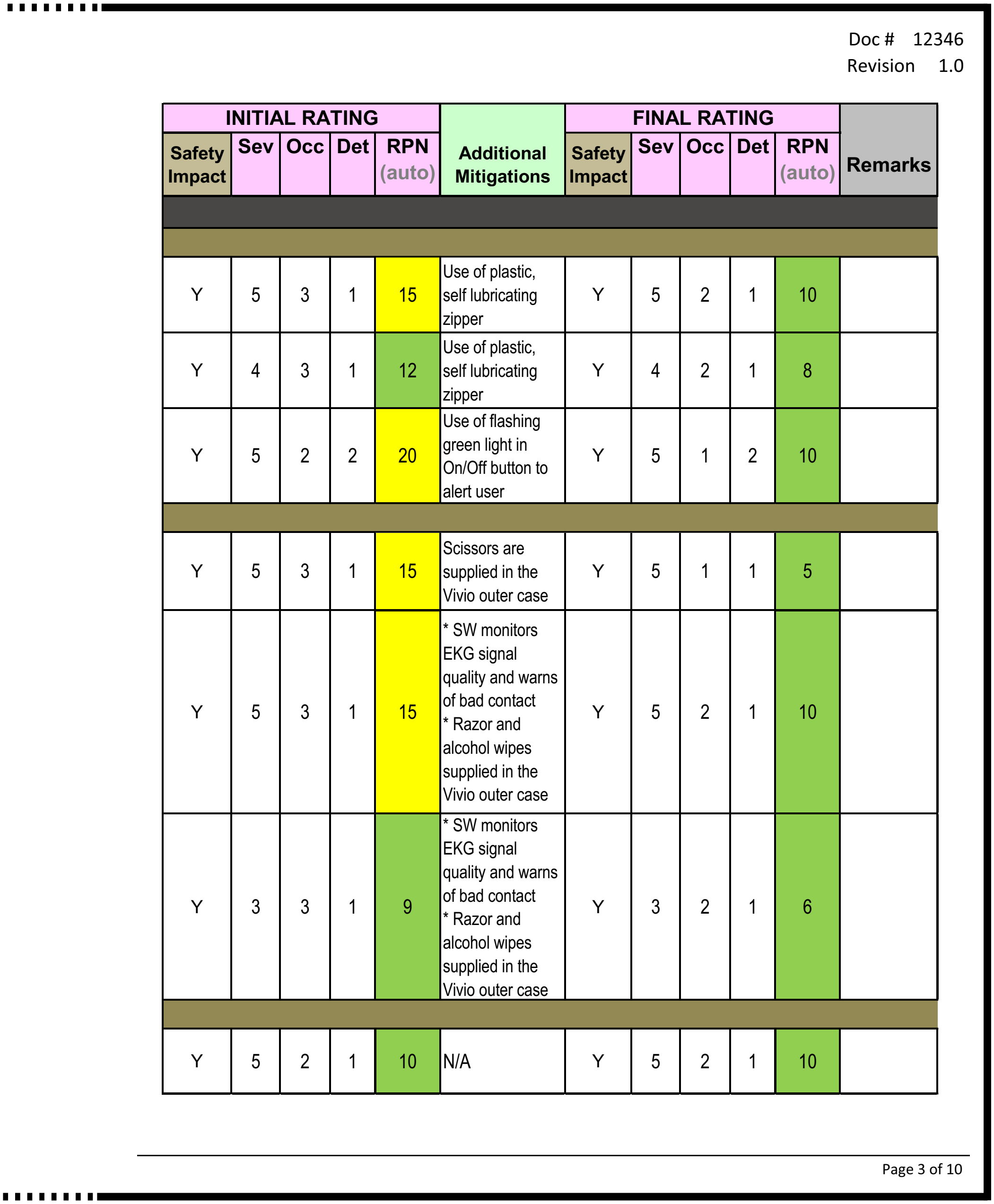


BXM

UMFMEA
Vivio AED

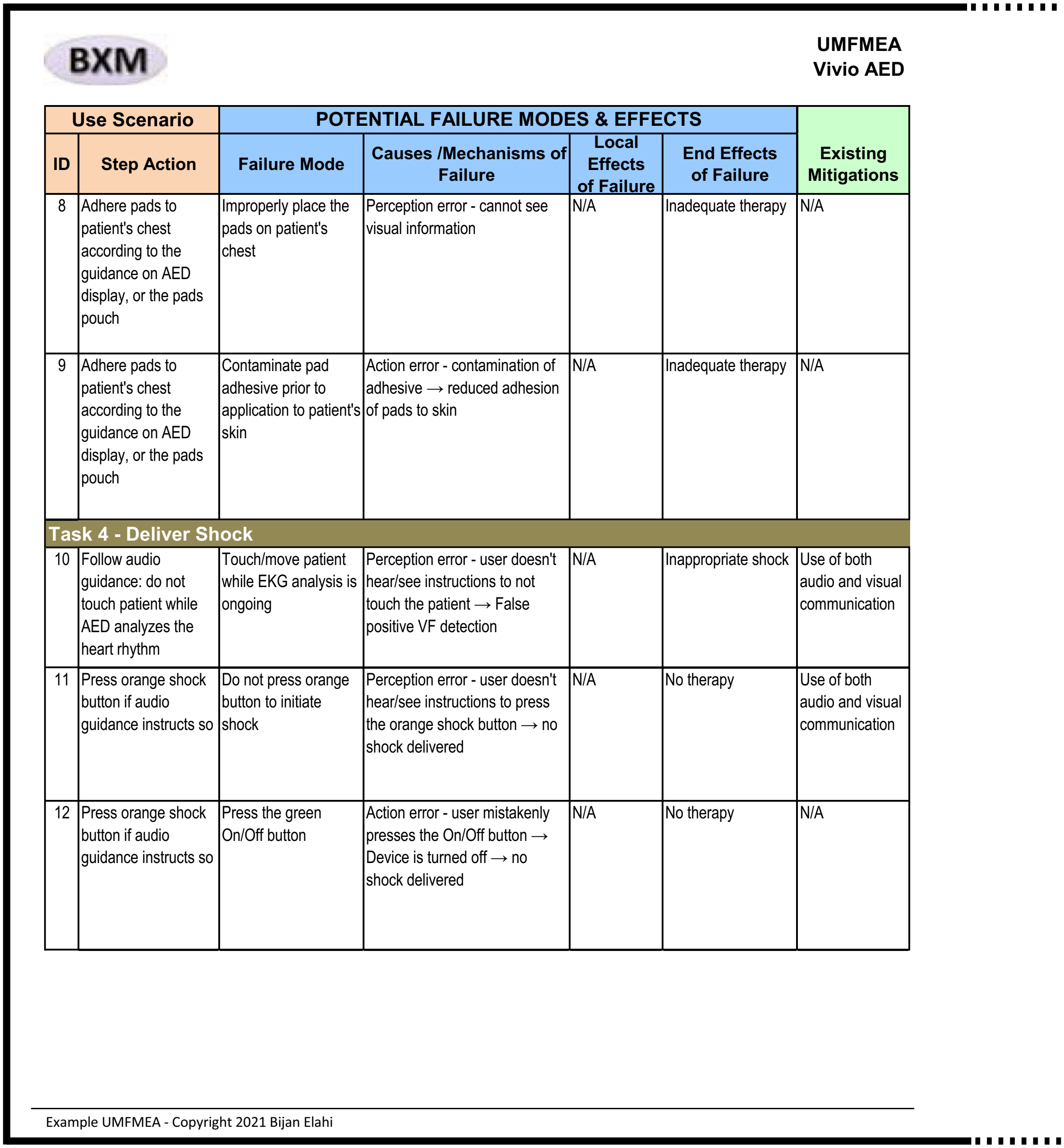
Use Scenario		POTENTIAL FAILURE MODES & EFFECTS				
ID	**Step Action**	**Failure Mode**	**Causes /Mechanisms of Failure**	**Local Effects of Failure**	**End Effects of Failure**	**Existing Mitigations**
Deliver Therapy						
Task 1 - Prepare AED						
1	Remove AED from the outer cover	Unable to open AED outer cover	Zipper too tight	N/A	No therapy delivered	N/A
2	Remove AED from the outer cover	Difficulty opening the AED outer cover	Zipper too tight	N/A	Delayed therapy	N/A
3	Press green On/Off button	Fail to press the green on/off button	Cognition error → device not started → defib shock not delivered	N/A	No therapy delivered	Use of audio commands to user
Task 2 - Prepare Patient						
4	Expose patient's chest	User doesn't expose patient's chest	Unable to remove clothing → Unable to attach defib pads → no shock delivered	N/A	No therapy delivered	N/A
5	Clean and ready skin for pads	Leave hair or dirt on patient's skin	Unable to clean and prepare skin → defib pads partially adhere to skin → Full shock energy is not delivered to patient	N/A	Inadequate therapy delivered	audio-visual guidance on UI
6	Clean and ready skin for pads	Leave hair or dirt on patient's skin	Unable to clean and prepare skin → defib pads partially adhere to skin → sparks between pads and skin	N/A	Sparks (pad to skin)	audio-visual guidance on UI
Task 3 - Apply Defib. Pads						
7	Remove pads from pouch	User doesn't remove pads from pouch	Cognition error	N/A	No therapy	Use of audio and visual commands to

Example UMFMEA - Copyright 2021 Bijan Elahi



Doc # 12346
Revision 1.0

INITIAL RATING					Additional Mitigations	FINAL RATING					Remarks
Safety Impact	Sev	Occ	Det	RPN (auto)		Safety Impact	Sev	Occ	Det	RPN (auto)	
Y	5	3	1	15	Use of plastic, self lubricating zipper	Y	5	2	1	10	
Y	4	3	1	12	Use of plastic, self lubricating zipper	Y	4	2	1	8	
Y	5	2	2	20	Use of flashing green light in On/Off button to alert user	Y	5	1	2	10	
Y	5	3	1	15	Scissors are supplied in the Vivio outer case	Y	5	1	1	5	
Y	5	3	1	15	* SW monitors EKG signal quality and warns of bad contact * Razor and alcohol wipes supplied in the Vivio outer case	Y	5	2	1	10	
Y	3	3	1	9	* SW monitors EKG signal quality and warns of bad contact * Razor and alcohol wipes supplied in the Vivio outer case	Y	3	2	1	6	
Y	5	2	1	10	N/A	Y	5	2	1	10	

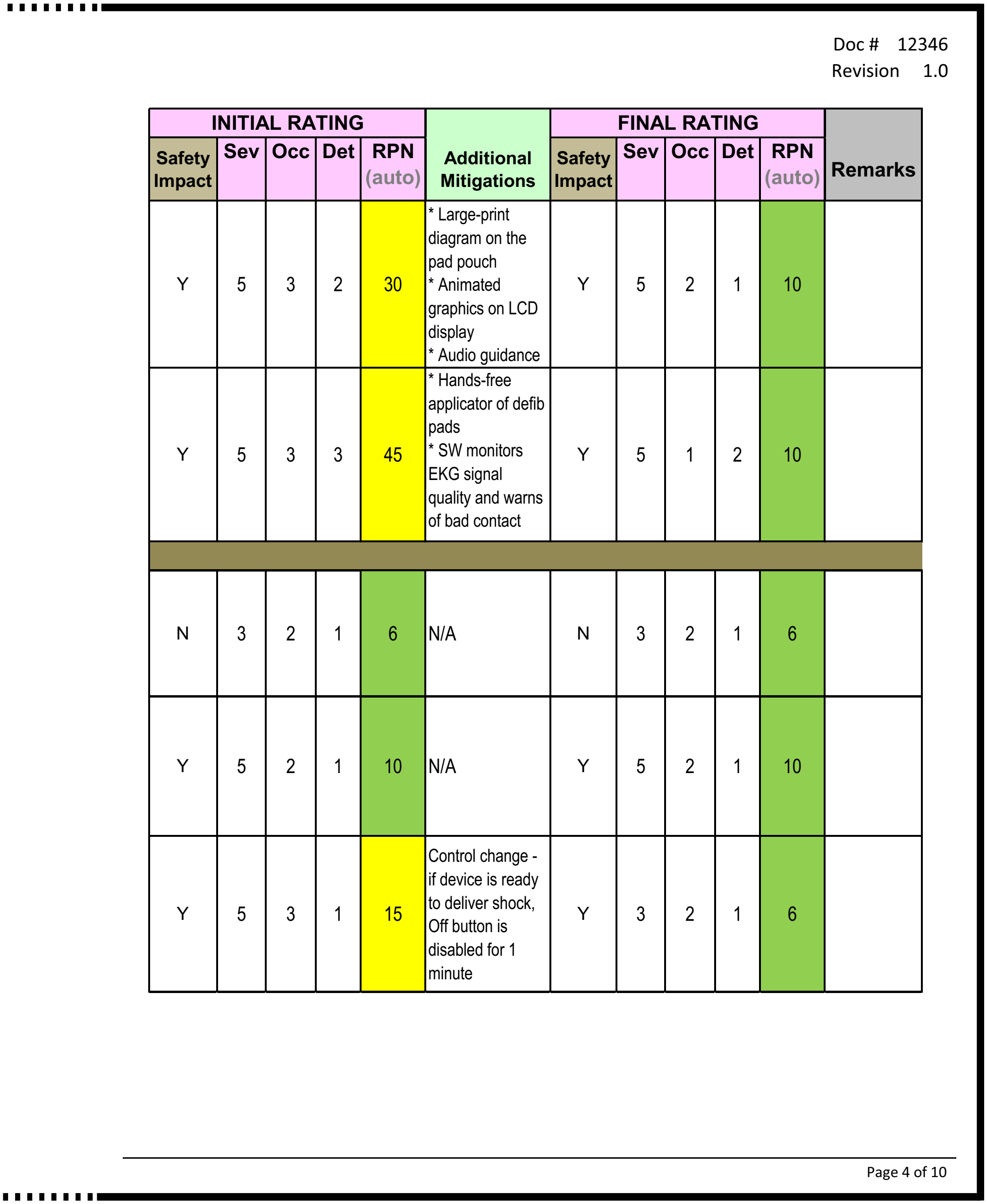


BXM

UMFMEA
Vivio AED

Use Scenario		POTENTIAL FAILURE MODES & EFFECTS				
ID	**Step Action**	**Failure Mode**	**Causes /Mechanisms of Failure**	**Local Effects of Failure**	**End Effects of Failure**	**Existing Mitigations**
8	Adhere pads to patient's chest according to the guidance on AED display, or the pads pouch	Improperly place the pads on patient's chest	Perception error - cannot see visual information	N/A	Inadequate therapy	N/A
9	Adhere pads to patient's chest according to the guidance on AED display, or the pads pouch	Contaminate pad adhesive prior to application to patient's skin	Action error - contamination of adhesive → reduced adhesion of pads to skin	N/A	Inadequate therapy	N/A
Task 4 - Deliver Shock						
10	Follow audio guidance: do not touch patient while AED analyzes the heart rhythm	Touch/move patient while EKG analysis is ongoing	Perception error - user doesn't hear/see instructions to not touch the patient → False positive VF detection	N/A	Inappropriate shock	Use of both audio and visual communication
11	Press orange shock button if audio guidance instructs so	Do not press orange button to initiate shock	Perception error - user doesn't hear/see instructions to press the orange shock button → no shock delivered	N/A	No therapy	Use of both audio and visual communication
12	Press orange shock button if audio guidance instructs so	Press the green On/Off button	Action error - user mistakenly presses the On/Off button → Device is turned off → no shock delivered	N/A	No therapy	N/A

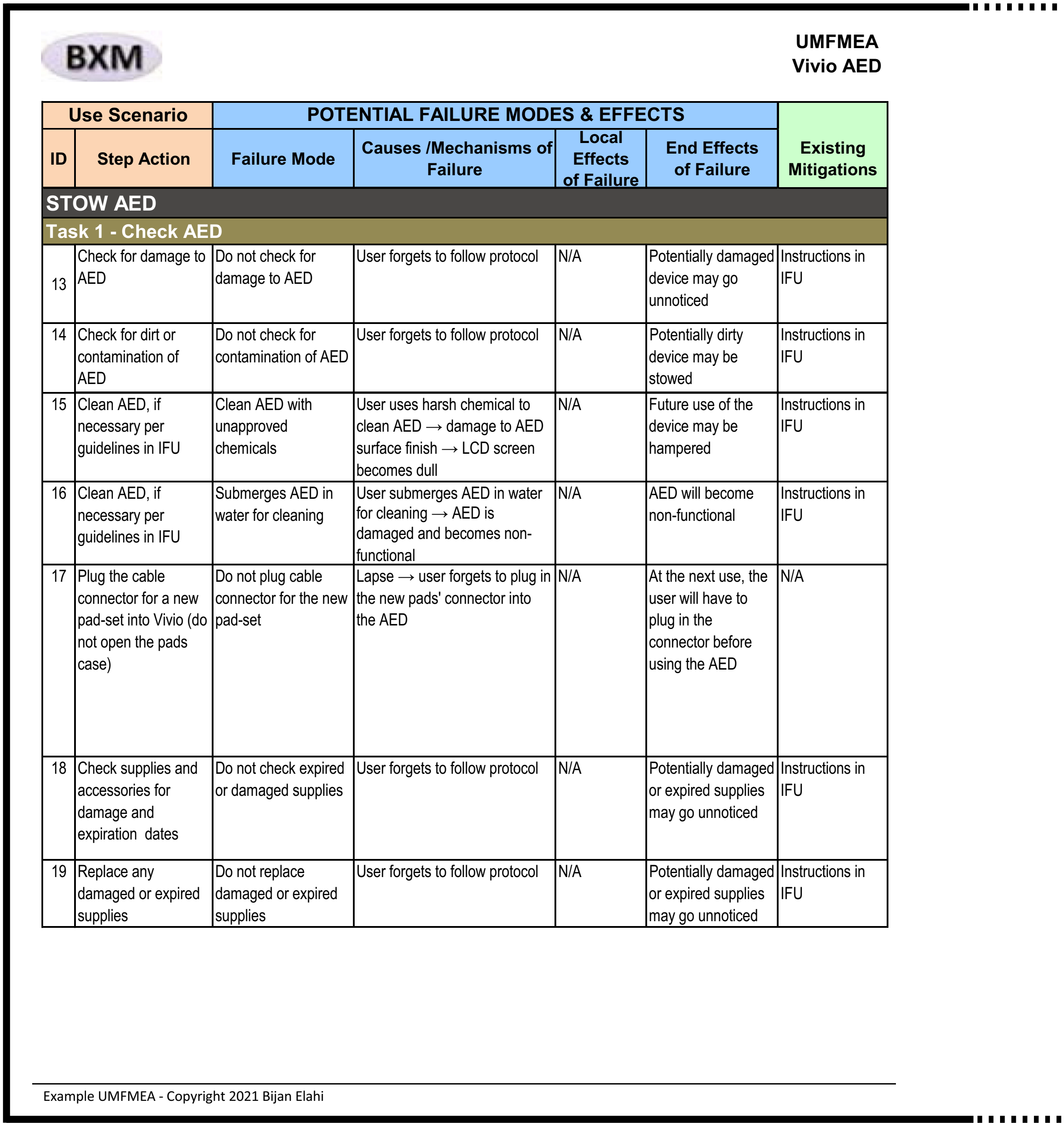
Example UMFMEA - Copyright 2021 Bijan Elahi



Doc # 12346
Revision 1.0

INITIAL RATING						FINAL RATING					
Safety Impact	Sev	Occ	Det	RPN (auto)	Additional Mitigations	Safety Impact	Sev	Occ	Det	RPN (auto)	Remarks
Y	5	3	2	30	* Large-print diagram on the pad pouch * Animated graphics on LCD display * Audio guidance	Y	5	2	1	10	
Y	5	3	3	45	* Hands-free applicator of defib pads * SW monitors EKG signal quality and warns of bad contact	Y	5	1	2	10	
N	3	2	1	6	N/A	N	3	2	1	6	
Y	5	2	1	10	N/A	Y	5	2	1	10	
Y	5	3	1	15	Control change - if device is ready to deliver shock, Off button is disabled for 1 minute	Y	3	2	1	6	

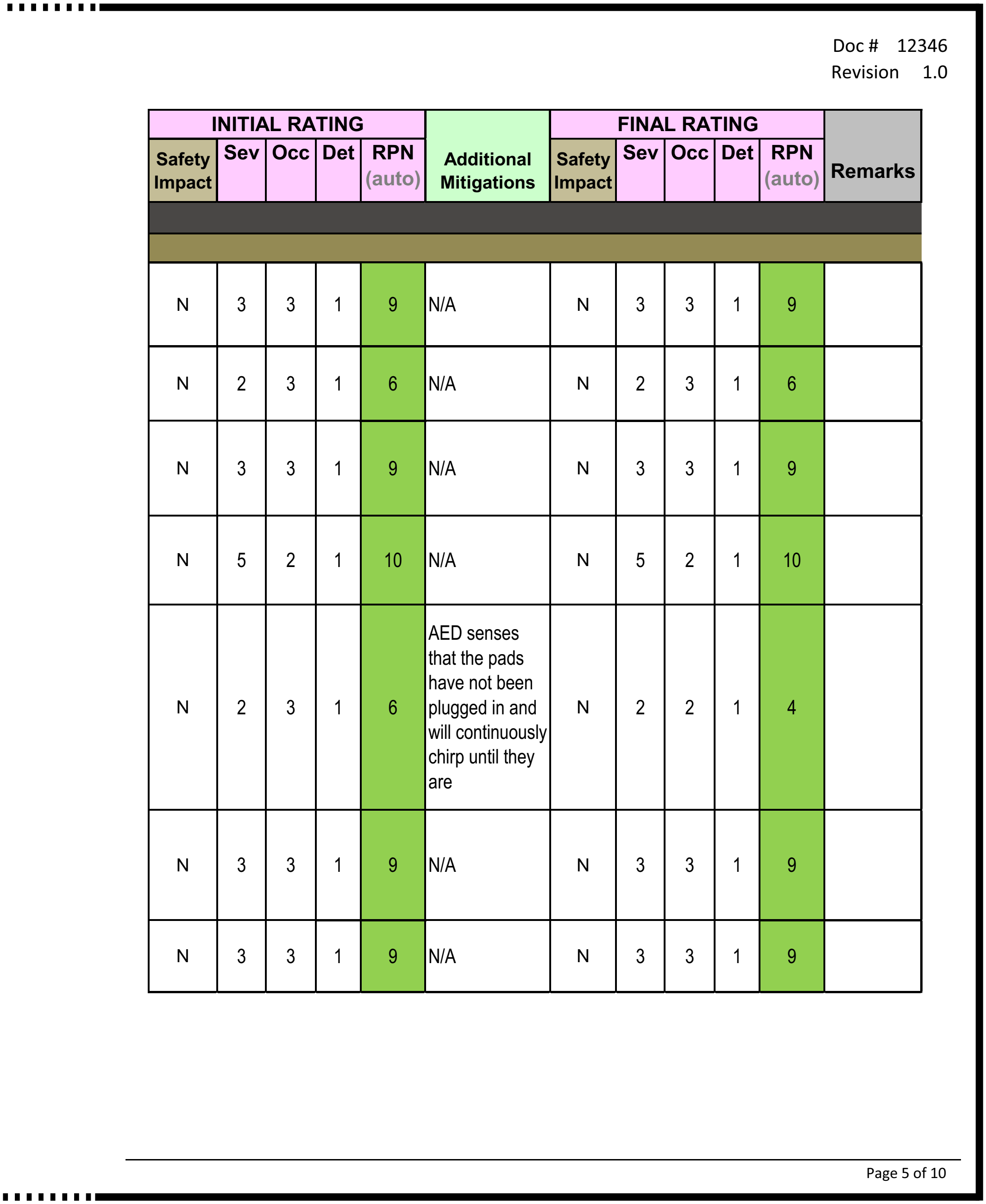
Page 4 of 10



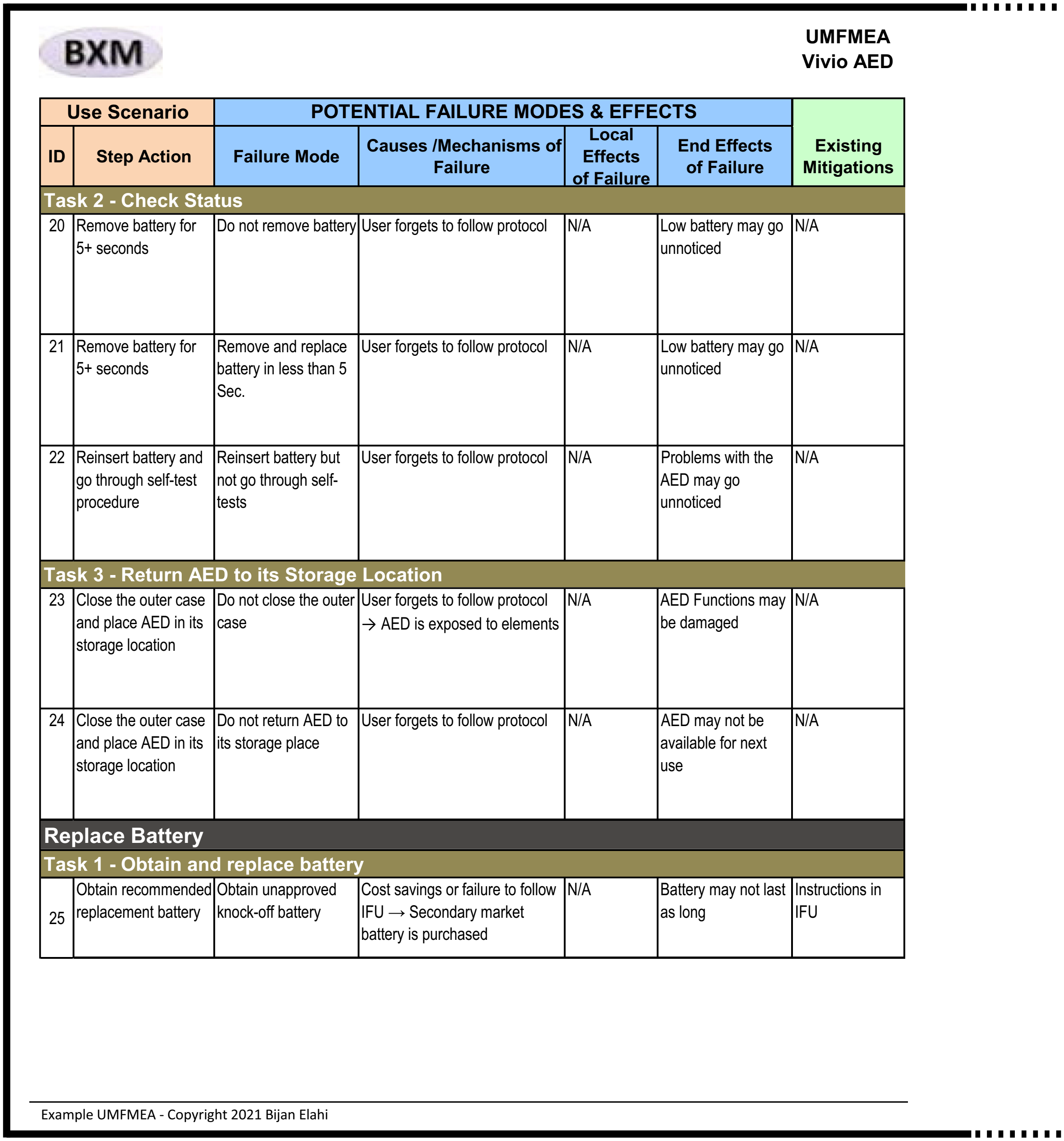
BXM

UMFMEA
Vivio AED

Use Scenario		POTENTIAL FAILURE MODES & EFFECTS				
ID	Step Action	Failure Mode	Causes /Mechanisms of Failure	Local Effects of Failure	End Effects of Failure	Existing Mitigations
STOW AED						
Task 1 - Check AED						
13	Check for damage to AED	Do not check for damage to AED	User forgets to follow protocol	N/A	Potentially damaged device may go unnoticed	Instructions in IFU
14	Check for dirt or contamination of AED	Do not check for contamination of AED	User forgets to follow protocol	N/A	Potentially dirty device may be stowed	Instructions in IFU
15	Clean AED, if necessary per guidelines in IFU	Clean AED with unapproved chemicals	User uses harsh chemical to clean AED → damage to AED surface finish → LCD screen becomes dull	N/A	Future use of the device may be hampered	Instructions in IFU
16	Clean AED, if necessary per guidelines in IFU	Submerges AED in water for cleaning	User submerges AED in water for cleaning → AED is damaged and becomes non-functional	N/A	AED will become non-functional	Instructions in IFU
17	Plug the cable connector for a new pad-set into Vivio (do not open the pads case)	Do not plug cable connector for the new pad-set	Lapse → user forgets to plug in the new pads' connector into the AED	N/A	At the next use, the user will have to plug in the connector before using the AED	N/A
18	Check supplies and accessories for damage and expiration dates	Do not check expired or damaged supplies	User forgets to follow protocol	N/A	Potentially damaged or expired supplies may go unnoticed	Instructions in IFU
19	Replace any damaged or expired supplies	Do not replace damaged or expired supplies	User forgets to follow protocol	N/A	Potentially damaged or expired supplies may go unnoticed	Instructions in IFU

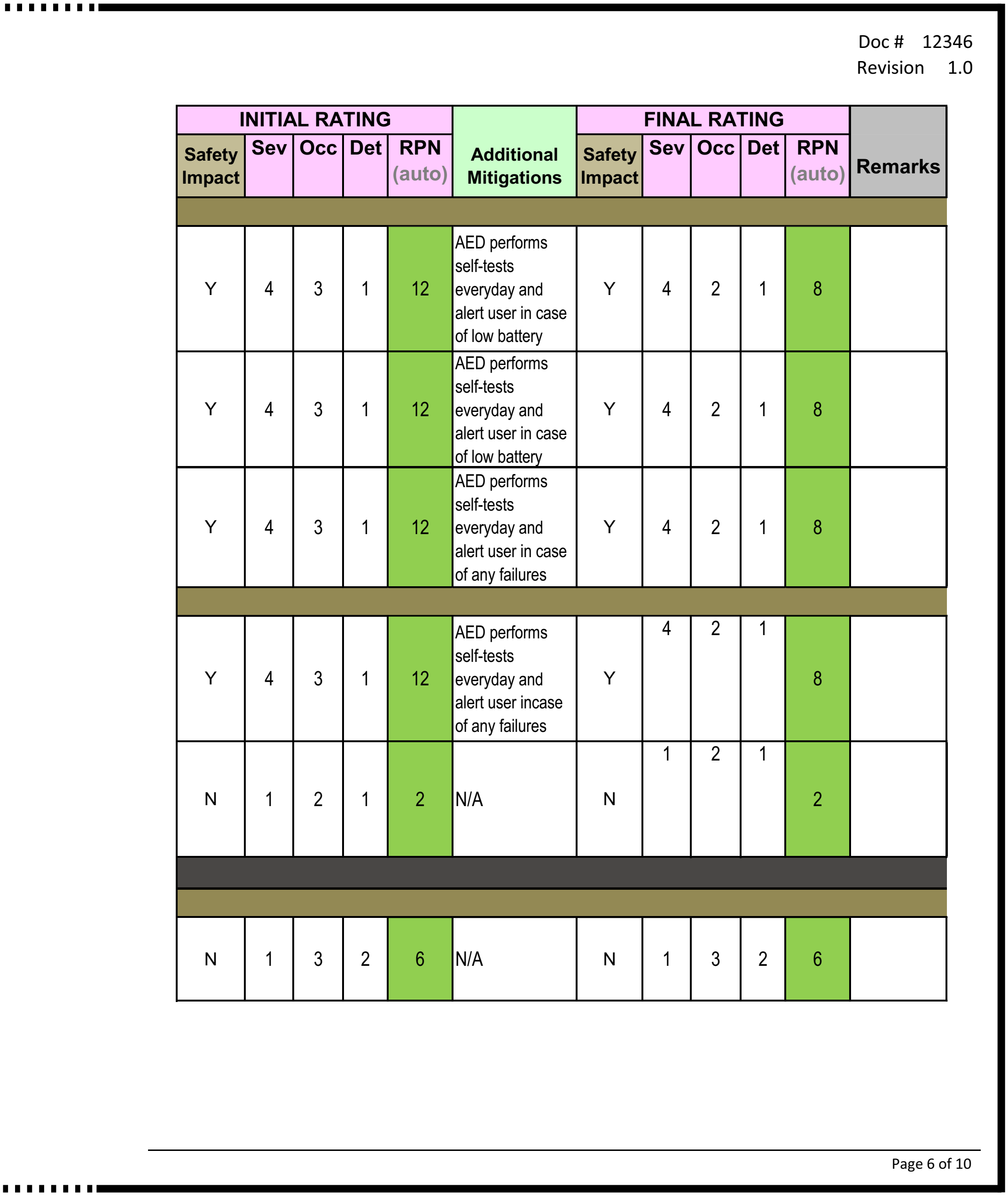


INITIAL RATING						FINAL RATING					
Safety Impact	Sev	Occ	Det	RPN (auto)	Additional Mitigations	Safety Impact	Sev	Occ	Det	RPN (auto)	Remarks
N	3	3	1	9	N/A	N	3	3	1	9	
N	2	3	1	6	N/A	N	2	3	1	6	
N	3	3	1	9	N/A	N	3	3	1	9	
N	5	2	1	10	N/A	N	5	2	1	10	
N	2	3	1	6	AED senses that the pads have not been plugged in and will continuously chirp until they are	N	2	2	1	4	
N	3	3	1	9	N/A	N	3	3	1	9	
N	3	3	1	9	N/A	N	3	3	1	9	



UMFMEA
Vivio AED

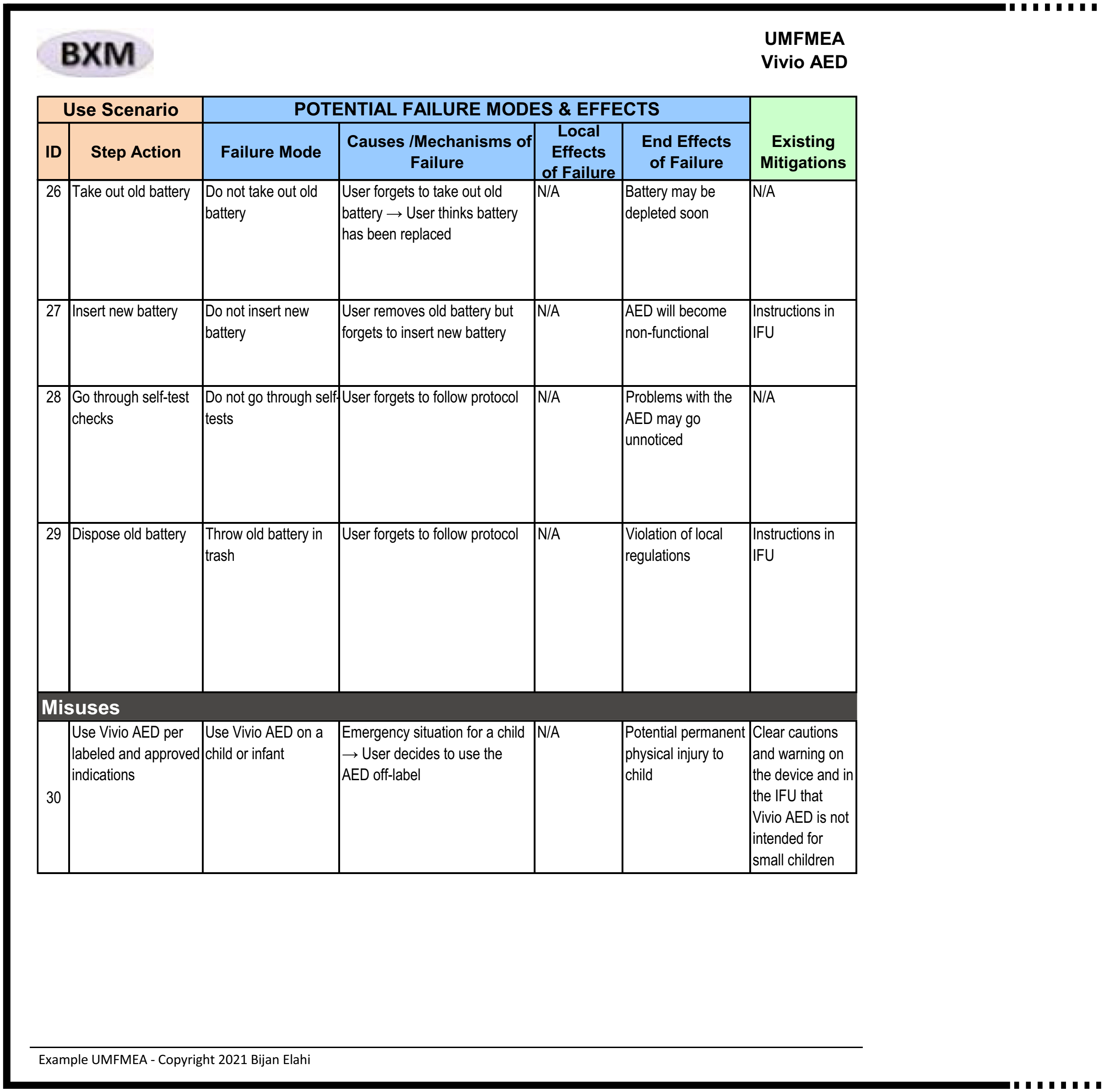
Use Scenario		POTENTIAL FAILURE MODES & EFFECTS				Existing Mitigations
ID	**Step Action**	**Failure Mode**	**Causes /Mechanisms of Failure**	**Local Effects of Failure**	**End Effects of Failure**	
Task 2 - Check Status						
20	Remove battery for 5+ seconds	Do not remove battery	User forgets to follow protocol	N/A	Low battery may go unnoticed	N/A
21	Remove battery for 5+ seconds	Remove and replace battery in less than 5 Sec.	User forgets to follow protocol	N/A	Low battery may go unnoticed	N/A
22	Reinsert battery and go through self-test procedure	Reinsert battery but not go through self-tests	User forgets to follow protocol	N/A	Problems with the AED may go unnoticed	N/A
Task 3 - Return AED to its Storage Location						
23	Close the outer case and place AED in its storage location	Do not close the outer case	User forgets to follow protocol → AED is exposed to elements	N/A	AED Functions may be damaged	N/A
24	Close the outer case and place AED in its storage location	Do not return AED to its storage place	User forgets to follow protocol	N/A	AED may not be available for next use	N/A
Replace Battery						
Task 1 - Obtain and replace battery						
25	Obtain recommended replacement battery	Obtain unapproved knock-off battery	Cost savings or failure to follow IFU → Secondary market battery is purchased	N/A	Battery may not last as long	Instructions in IFU



Doc # 12346
Revision 1.0

INITIAL RATING					Additional Mitigations	FINAL RATING					Remarks
Safety Impact	Sev	Occ	Det	RPN (auto)		Safety Impact	Sev	Occ	Det	RPN (auto)	
Y	4	3	1	12	AED performs self-tests everyday and alert user in case of low battery	Y	4	2	1	8	
Y	4	3	1	12	AED performs self-tests everyday and alert user in case of low battery	Y	4	2	1	8	
Y	4	3	1	12	AED performs self-tests everyday and alert user in case of any failures	Y	4	2	1	8	
Y	4	3	1	12	AED performs self-tests everyday and alert user incase of any failures	Y	4	2	1	8	
N	1	2	1	2	N/A	N	1	2	1	2	
N	1	3	2	6	N/A	N	1	3	2	6	

Page 6 of 10

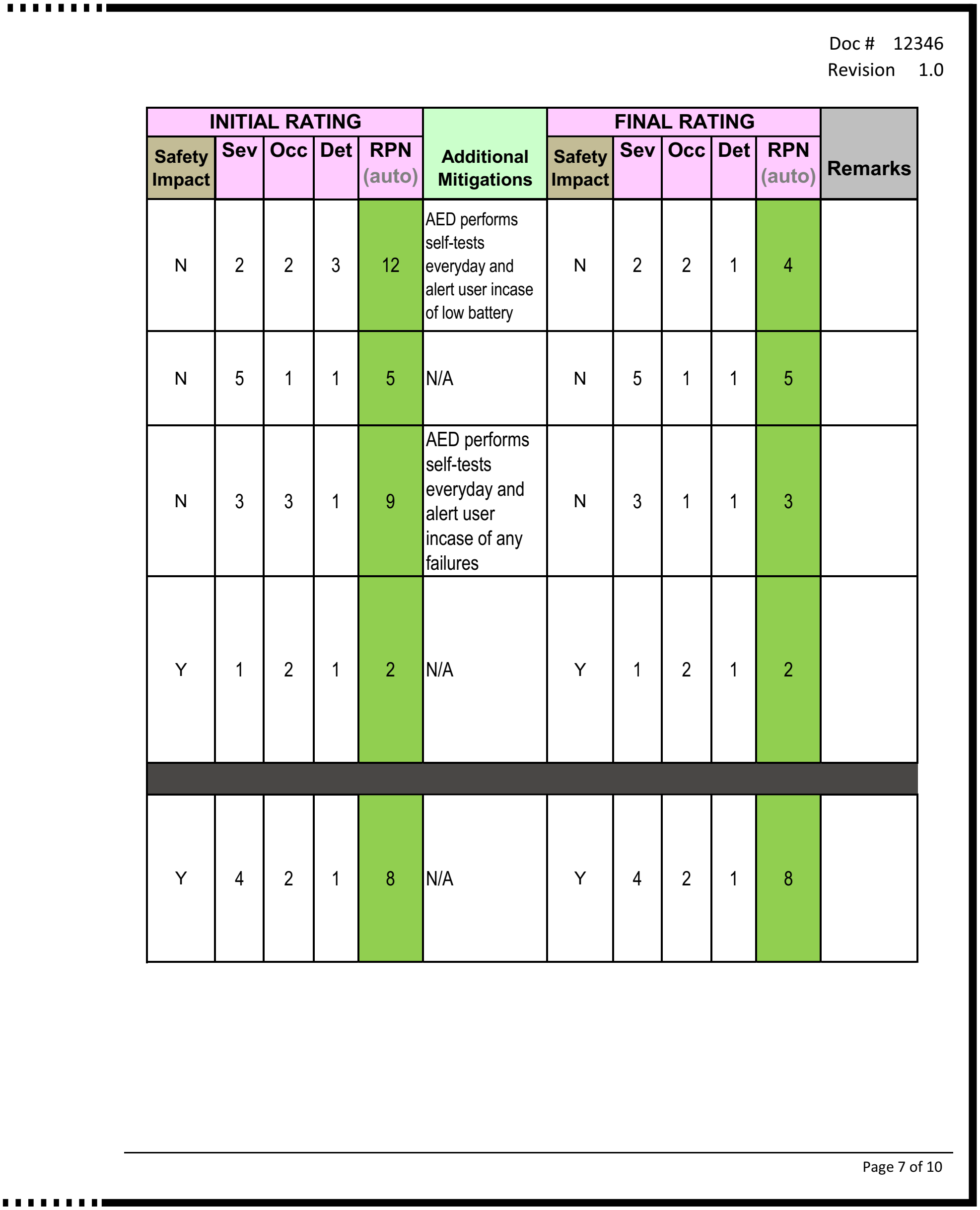


BXM

UMFMEA
Vivio AED

Use Scenario		POTENTIAL FAILURE MODES & EFFECTS				
ID	Step Action	Failure Mode	Causes /Mechanisms of Failure	Local Effects of Failure	End Effects of Failure	Existing Mitigations
26	Take out old battery	Do not take out old battery	User forgets to take out old battery → User thinks battery has been replaced	N/A	Battery may be depleted soon	N/A
27	Insert new battery	Do not insert new battery	User removes old battery but forgets to insert new battery	N/A	AED will become non-functional	Instructions in IFU
28	Go through self-test checks	Do not go through self-tests	User forgets to follow protocol	N/A	Problems with the AED may go unnoticed	N/A
29	Dispose old battery	Throw old battery in trash	User forgets to follow protocol	N/A	Violation of local regulations	Instructions in IFU
Misuses						
30	Use Vivio AED per labeled and approved indications	Use Vivio AED on a child or infant	Emergency situation for a child → User decides to use the AED off-label	N/A	Potential permanent physical injury to child	Clear cautions and warning on the device and in the IFU that Vivio AED is not intended for small children

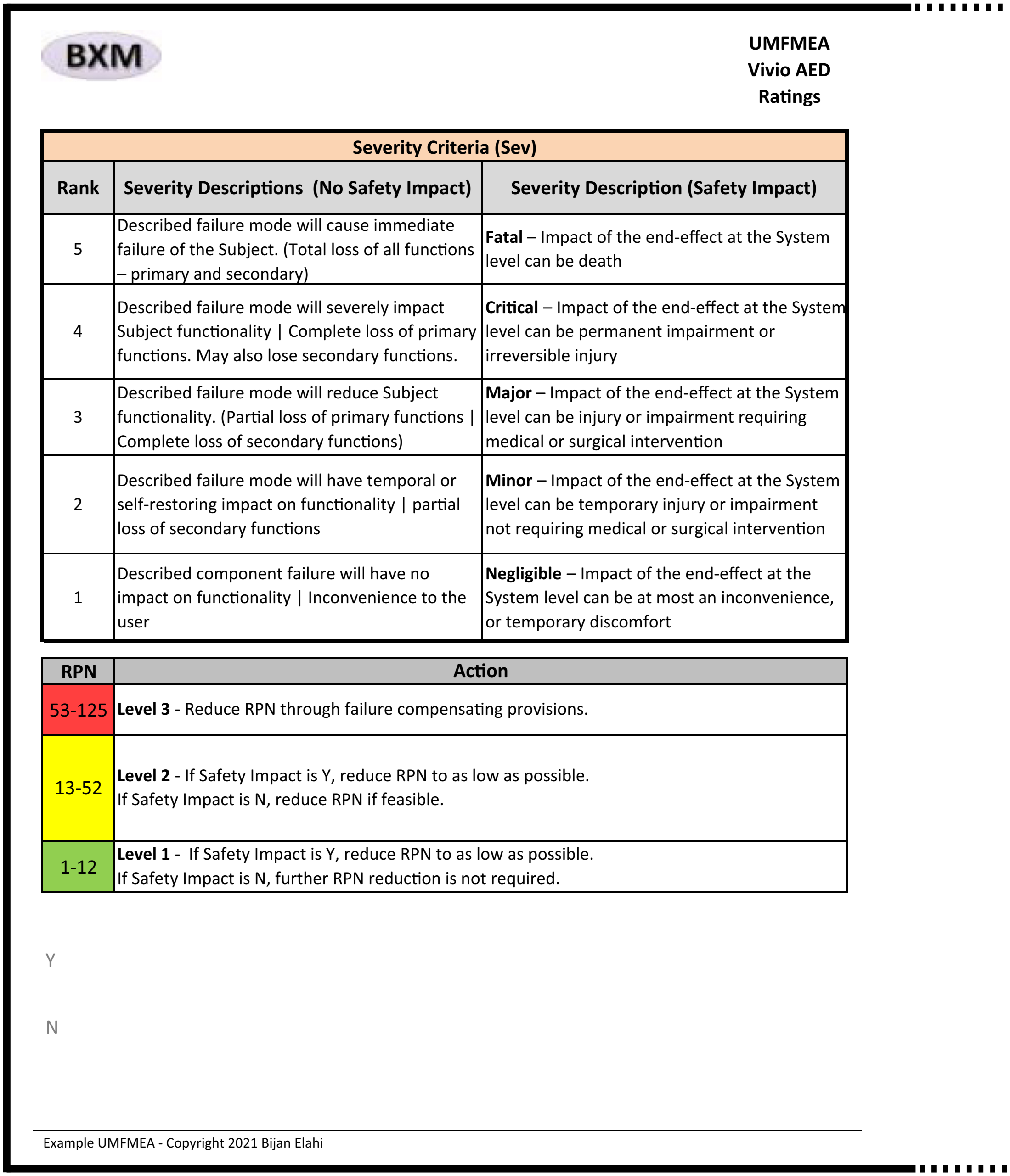
Example UMFMEA - Copyright 2021 Bijan Elahi



Doc # 12346
Revision 1.0

INITIAL RATING					Additional Mitigations	FINAL RATING					Remarks
Safety Impact	Sev	Occ	Det	RPN (auto)		Safety Impact	Sev	Occ	Det	RPN (auto)	
N	2	2	3	12	AED performs self-tests everyday and alert user incase of low battery	N	2	2	1	4	
N	5	1	1	5	N/A	N	5	1	1	5	
N	3	3	1	9	AED performs self-tests everyday and alert user incase of any failures	N	3	1	1	3	
Y	1	2	1	2	N/A	Y	1	2	1	2	
Y	4	2	1	8	N/A	Y	4	2	1	8	

Page 7 of 10



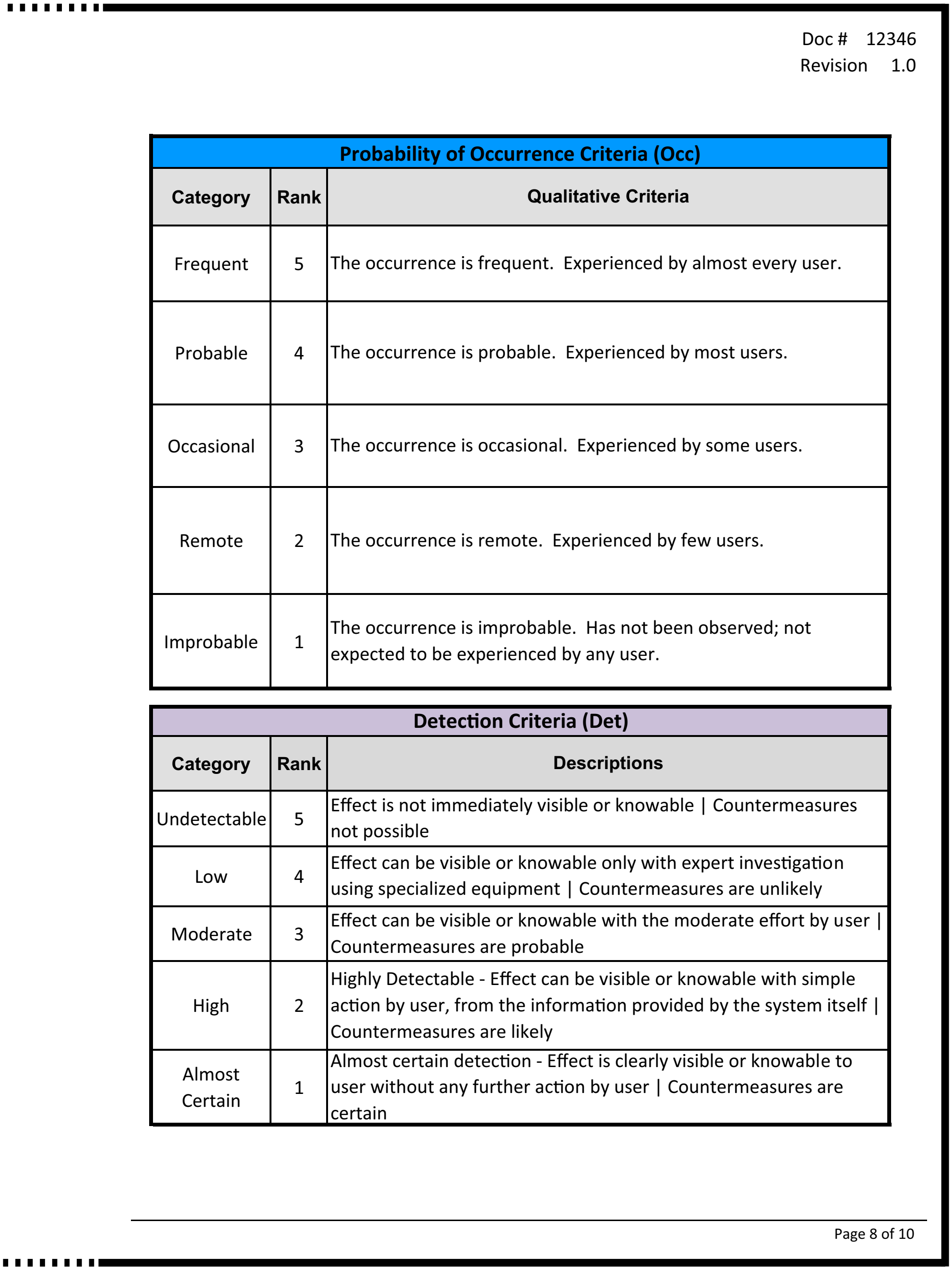
UMFMEA
Vivio AED
Ratings

Severity Criteria (Sev)		
Rank	**Severity Descriptions (No Safety Impact)**	**Severity Description (Safety Impact)**
5	Described failure mode will cause immediate failure of the Subject. (Total loss of all functions – primary and secondary)	**Fatal** – Impact of the end-effect at the System level can be death
4	Described failure mode will severely impact Subject functionality | Complete loss of primary functions. May also lose secondary functions.	**Critical** – Impact of the end-effect at the System level can be permanent impairment or irreversible injury
3	Described failure mode will reduce Subject functionality. (Partial loss of primary functions | Complete loss of secondary functions)	**Major** – Impact of the end-effect at the System level can be injury or impairment requiring medical or surgical intervention
2	Described failure mode will have temporal or self-restoring impact on functionality | partial loss of secondary functions	**Minor** – Impact of the end-effect at the System level can be temporary injury or impairment not requiring medical or surgical intervention
1	Described component failure will have no impact on functionality | Inconvenience to the user	**Negligible** – Impact of the end-effect at the System level can be at most an inconvenience, or temporary discomfort

RPN	Action
53-125	**Level 3** - Reduce RPN through failure compensating provisions.
13-52	**Level 2** - If Safety Impact is Y, reduce RPN to as low as possible. If Safety Impact is N, reduce RPN if feasible.
1-12	**Level 1** - If Safety Impact is Y, reduce RPN to as low as possible. If Safety Impact is N, further RPN reduction is not required.

Y

N



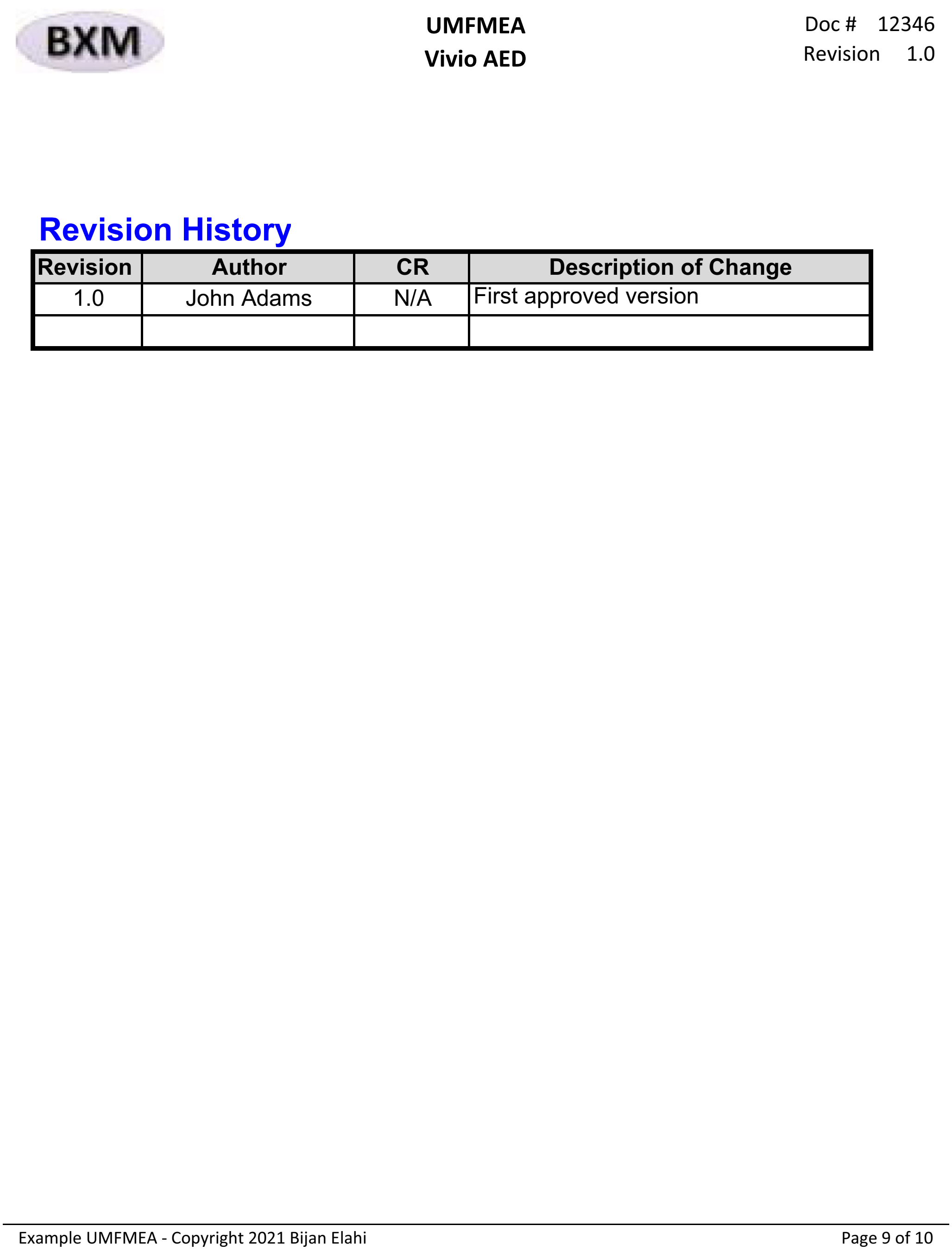
Doc # 12346
Revision 1.0

Probability of Occurrence Criteria (Occ)

Category	Rank	Qualitative Criteria
Frequent	5	The occurrence is frequent. Experienced by almost every user.
Probable	4	The occurrence is probable. Experienced by most users.
Occasional	3	The occurrence is occasional. Experienced by some users.
Remote	2	The occurrence is remote. Experienced by few users.
Improbable	1	The occurrence is improbable. Has not been observed; not expected to be experienced by any user.

Detection Criteria (Det)

Category	Rank	Descriptions
Undetectable	5	Effect is not immediately visible or knowable | Countermeasures not possible
Low	4	Effect can be visible or knowable only with expert investigation using specialized equipment | Countermeasures are unlikely
Moderate	3	Effect can be visible or knowable with the moderate effort by user | Countermeasures are probable
High	2	Highly Detectable - Effect can be visible or knowable with simple action by user, from the information provided by the system itself | Countermeasures are likely
Almost Certain	1	Almost certain detection - Effect is clearly visible or knowable to user without any further action by user | Countermeasures are certain

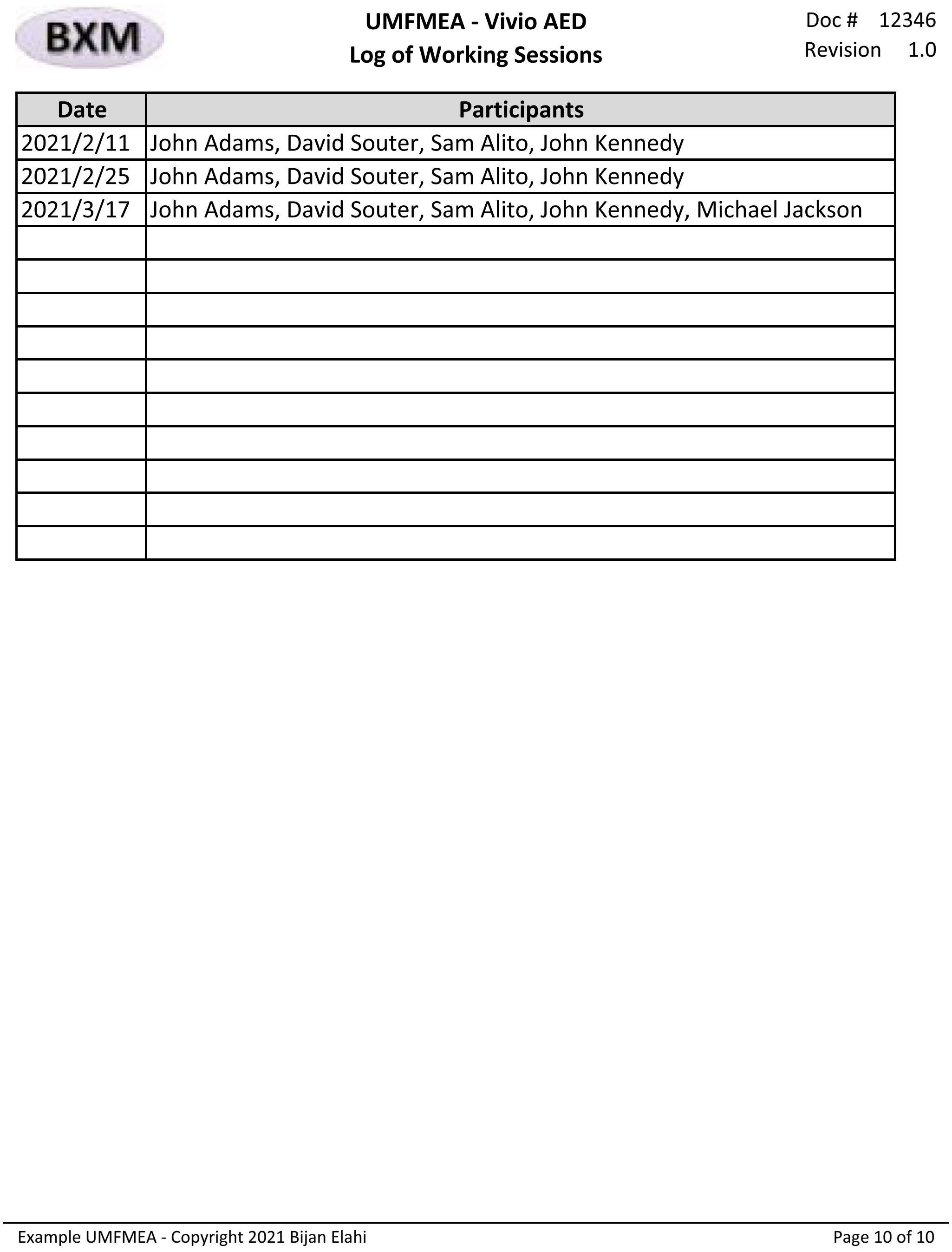


UMFMEA
Vivio AED

Doc # 12346
Revision 1.0

Revision History

Revision	Author	CR	Description of Change
1.0	John Adams	N/A	First approved version



BXM

UMFMEA - Vivio AED
Log of Working Sessions

Doc # 12346
Revision 1.0

Date	Participants
2021/2/11	John Adams, David Souter, Sam Alito, John Kennedy
2021/2/25	John Adams, David Souter, Sam Alito, John Kennedy
2021/3/17	John Adams, David Souter, Sam Alito, John Kennedy, Michael Jackson

C.11 SOFTWARE FAILURE MODES AND EFFECTS ANALYSIS

SFMEA
Vivio AED

Doc # 12348
Revision 1.0

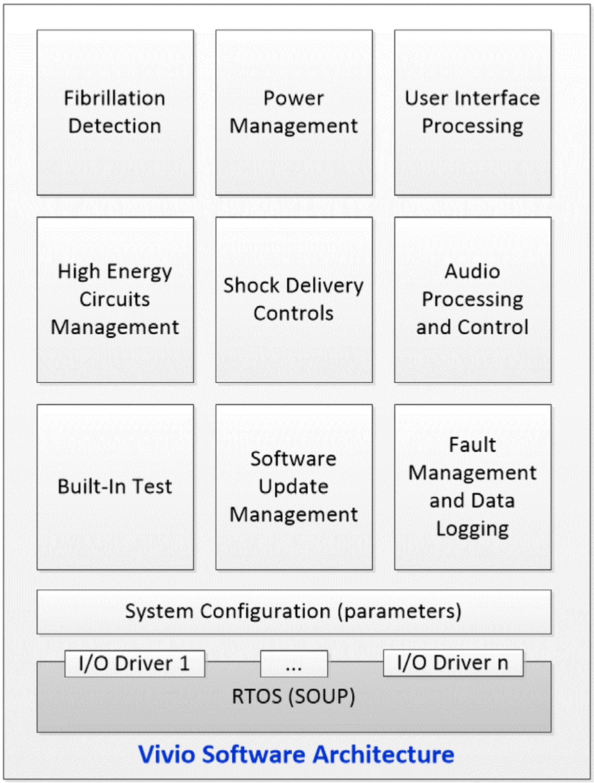
Scope

This SFMEA covers the Vivio Software System.
The scope of the analysis is bounded in the diagram below and encompases all the items within the analysis boundary.

Item Under Analysis: Vivio SW design v 1.0

Primary functions: VF detection, shock delivery

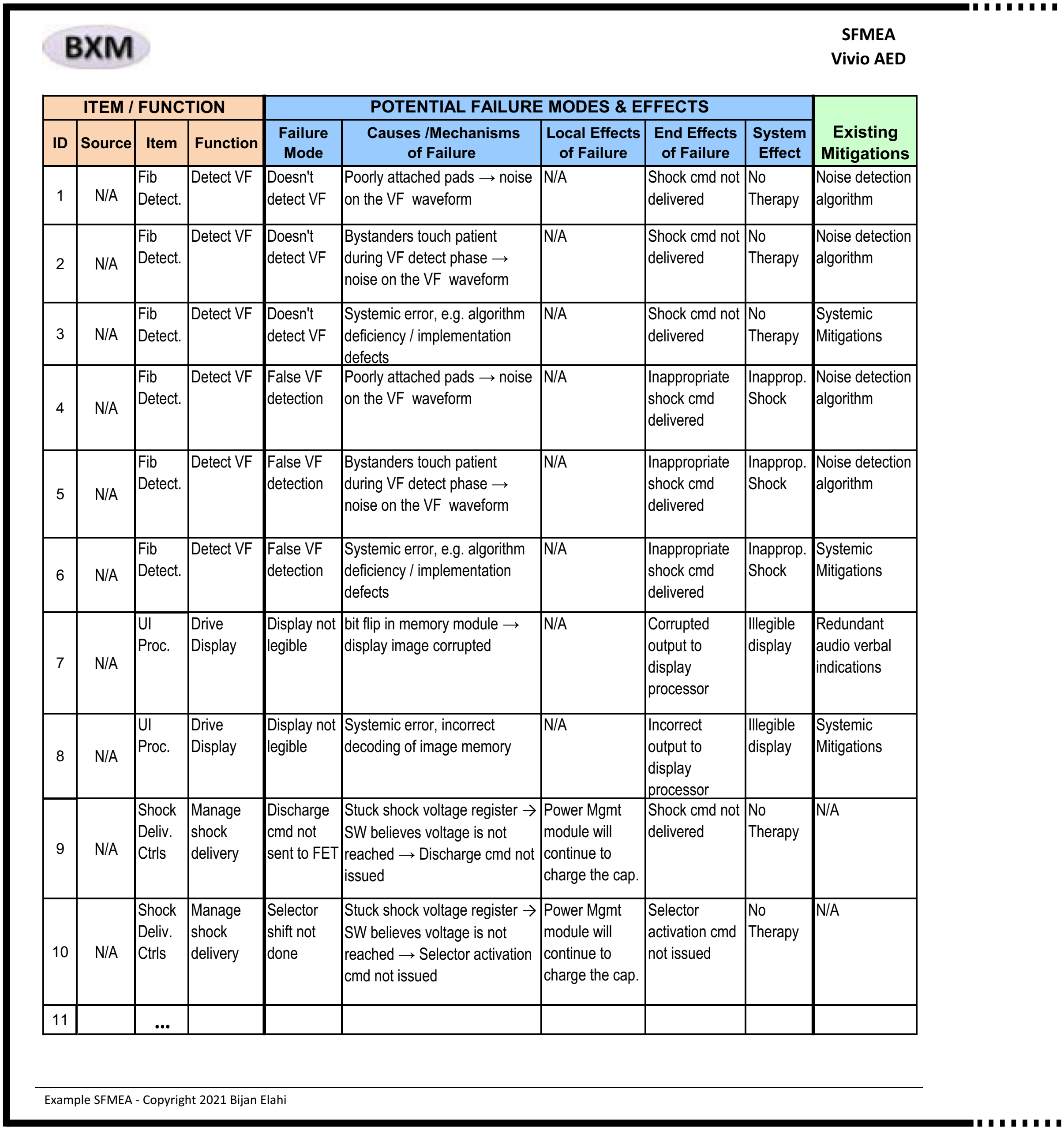
Secondary functions: Audio processing, fault logging


Fibrillation Detection
Power Management
User Interface Processing
High Energy Circuits Management
Shock Delivery Controls
Audio Processing and Control
Built-In Test
Software Update Management
Fault Management and Data Logging
System Configuration (parameters)
I/O Driver 1
...
I/O Driver n
RTOS (SOUP)

Vivio Software Architecture

G065 © 2018 Bijan Elahi

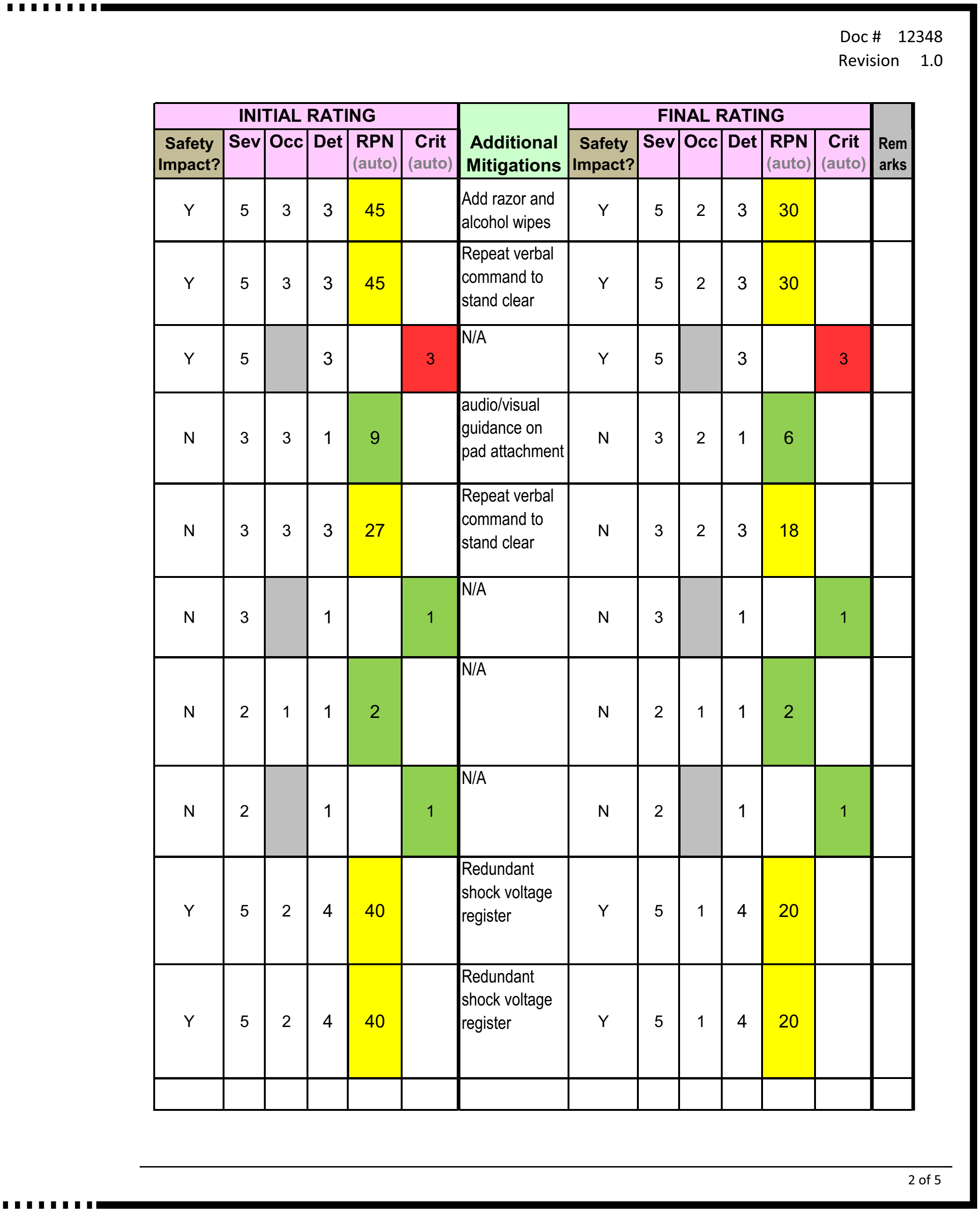
Note - This Example SFMEA is abbreviated and truncated due to page limitations in the book.



BXM

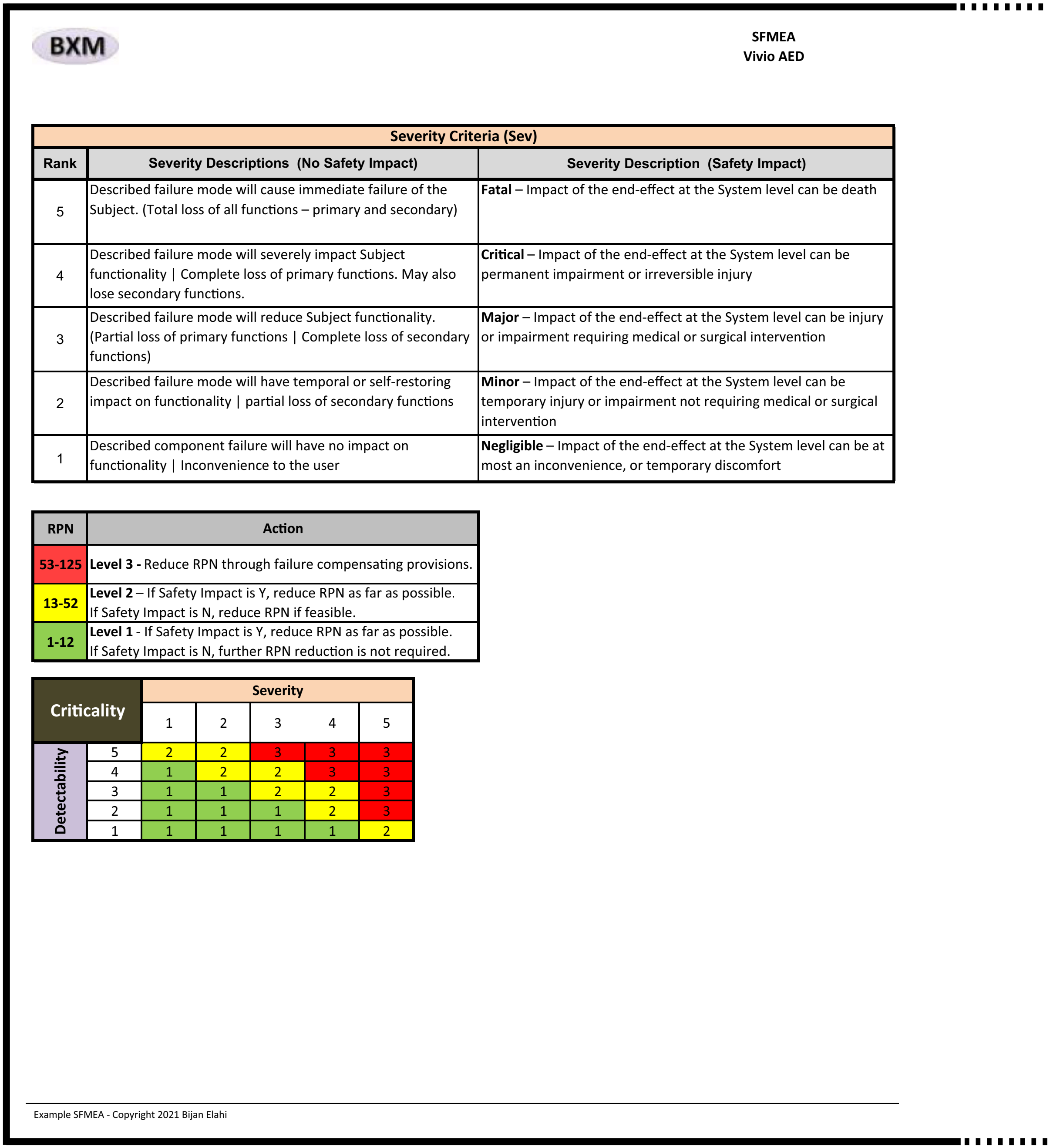
SFMEA
Vivio AED

ITEM / FUNCTION				POTENTIAL FAILURE MODES & EFFECTS					Existing Mitigations
ID	Source	Item	Function	Failure Mode	Causes /Mechanisms of Failure	Local Effects of Failure	End Effects of Failure	System Effect	
1	N/A	Fib Detect.	Detect VF	Doesn't detect VF	Poorly attached pads → noise on the VF waveform	N/A	Shock cmd not delivered	No Therapy	Noise detection algorithm
2	N/A	Fib Detect.	Detect VF	Doesn't detect VF	Bystanders touch patient during VF detect phase → noise on the VF waveform	N/A	Shock cmd not delivered	No Therapy	Noise detection algorithm
3	N/A	Fib Detect.	Detect VF	Doesn't detect VF	Systemic error, e.g. algorithm deficiency / implementation defects	N/A	Shock cmd not delivered	No Therapy	Systemic Mitigations
4	N/A	Fib Detect.	Detect VF	False VF detection	Poorly attached pads → noise on the VF waveform	N/A	Inappropriate shock cmd delivered	Inapprop. Shock	Noise detection algorithm
5	N/A	Fib Detect.	Detect VF	False VF detection	Bystanders touch patient during VF detect phase → noise on the VF waveform	N/A	Inappropriate shock cmd delivered	Inapprop. Shock	Noise detection algorithm
6	N/A	Fib Detect.	Detect VF	False VF detection	Systemic error, e.g. algorithm deficiency / implementation defects	N/A	Inappropriate shock cmd delivered	Inapprop. Shock	Systemic Mitigations
7	N/A	UI Proc.	Drive Display	Display not legible	bit flip in memory module → display image corrupted	N/A	Corrupted output to display processor	Illegible display	Redundant audio verbal indications
8	N/A	UI Proc.	Drive Display	Display not legible	Systemic error, incorrect decoding of image memory	N/A	Incorrect output to display processor	Illegible display	Systemic Mitigations
9	N/A	Shock Deliv. Ctrls	Manage shock delivery	Discharge cmd not sent to FET	Stuck shock voltage register → SW believes voltage is not reached → Discharge cmd not issued	Power Mgmt module will continue to charge the cap.	Shock cmd not delivered	No Therapy	N/A
10	N/A	Shock Deliv. Ctrls	Manage shock delivery	Selector shift not done	Stuck shock voltage register → SW believes voltage is not reached → Selector activation cmd not issued	Power Mgmt module will continue to charge the cap.	Selector activation cmd not issued	No Therapy	N/A
11		...							



Doc # 12348
Revision 1.0

INITIAL RATING						Additional Mitigations	FINAL RATING						Remarks
Safety Impact?	Sev	Occ	Det	RPN (auto)	Crit (auto)		Safety Impact?	Sev	Occ	Det	RPN (auto)	Crit (auto)	
Y	5	3	3	45		Add razor and alcohol wipes	Y	5	2	3	30		
Y	5	3	3	45		Repeat verbal command to stand clear	Y	5	2	3	30		
Y	5		3		3	N/A	Y	5		3		3	
N	3	3	1	9		audio/visual guidance on pad attachment	N	3	2	1	6		
N	3	3	3	27		Repeat verbal command to stand clear	N	3	2	3	18		
N	3		1		1	N/A	N	3		1		1	
N	2	1	1	2		N/A	N	2	1	1	2		
N	2		1		1	N/A	N	2		1		1	
Y	5	2	4	40		Redundant shock voltage register	Y	5	1	4	20		
Y	5	2	4	40		Redundant shock voltage register	Y	5	1	4	20		



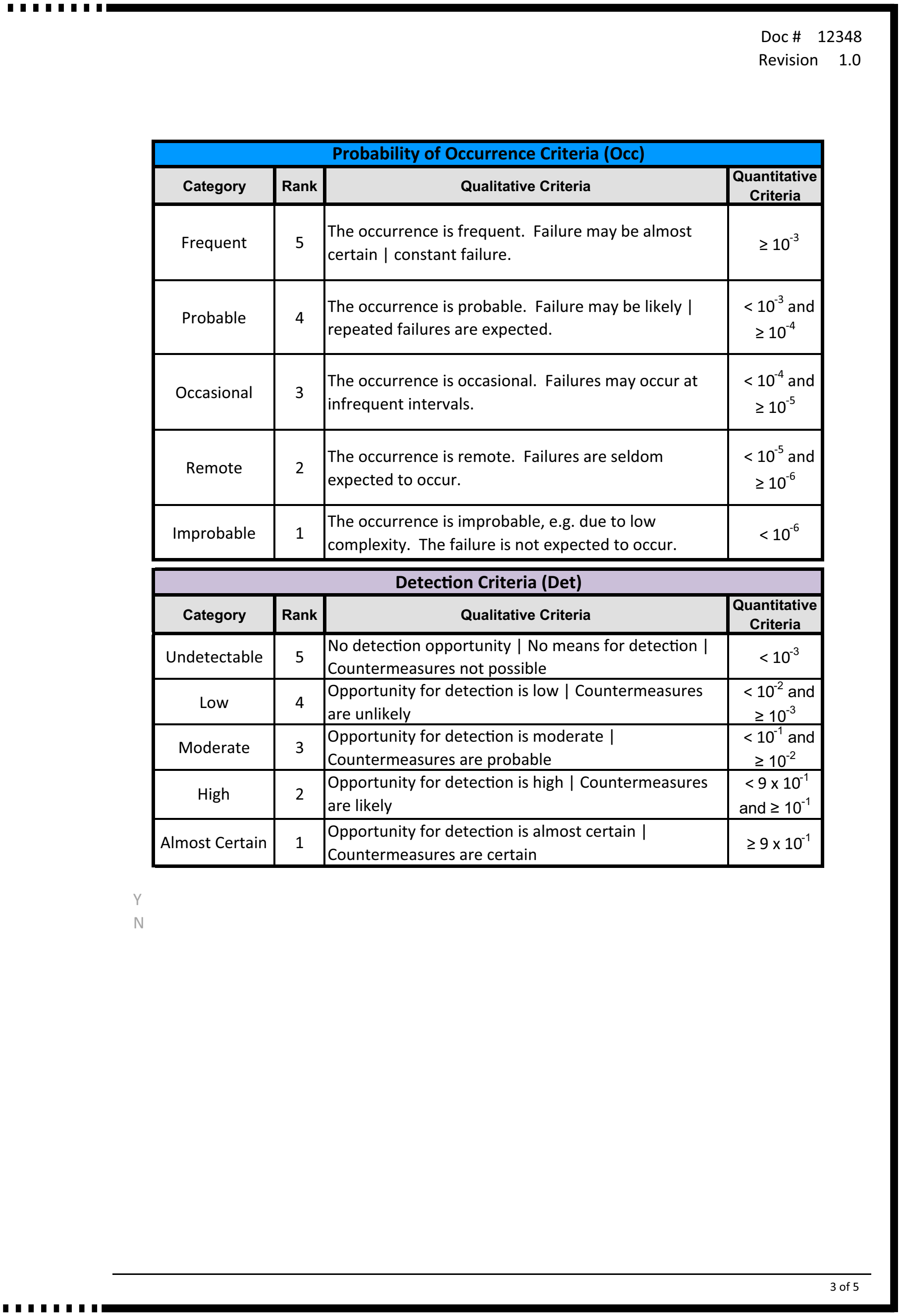
BXM

SFMEA
Vivio AED

Severity Criteria (Sev)		
Rank	Severity Descriptions (No Safety Impact)	Severity Description (Safety Impact)
5	Described failure mode will cause immediate failure of the Subject. (Total loss of all functions – primary and secondary)	**Fatal** – Impact of the end-effect at the System level can be death
4	Described failure mode will severely impact Subject functionality | Complete loss of primary functions. May also lose secondary functions.	**Critical** – Impact of the end-effect at the System level can be permanent impairment or irreversible injury
3	Described failure mode will reduce Subject functionality. (Partial loss of primary functions | Complete loss of secondary functions)	**Major** – Impact of the end-effect at the System level can be injury or impairment requiring medical or surgical intervention
2	Described failure mode will have temporal or self-restoring impact on functionality | partial loss of secondary functions	**Minor** – Impact of the end-effect at the System level can be temporary injury or impairment not requiring medical or surgical intervention
1	Described component failure will have no impact on functionality | Inconvenience to the user	**Negligible** – Impact of the end-effect at the System level can be at most an inconvenience, or temporary discomfort

RPN	Action
53-125	**Level 3 -** Reduce RPN through failure compensating provisions.
13-52	**Level 2** – If Safety Impact is Y, reduce RPN as far as possible. If Safety Impact is N, reduce RPN if feasible.
1-12	**Level 1** - If Safety Impact is Y, reduce RPN as far as possible. If Safety Impact is N, further RPN reduction is not required.

Criticality		Severity				
		1	2	3	4	5
Detectability	5	2	2	3	3	3
	4	1	2	2	3	3
	3	1	1	2	2	3
	2	1	1	1	2	3
	1	1	1	1	1	2

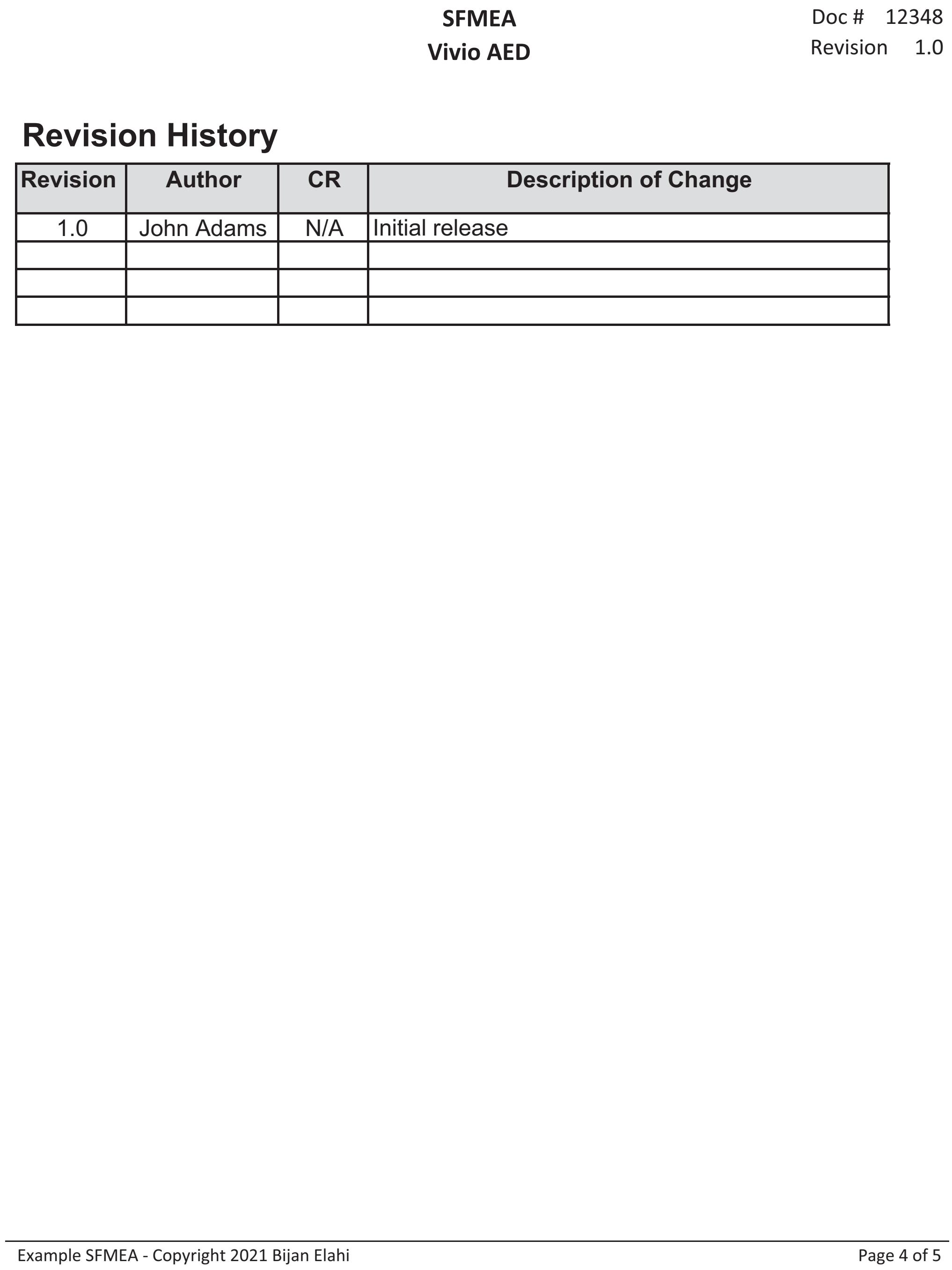


Doc # 12348
Revision 1.0

Probability of Occurrence Criteria (Occ)			
Category	**Rank**	**Qualitative Criteria**	**Quantitative Criteria**
Frequent	5	The occurrence is frequent. Failure may be almost certain | constant failure.	$\geq 10^{-3}$
Probable	4	The occurrence is probable. Failure may be likely | repeated failures are expected.	$< 10^{-3}$ and $\geq 10^{-4}$
Occasional	3	The occurrence is occasional. Failures may occur at infrequent intervals.	$< 10^{-4}$ and $\geq 10^{-5}$
Remote	2	The occurrence is remote. Failures are seldom expected to occur.	$< 10^{-5}$ and $\geq 10^{-6}$
Improbable	1	The occurrence is improbable, e.g. due to low complexity. The failure is not expected to occur.	$< 10^{-6}$

Detection Criteria (Det)			
Category	**Rank**	**Qualitative Criteria**	**Quantitative Criteria**
Undetectable	5	No detection opportunity | No means for detection | Countermeasures not possible	$< 10^{-3}$
Low	4	Opportunity for detection is low | Countermeasures are unlikely	$< 10^{-2}$ and $\geq 10^{-3}$
Moderate	3	Opportunity for detection is moderate | Countermeasures are probable	$< 10^{-1}$ and $\geq 10^{-2}$
High	2	Opportunity for detection is high | Countermeasures are likely	$< 9 \times 10^{-1}$ and $\geq 10^{-1}$
Almost Certain	1	Opportunity for detection is almost certain | Countermeasures are certain	$\geq 9 \times 10^{-1}$

Y
N



SFMEA
Vivio AED

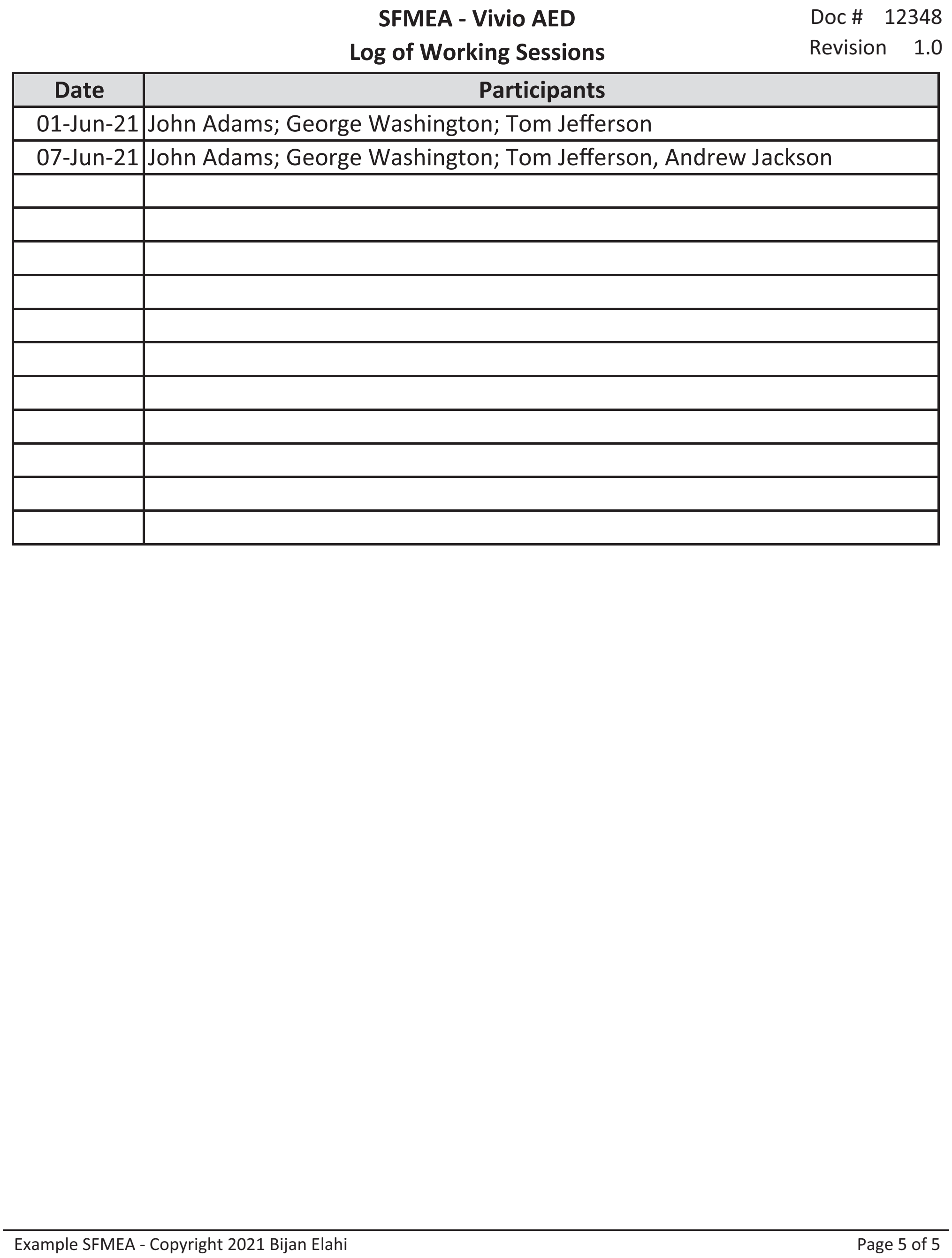
Doc # 12348
Revision 1.0

Revision History

Revision	Author	CR	Description of Change
1.0	John Adams	N/A	Initial release

Example SFMEA - Copyright 2021 Bijan Elahi

Page 4 of 5

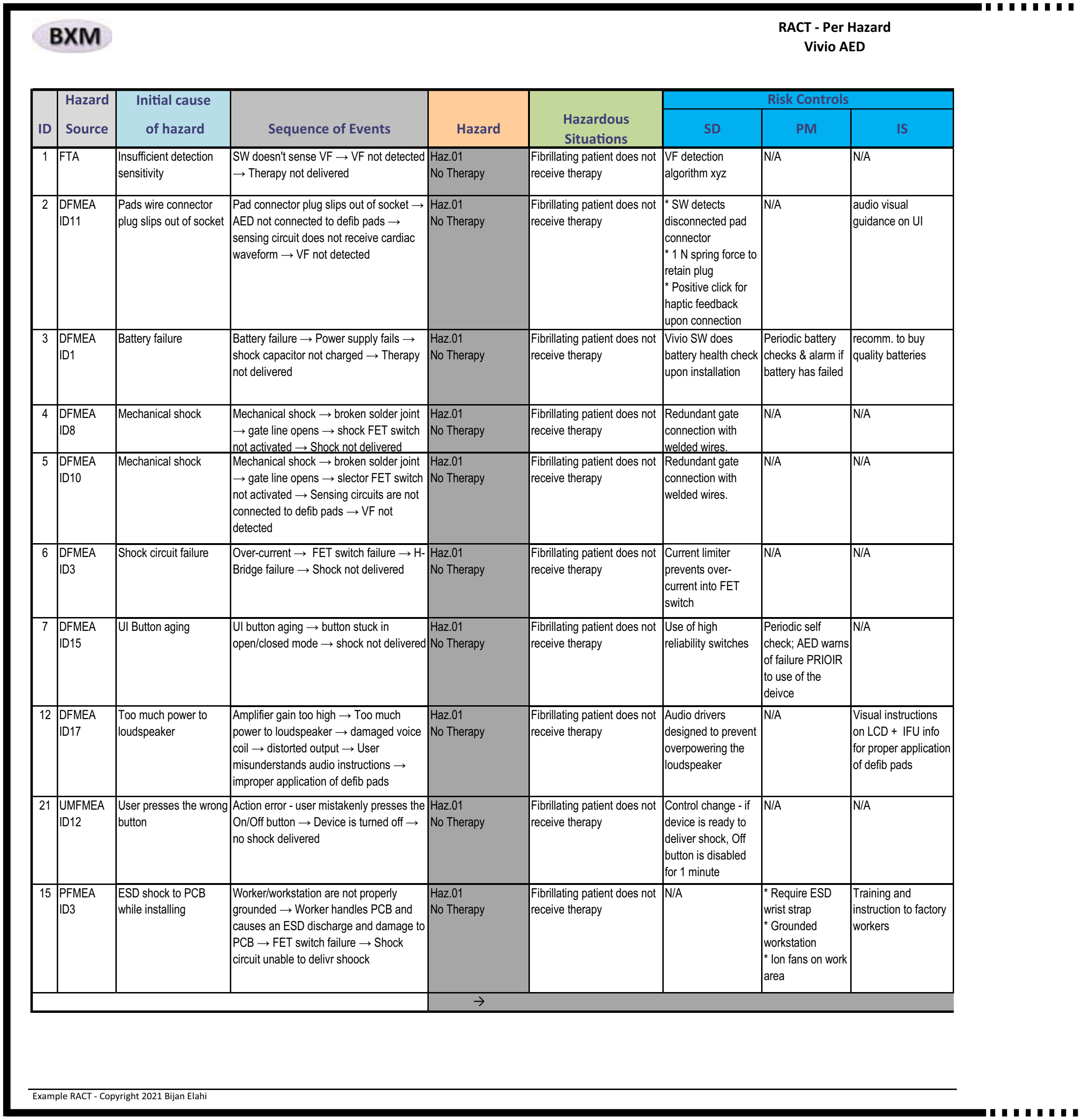


Doc # 12348
Revision 1.0

SFMEA - Vivio AED
Log of Working Sessions

Date	Participants
01-Jun-21	John Adams; George Washington; Tom Jefferson
07-Jun-21	John Adams; George Washington; Tom Jefferson, Andrew Jackson

C.12 RISK ASSESSMENT AND CONTROLS TABLE

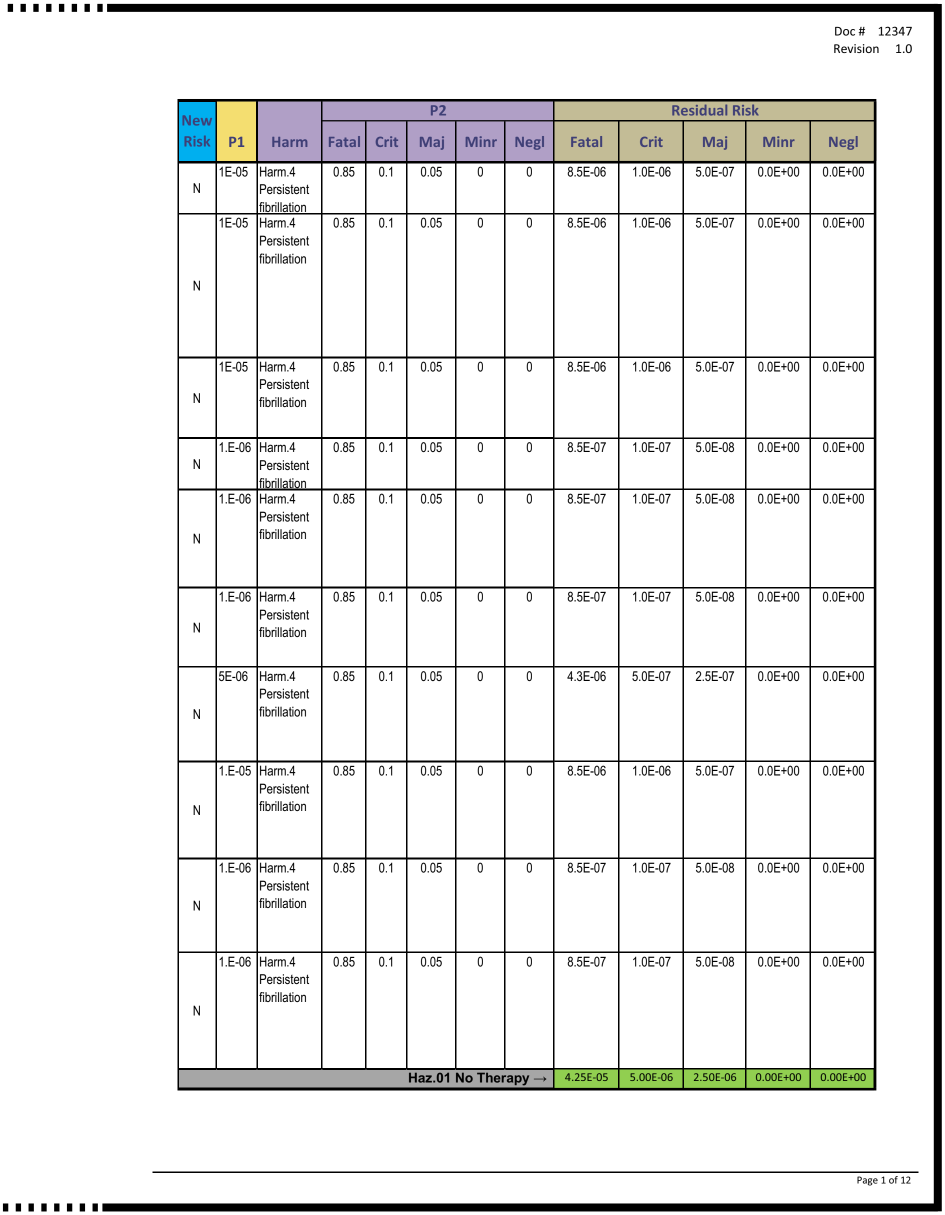


BXM

RACT - Per Hazard
Vivio AED

ID	Hazard Source	Initial cause of hazard	Sequence of Events	Hazard	Hazardous Situations	Risk Controls		
						SD	PM	IS
1	FTA	Insufficient detection sensitivity	SW doesn't sense VF → VF not detected → Therapy not delivered	Haz.01 No Therapy	Fibrillating patient does not receive therapy	VF detection algorithm xyz	N/A	N/A
2	DFMEA ID11	Pads wire connector plug slips out of socket	Pad connector plug slips out of socket → AED not connected to defib pads → sensing circuit does not receive cardiac waveform → VF not detected	Haz.01 No Therapy	Fibrillating patient does not receive therapy	* SW detects disconnected pad connector * 1 N spring force to retain plug * Positive click for haptic feedback upon connection	N/A	audio visual guidance on UI
3	DFMEA ID1	Battery failure	Battery failure → Power supply fails → shock capacitor not charged → Therapy not delivered	Haz.01 No Therapy	Fibrillating patient does not receive therapy	Vivio SW does battery health check upon installation	Periodic battery checks & alarm if battery has failed	recomm. to buy quality batteries
4	DFMEA ID8	Mechanical shock	Mechanical shock → broken solder joint → gate line opens → shock FET switch not activated → Shock not delivered	Haz.01 No Therapy	Fibrillating patient does not receive therapy	Redundant gate connection with welded wires.	N/A	N/A
5	DFMEA ID10	Mechanical shock	Mechanical shock → broken solder joint → gate line opens → slector FET switch not activated → Sensing circuits are not connected to defib pads → VF not detected	Haz.01 No Therapy	Fibrillating patient does not receive therapy	Redundant gate connection with welded wires.	N/A	N/A
6	DFMEA ID3	Shock circuit failure	Over-current → FET switch failure → H-Bridge failure → Shock not delivered	Haz.01 No Therapy	Fibrillating patient does not receive therapy	Current limiter prevents over-current into FET switch	N/A	N/A
7	DFMEA ID15	UI Button aging	UI button aging → button stuck in open/closed mode → shock not delivered	Haz.01 No Therapy	Fibrillating patient does not receive therapy	Use of high reliability switches	Periodic self check; AED warns of failure PRIOIR to use of the deivce	N/A
12	DFMEA ID17	Too much power to loudspeaker	Amplifier gain too high → Too much power to loudspeaker → damaged voice coil → distorted output → User misunderstands audio instructions → improper application of defib pads	Haz.01 No Therapy	Fibrillating patient does not receive therapy	Audio drivers designed to prevent overpowering the loudspeaker	N/A	Visual instructions on LCD + IFU info for proper application of defib pads
21	UMFMEA ID12	User presses the wrong button	Action error - user mistakenly presses the On/Off button → Device is turned off → no shock delivered	Haz.01 No Therapy	Fibrillating patient does not receive therapy	Control change - if device is ready to deliver shock, Off button is disabled for 1 minute	N/A	N/A
15	PFMEA ID3	ESD shock to PCB while installing	Worker/workstation are not properly grounded → Worker handles PCB and causes an ESD discharge and damage to PCB → FET switch failure → Shock circuit unable to delivr shoock	Haz.01 No Therapy	Fibrillating patient does not receive therapy	N/A	* Require ESD wrist strap * Grounded workstation * Ion fans on work area	Training and instruction to factory workers
				→				

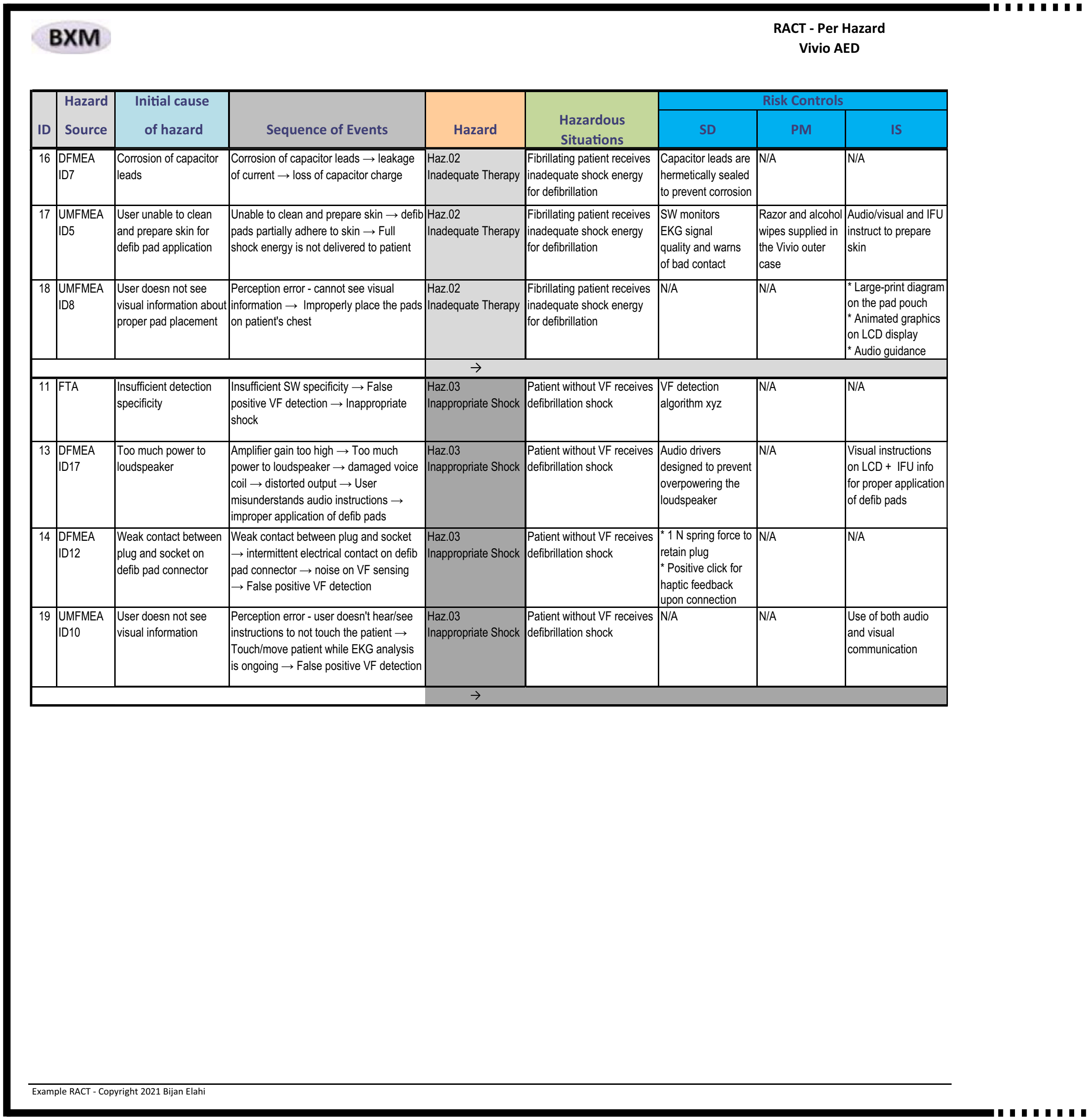
Example RACT - Copyright 2021 Bijan Elahi



Doc # 12347
Revision 1.0

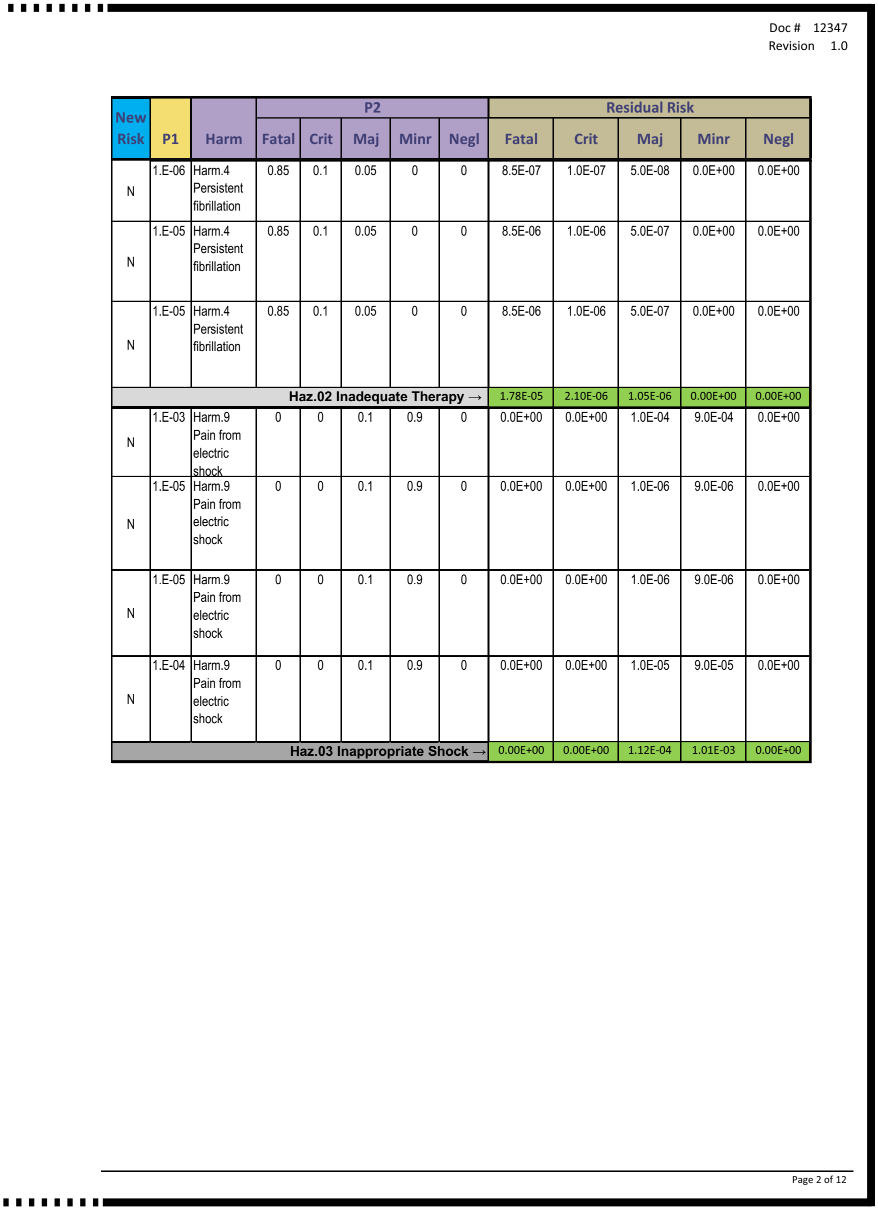
New Risk	P1	Harm	P2					Residual Risk				
			Fatal	Crit	Maj	Minr	Negl	Fatal	Crit	Maj	Minr	Negl
N	1E-05	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-06	1.0E-06	5.0E-07	0.0E+00	0.0E+00
N	1E-05	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-06	1.0E-06	5.0E-07	0.0E+00	0.0E+00
N	1E-05	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-06	1.0E-06	5.0E-07	0.0E+00	0.0E+00
N	1.E-06	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-07	1.0E-07	5.0E-08	0.0E+00	0.0E+00
N	1.E-06	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-07	1.0E-07	5.0E-08	0.0E+00	0.0E+00
N	1.E-06	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-07	1.0E-07	5.0E-08	0.0E+00	0.0E+00
N	5E-06	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	4.3E-06	5.0E-07	2.5E-07	0.0E+00	0.0E+00
N	1.E-05	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-06	1.0E-06	5.0E-07	0.0E+00	0.0E+00
N	1.E-06	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-07	1.0E-07	5.0E-08	0.0E+00	0.0E+00
N	1.E-06	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-07	1.0E-07	5.0E-08	0.0E+00	0.0E+00
Haz.01 No Therapy →								4.25E-05	5.00E-06	2.50E-06	0.00E+00	0.00E+00

Page 1 of 12



RACT - Per Hazard
Vivio AED

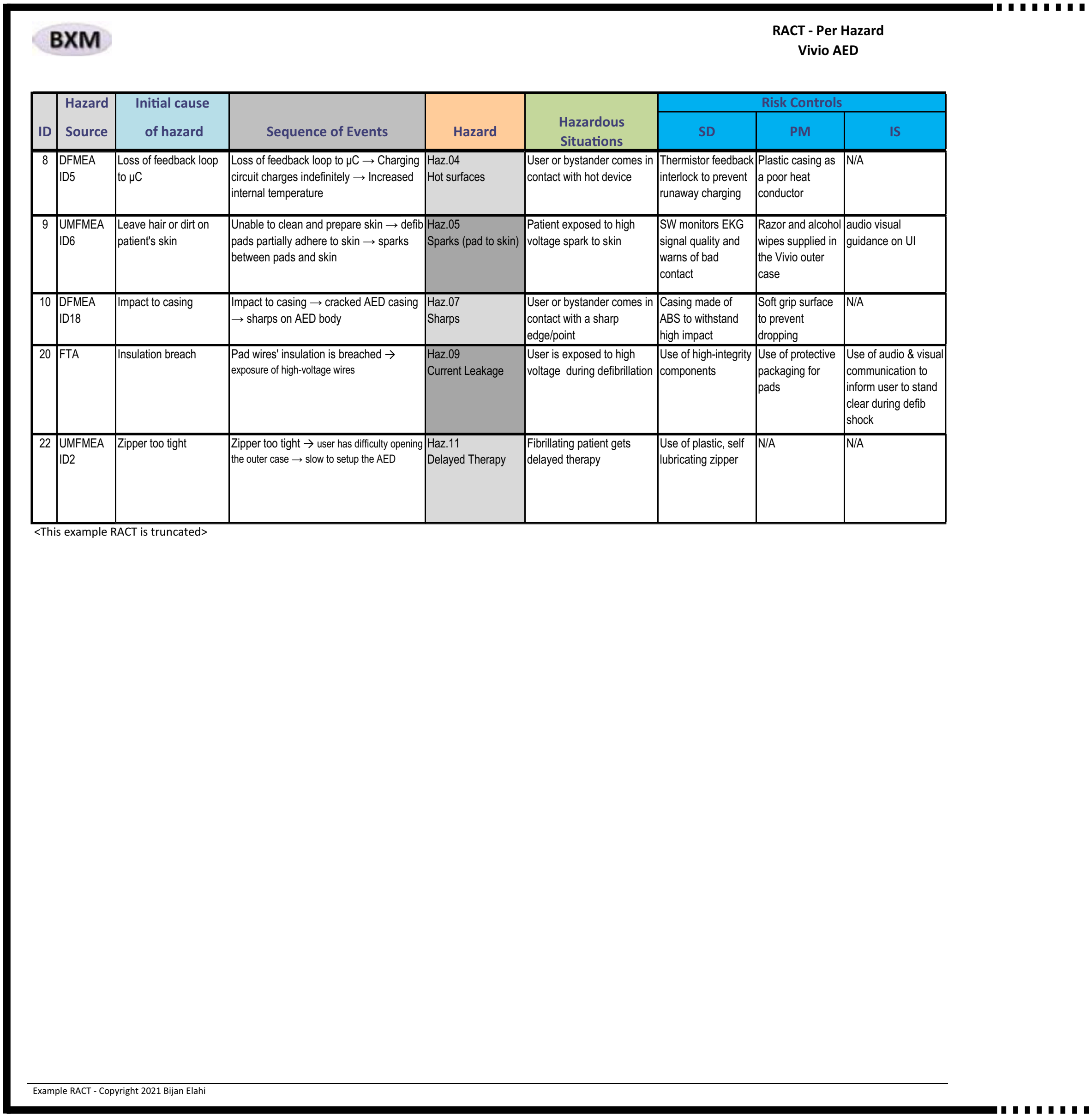
	Hazard	Initial cause			Hazardous	Risk Controls		
ID	Source	of hazard	Sequence of Events	Hazard	Situations	SD	PM	IS
16	DFMEA ID7	Corrosion of capacitor leads	Corrosion of capacitor leads → leakage of current → loss of capacitor charge	Haz.02 Inadequate Therapy	Fibrillating patient receives inadequate shock energy for defibrillation	Capacitor leads are hermetically sealed to prevent corrosion	N/A	N/A
17	UMFMEA ID5	User unable to clean and prepare skin for defib pad application	Unable to clean and prepare skin → defib pads partially adhere to skin → Full shock energy is not delivered to patient	Haz.02 Inadequate Therapy	Fibrillating patient receives inadequate shock energy for defibrillation	SW monitors EKG signal quality and warns of bad contact	Razor and alcohol wipes supplied in the Vivio outer case	Audio/visual and IFU instruct to prepare skin
18	UMFMEA ID8	User doesn not see visual information about proper pad placement	Perception error - cannot see visual information → Improperly place the pads on patient's chest	Haz.02 Inadequate Therapy	Fibrillating patient receives inadequate shock energy for defibrillation	N/A	N/A	* Large-print diagram on the pad pouch * Animated graphics on LCD display * Audio guidance
				→				
11	FTA	Insufficient detection specificity	Insufficient SW specificity → False positive VF detection → Inappropriate shock	Haz.03 Inappropriate Shock	Patient without VF receives defibrillation shock	VF detection algorithm xyz	N/A	N/A
13	DFMEA ID17	Too much power to loudspeaker	Amplifier gain too high → Too much power to loudspeaker → damaged voice coil → distorted output → User misunderstands audio instructions → improper application of defib pads	Haz.03 Inappropriate Shock	Patient without VF receives defibrillation shock	Audio drivers designed to prevent overpowering the loudspeaker	N/A	Visual instructions on LCD + IFU info for proper application of defib pads
14	DFMEA ID12	Weak contact between plug and socket on defib pad connector	Weak contact between plug and socket → intermittent electrical contact on defib pad connector → noise on VF sensing → False positive VF detection	Haz.03 Inappropriate Shock	Patient without VF receives defibrillation shock	* 1 N spring force to retain plug * Positive click for haptic feedback upon connection	N/A	N/A
19	UMFMEA ID10	User doesn not see visual information	Perception error - user doesn't hear/see instructions to not touch the patient → Touch/move patient while EKG analysis is ongoing → False positive VF detection	Haz.03 Inappropriate Shock	Patient without VF receives defibrillation shock	N/A	N/A	Use of both audio and visual communication
				→				



Doc # 12347
Revision 1.0

New Risk	P1	Harm	P2					Residual Risk				
			Fatal	Crit	Maj	Minr	Negl	Fatal	Crit	Maj	Minr	Negl
N	1.E-06	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-07	1.0E-07	5.0E-08	0.0E+00	0.0E+00
N	1.E-05	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-06	1.0E-06	5.0E-07	0.0E+00	0.0E+00
N	1.E-05	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-06	1.0E-06	5.0E-07	0.0E+00	0.0E+00
Haz.02 Inadequate Therapy →								1.78E-05	2.10E-06	1.05E-06	0.00E+00	0.00E+00
N	1.E-03	Harm.9 Pain from electric shock	0	0	0.1	0.9	0	0.0E+00	0.0E+00	1.0E-04	9.0E-04	0.0E+00
N	1.E-05	Harm.9 Pain from electric shock	0	0	0.1	0.9	0	0.0E+00	0.0E+00	1.0E-06	9.0E-06	0.0E+00
N	1.E-05	Harm.9 Pain from electric shock	0	0	0.1	0.9	0	0.0E+00	0.0E+00	1.0E-06	9.0E-06	0.0E+00
N	1.E-04	Harm.9 Pain from electric shock	0	0	0.1	0.9	0	0.0E+00	0.0E+00	1.0E-05	9.0E-05	0.0E+00
Haz.03 Inappropriate Shock →								0.00E+00	0.00E+00	1.12E-04	1.01E-03	0.00E+00

Page 2 of 12



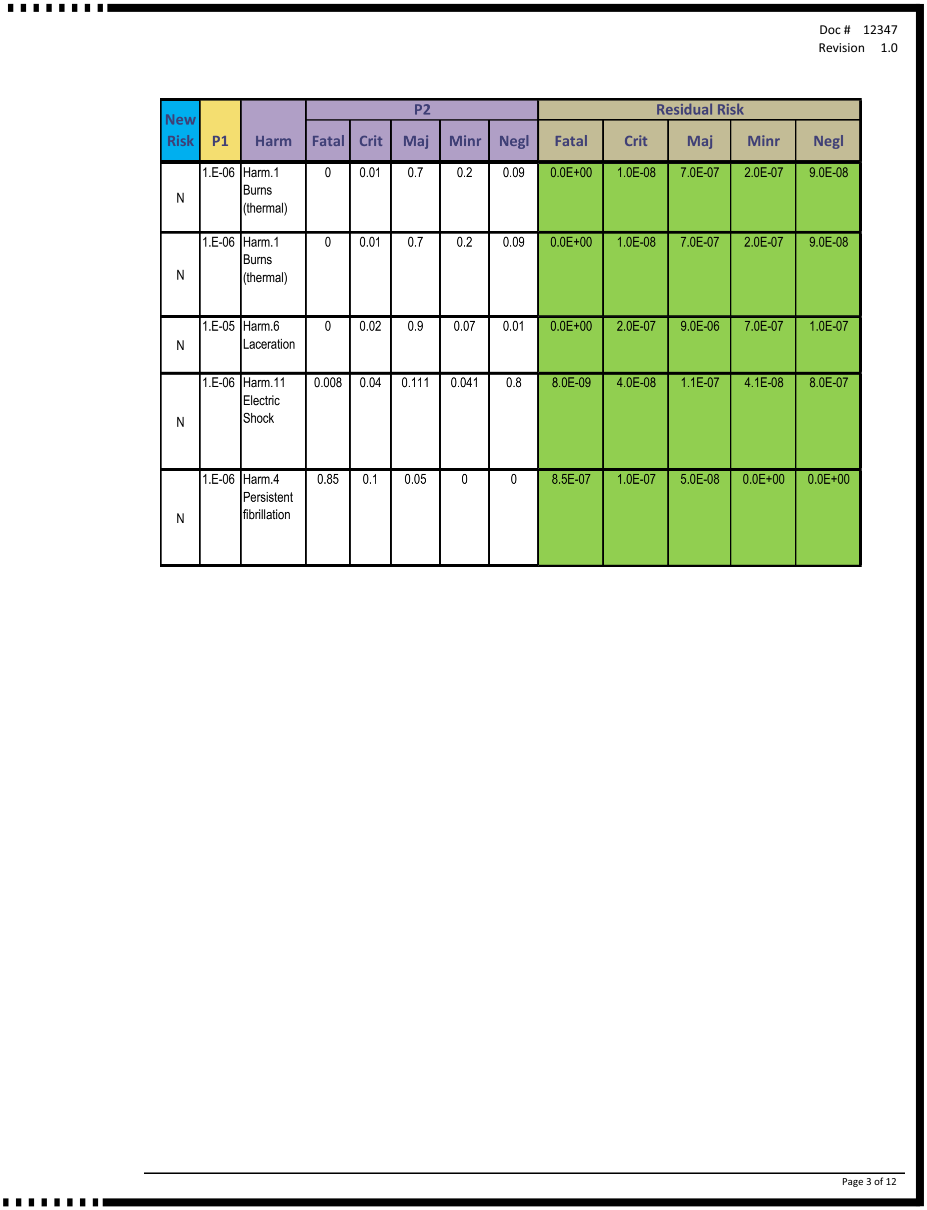
BXM

RACT - Per Hazard
Vivio AED

ID	Hazard Source	Initial cause of hazard	Sequence of Events	Hazard	Hazardous Situations	Risk Controls		
						SD	PM	IS
8	DFMEA ID5	Loss of feedback loop to µC	Loss of feedback loop to µC → Charging circuit charges indefinitely → Increased internal temperature	Haz.04 Hot surfaces	User or bystander comes in contact with hot device	Thermistor feedback interlock to prevent runaway charging	Plastic casing as a poor heat conductor	N/A
9	UMFMEA ID6	Leave hair or dirt on patient's skin	Unable to clean and prepare skin → defib pads partially adhere to skin → sparks between pads and skin	Haz.05 Sparks (pad to skin)	Patient exposed to high voltage spark to skin	SW monitors EKG signal quality and warns of bad contact	Razor and alcohol wipes supplied in the Vivio outer case	audio visual guidance on UI
10	DFMEA ID18	Impact to casing	Impact to casing → cracked AED casing → sharps on AED body	Haz.07 Sharps	User or bystander comes in contact with a sharp edge/point	Casing made of ABS to withstand high impact	Soft grip surface to prevent dropping	N/A
20	FTA	Insulation breach	Pad wires' insulation is breached → exposure of high-voltage wires	Haz.09 Current Leakage	User is exposed to high voltage during defibrillation	Use of high-integrity components	Use of protective packaging for pads	Use of audio & visual communication to inform user to stand clear during defib shock
22	UMFMEA ID2	Zipper too tight	Zipper too tight → user has difficulty opening the outer case → slow to setup the AED	Haz.11 Delayed Therapy	Fibrillating patient gets delayed therapy	Use of plastic, self lubricating zipper	N/A	N/A

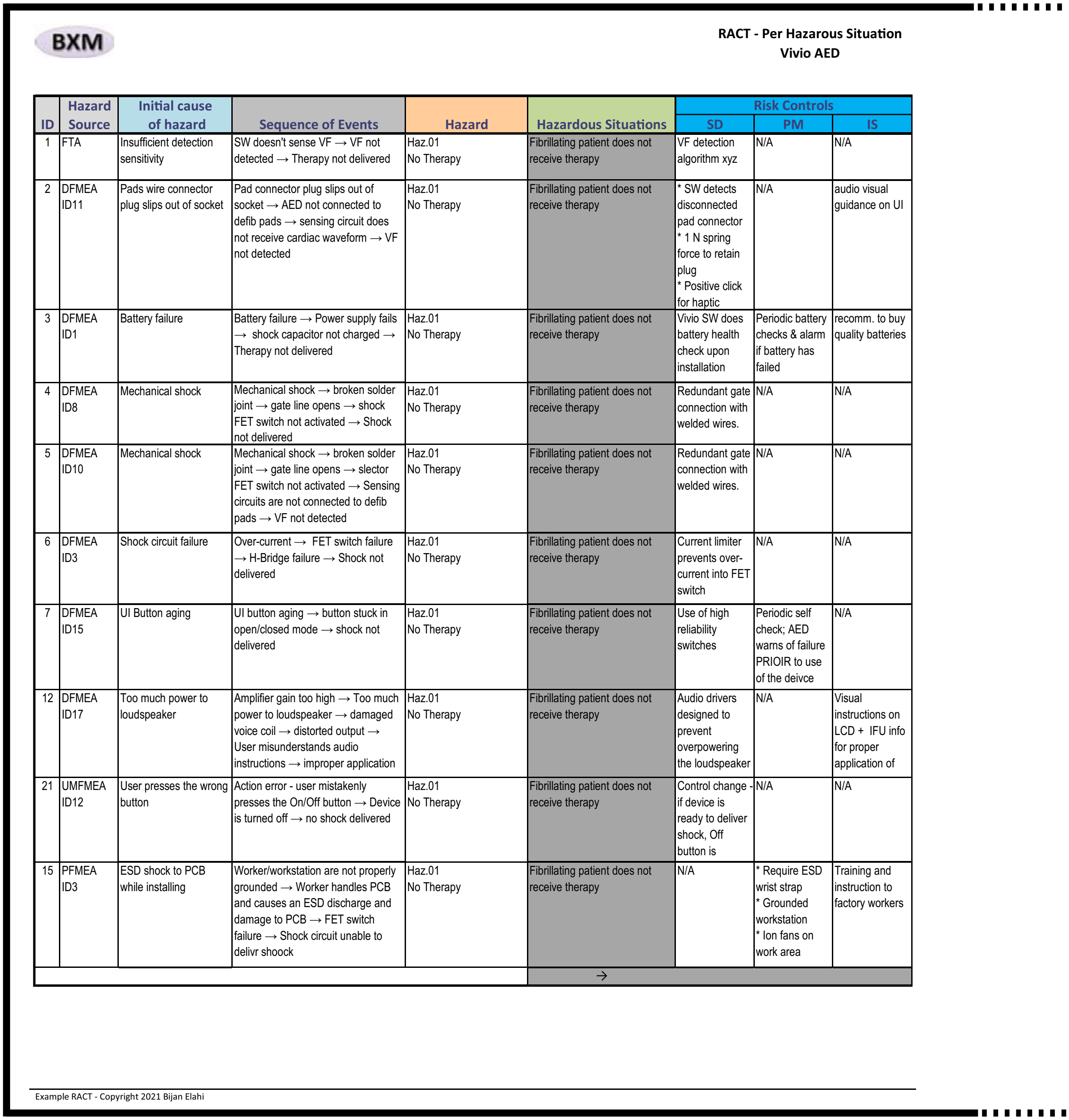
<This example RACT is truncated>

Example RACT - Copyright 2021 Bijan Elahi



Doc # 12347
Revision 1.0

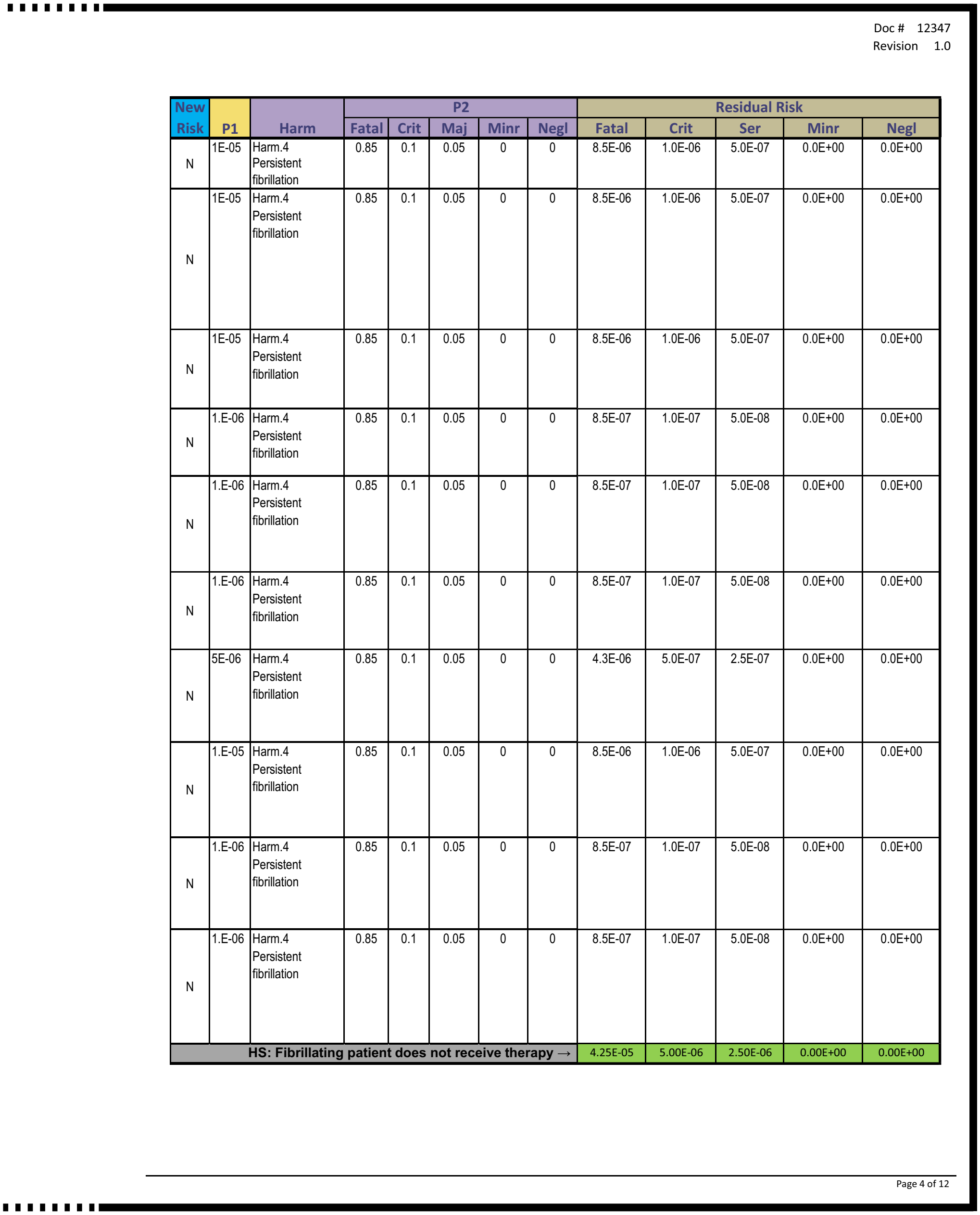
New Risk	P1	Harm	P2					Residual Risk				
			Fatal	Crit	Maj	Minr	Negl	Fatal	Crit	Maj	Minr	Negl
N	1.E-06	Harm.1 Burns (thermal)	0	0.01	0.7	0.2	0.09	0.0E+00	1.0E-08	7.0E-07	2.0E-07	9.0E-08
N	1.E-06	Harm.1 Burns (thermal)	0	0.01	0.7	0.2	0.09	0.0E+00	1.0E-08	7.0E-07	2.0E-07	9.0E-08
N	1.E-05	Harm.6 Laceration	0	0.02	0.9	0.07	0.01	0.0E+00	2.0E-07	9.0E-06	7.0E-07	1.0E-07
N	1.E-06	Harm.11 Electric Shock	0.008	0.04	0.111	0.041	0.8	8.0E-09	4.0E-08	1.1E-07	4.1E-08	8.0E-07
N	1.E-06	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-07	1.0E-07	5.0E-08	0.0E+00	0.0E+00



RACT - Per Hazarous Situation
Vivio AED

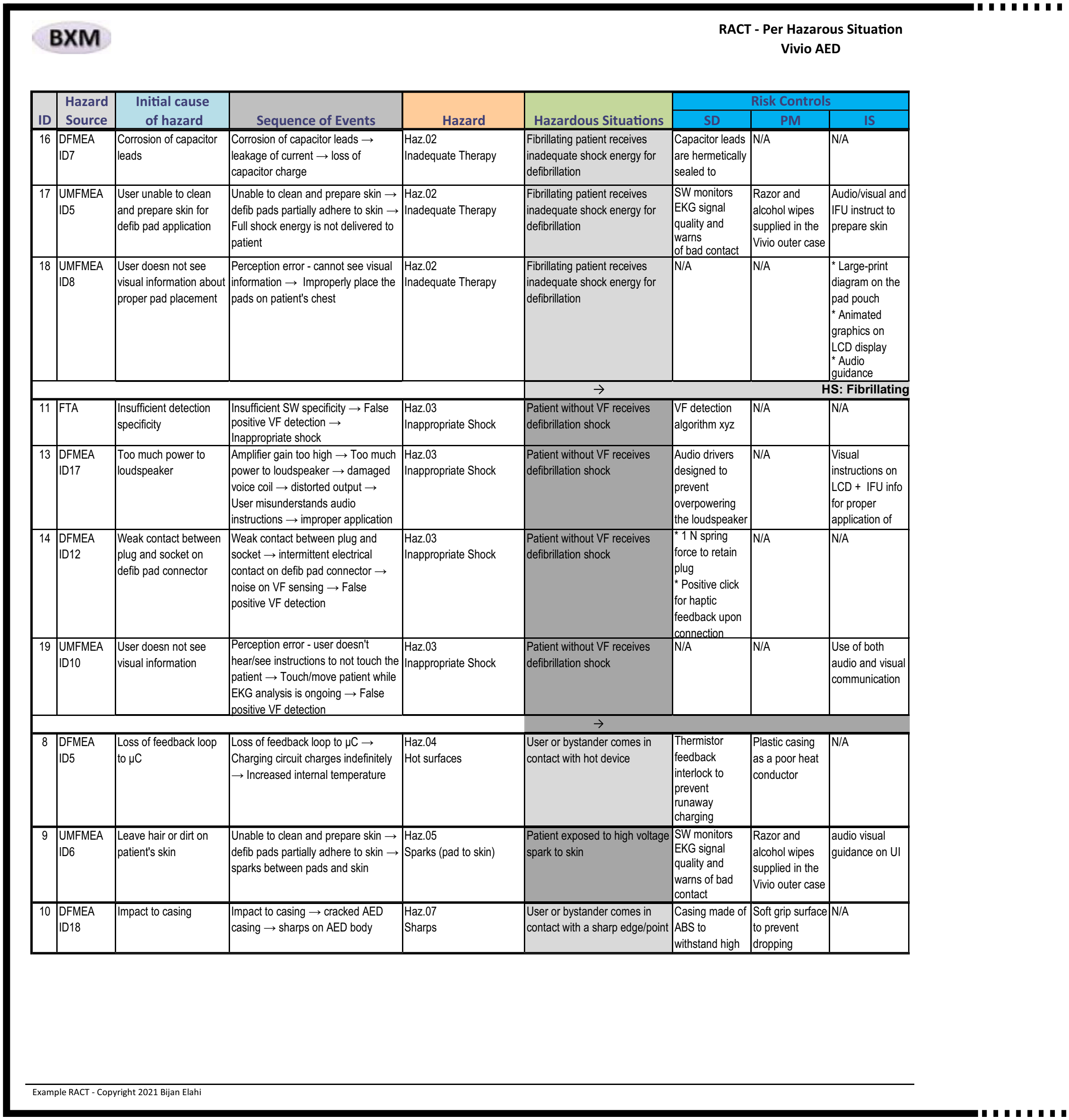
ID	Hazard Source	Initial cause of hazard	Sequence of Events	Hazard	Hazardous Situations	Risk Controls		
						SD	PM	IS
1	FTA	Insufficient detection sensitivity	SW doesn't sense VF → VF not detected → Therapy not delivered	Haz.01 No Therapy	Fibrillating patient does not receive therapy	VF detection algorithm xyz	N/A	N/A
2	DFMEA ID11	Pads wire connector plug slips out of socket	Pad connector plug slips out of socket → AED not connected to defib pads → sensing circuit does not receive cardiac waveform → VF not detected	Haz.01 No Therapy	Fibrillating patient does not receive therapy	* SW detects disconnected pad connector * 1 N spring force to retain plug * Positive click for haptic	N/A	audio visual guidance on UI
3	DFMEA ID1	Battery failure	Battery failure → Power supply fails → shock capacitor not charged → Therapy not delivered	Haz.01 No Therapy	Fibrillating patient does not receive therapy	Vivio SW does battery health check upon installation	Periodic battery checks & alarm if battery has failed	recomm. to buy quality batteries
4	DFMEA ID8	Mechanical shock	Mechanical shock → broken solder joint → gate line opens → shock FET switch not activated → Shock not delivered	Haz.01 No Therapy	Fibrillating patient does not receive therapy	Redundant gate connection with welded wires.	N/A	N/A
5	DFMEA ID10	Mechanical shock	Mechanical shock → broken solder joint → gate line opens → slector FET switch not activated → Sensing circuits are not connected to defib pads → VF not detected	Haz.01 No Therapy	Fibrillating patient does not receive therapy	Redundant gate connection with welded wires.	N/A	N/A
6	DFMEA ID3	Shock circuit failure	Over-current → FET switch failure → H-Bridge failure → Shock not delivered	Haz.01 No Therapy	Fibrillating patient does not receive therapy	Current limiter prevents over-current into FET switch	N/A	N/A
7	DFMEA ID15	UI Button aging	UI button aging → button stuck in open/closed mode → shock not delivered	Haz.01 No Therapy	Fibrillating patient does not receive therapy	Use of high reliability switches	Periodic self check; AED warns of failure PRIOIR to use of the deivce	N/A
12	DFMEA ID17	Too much power to loudspeaker	Amplifier gain too high → Too much power to loudspeaker → damaged voice coil → distorted output → User misunderstands audio instructions → improper application	Haz.01 No Therapy	Fibrillating patient does not receive therapy	Audio drivers designed to prevent overpowering the loudspeaker	N/A	Visual instructions on LCD + IFU info for proper application of
21	UMFMEA ID12	User presses the wrong button	Action error - user mistakenly presses the On/Off button → Device is turned off → no shock delivered	Haz.01 No Therapy	Fibrillating patient does not receive therapy	Control change - if device is ready to deliver shock, Off button is	N/A	N/A
15	PFMEA ID3	ESD shock to PCB while installing	Worker/workstation are not properly grounded → Worker handles PCB and causes an ESD discharge and damage to PCB → FET switch failure → Shock circuit unable to delivr shoock	Haz.01 No Therapy	Fibrillating patient does not receive therapy	N/A	* Require ESD wrist strap * Grounded workstation * Ion fans on work area	Training and instruction to factory workers
					→			

Example RACT - Copyright 2021 Bijan Elahi



Doc # 12347
Revision 1.0

New Risk	P1	Harm	P2					Residual Risk				
			Fatal	Crit	Maj	Minr	Negl	Fatal	Crit	Ser	Minr	Negl
N	1E-05	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-06	1.0E-06	5.0E-07	0.0E+00	0.0E+00
N	1E-05	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-06	1.0E-06	5.0E-07	0.0E+00	0.0E+00
N	1E-05	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-06	1.0E-06	5.0E-07	0.0E+00	0.0E+00
N	1.E-06	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-07	1.0E-07	5.0E-08	0.0E+00	0.0E+00
N	1.E-06	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-07	1.0E-07	5.0E-08	0.0E+00	0.0E+00
N	1.E-06	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-07	1.0E-07	5.0E-08	0.0E+00	0.0E+00
N	5E-06	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	4.3E-06	5.0E-07	2.5E-07	0.0E+00	0.0E+00
N	1.E-05	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-06	1.0E-06	5.0E-07	0.0E+00	0.0E+00
N	1.E-06	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-07	1.0E-07	5.0E-08	0.0E+00	0.0E+00
N	1.E-06	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-07	1.0E-07	5.0E-08	0.0E+00	0.0E+00
HS: Fibrillating patient does not receive therapy →								4.25E-05	5.00E-06	2.50E-06	0.00E+00	0.00E+00

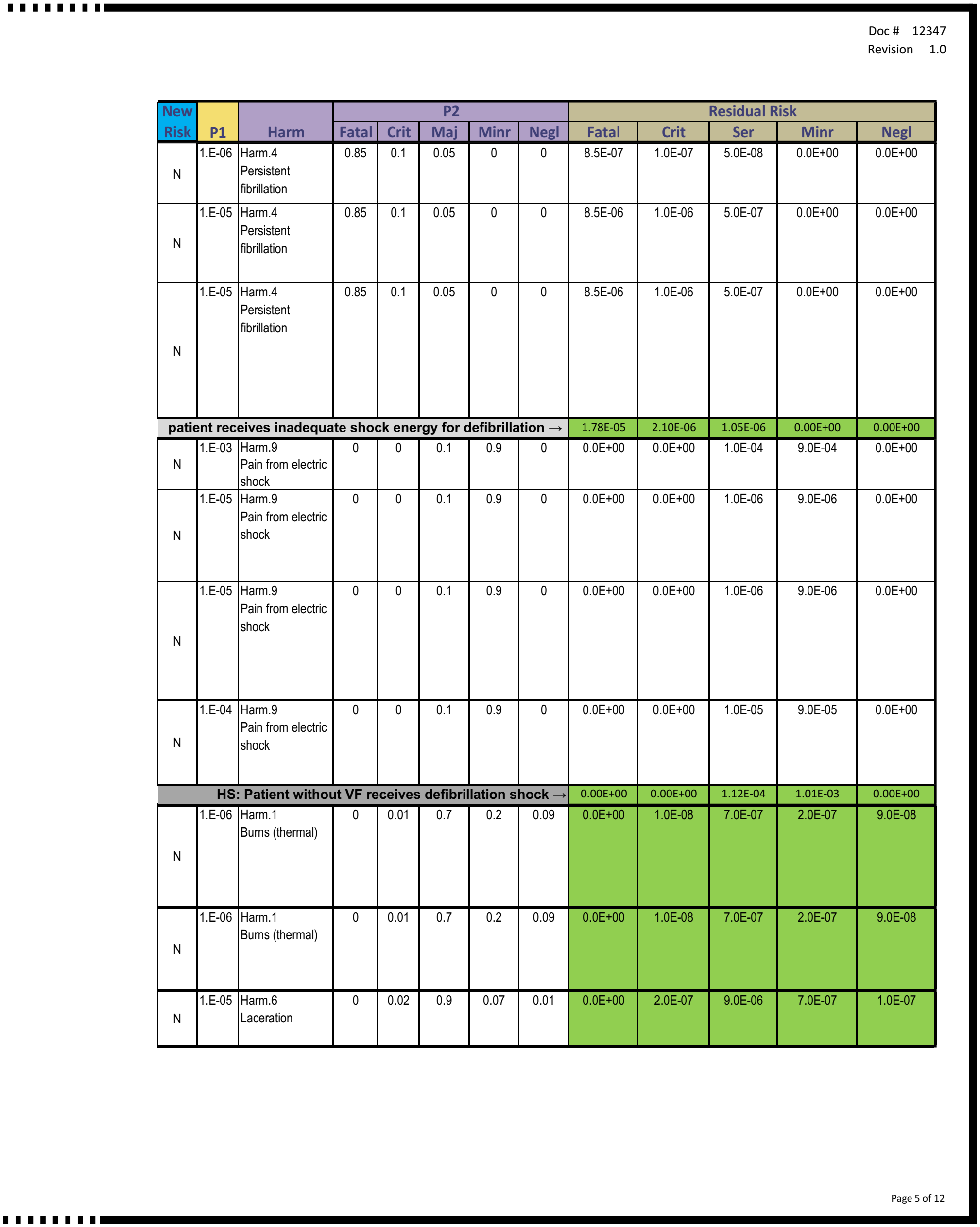


BXM

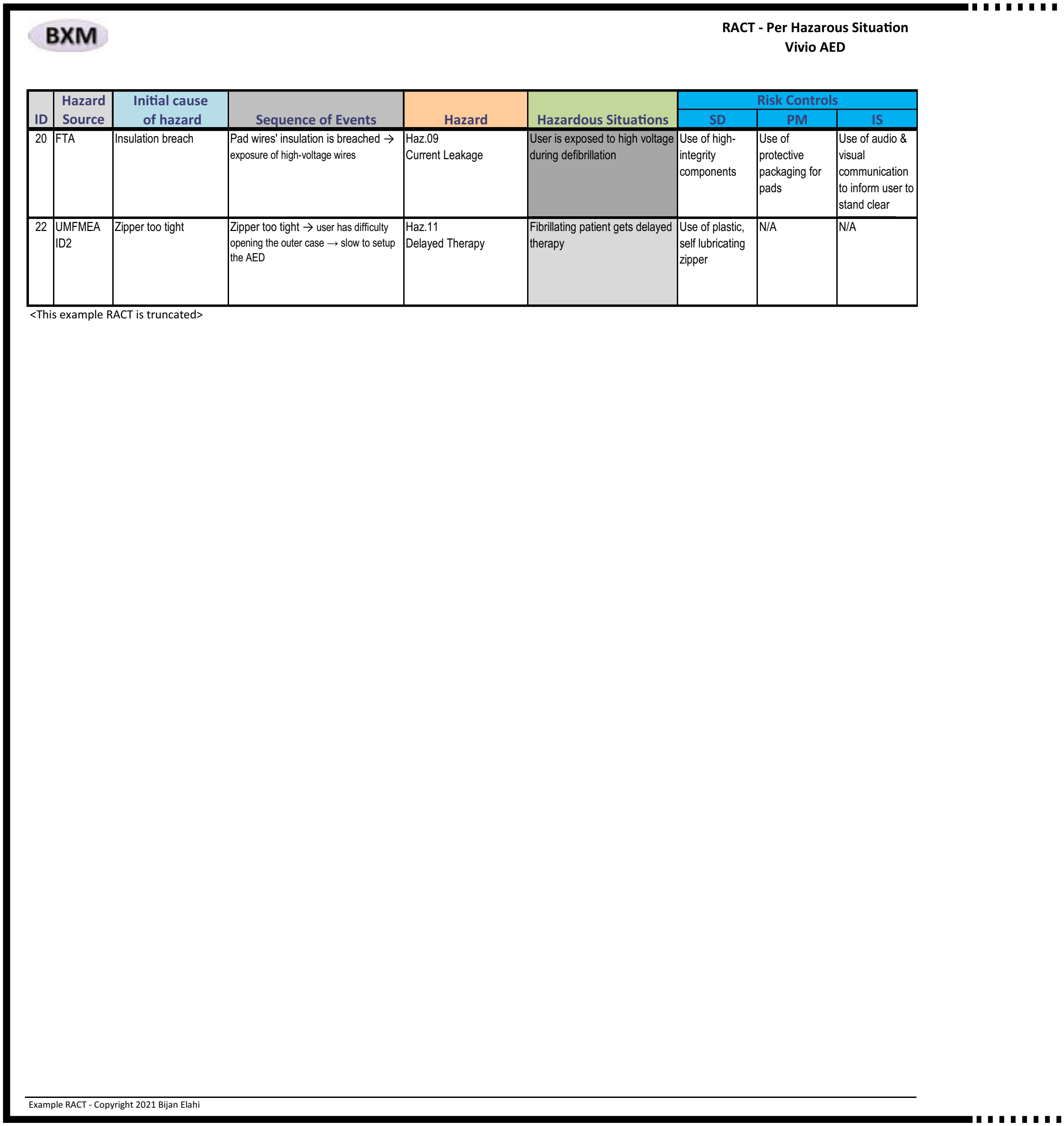
RACT - Per Hazarous Situation
Vivio AED

	Hazard	Initial cause				Risk Controls		
ID	Source	of hazard	Sequence of Events	Hazard	Hazardous Situations	SD	PM	IS
16	DFMEA ID7	Corrosion of capacitor leads	Corrosion of capacitor leads → leakage of current → loss of capacitor charge	Haz.02 Inadequate Therapy	Fibrillating patient receives inadequate shock energy for defibrillation	Capacitor leads are hermetically sealed to	N/A	N/A
17	UMFMEA ID5	User unable to clean and prepare skin for defib pad application	Unable to clean and prepare skin → defib pads partially adhere to skin → Full shock energy is not delivered to patient	Haz.02 Inadequate Therapy	Fibrillating patient receives inadequate shock energy for defibrillation	SW monitors EKG signal quality and warns of bad contact	Razor and alcohol wipes supplied in the Vivio outer case	Audio/visual and IFU instruct to prepare skin
18	UMFMEA ID8	User doesn not see visual information about proper pad placement	Perception error - cannot see visual information → Improperly place the pads on patient's chest	Haz.02 Inadequate Therapy	Fibrillating patient receives inadequate shock energy for defibrillation	N/A	N/A	* Large-print diagram on the pad pouch * Animated graphics on LCD display * Audio guidance
					→			HS: Fibrillating
11	FTA	Insufficient detection specificity	Insufficient SW specificity → False positive VF detection → Inappropriate shock	Haz.03 Inappropriate Shock	Patient without VF receives defibrillation shock	VF detection algorithm xyz	N/A	N/A
13	DFMEA ID17	Too much power to loudspeaker	Amplifier gain too high → Too much power to loudspeaker → damaged voice coil → distorted output → User misunderstands audio instructions → improper application	Haz.03 Inappropriate Shock	Patient without VF receives defibrillation shock	Audio drivers designed to prevent overpowering the loudspeaker	N/A	Visual instructions on LCD + IFU info for proper application of
14	DFMEA ID12	Weak contact between plug and socket on defib pad connector	Weak contact between plug and socket → intermittent electrical contact on defib pad connector → noise on VF sensing → False positive VF detection	Haz.03 Inappropriate Shock	Patient without VF receives defibrillation shock	* 1 N spring force to retain plug * Positive click for haptic feedback upon connection	N/A	N/A
19	UMFMEA ID10	User doesn not see visual information	Perception error - user doesn't hear/see instructions to not touch the patient → Touch/move patient while EKG analysis is ongoing → False positive VF detection	Haz.03 Inappropriate Shock	Patient without VF receives defibrillation shock	N/A	N/A	Use of both audio and visual communication
					→			
8	DFMEA ID5	Loss of feedback loop to µC	Loss of feedback loop to µC → Charging circuit charges indefinitely → Increased internal temperature	Haz.04 Hot surfaces	User or bystander comes in contact with hot device	Thermistor feedback interlock to prevent runaway charging	Plastic casing as a poor heat conductor	N/A
9	UMFMEA ID6	Leave hair or dirt on patient's skin	Unable to clean and prepare skin → defib pads partially adhere to skin → sparks between pads and skin	Haz.05 Sparks (pad to skin)	Patient exposed to high voltage spark to skin	SW monitors EKG signal quality and warns of bad contact	Razor and alcohol wipes supplied in the Vivio outer case	audio visual guidance on UI
10	DFMEA ID18	Impact to casing	Impact to casing → cracked AED casing → sharps on AED body	Haz.07 Sharps	User or bystander comes in contact with a sharp edge/point	Casing made of ABS to withstand high	Soft grip surface to prevent dropping	N/A

Example RACT - Copyright 2021 Bijan Elahi



New			P2					Residual Risk				
Risk	P1	Harm	Fatal	Crit	Maj	Minr	Negl	Fatal	Crit	Ser	Minr	Negl
N	1.E-06	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-07	1.0E-07	5.0E-08	0.0E+00	0.0E+00
N	1.E-05	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-06	1.0E-06	5.0E-07	0.0E+00	0.0E+00
N	1.E-05	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-06	1.0E-06	5.0E-07	0.0E+00	0.0E+00
patient receives inadequate shock energy for defibrillation →								1.78E-05	2.10E-06	1.05E-06	0.00E+00	0.00E+00
N	1.E-03	Harm.9 Pain from electric shock	0	0	0.1	0.9	0	0.0E+00	0.0E+00	1.0E-04	9.0E-04	0.0E+00
N	1.E-05	Harm.9 Pain from electric shock	0	0	0.1	0.9	0	0.0E+00	0.0E+00	1.0E-06	9.0E-06	0.0E+00
N	1.E-05	Harm.9 Pain from electric shock	0	0	0.1	0.9	0	0.0E+00	0.0E+00	1.0E-06	9.0E-06	0.0E+00
N	1.E-04	Harm.9 Pain from electric shock	0	0	0.1	0.9	0	0.0E+00	0.0E+00	1.0E-05	9.0E-05	0.0E+00
HS: Patient without VF receives defibrillation shock →								0.00E+00	0.00E+00	1.12E-04	1.01E-03	0.00E+00
N	1.E-06	Harm.1 Burns (thermal)	0	0.01	0.7	0.2	0.09	0.0E+00	1.0E-08	7.0E-07	2.0E-07	9.0E-08
N	1.E-06	Harm.1 Burns (thermal)	0	0.01	0.7	0.2	0.09	0.0E+00	1.0E-08	7.0E-07	2.0E-07	9.0E-08
N	1.E-05	Harm.6 Laceration	0	0.02	0.9	0.07	0.01	0.0E+00	2.0E-07	9.0E-06	7.0E-07	1.0E-07



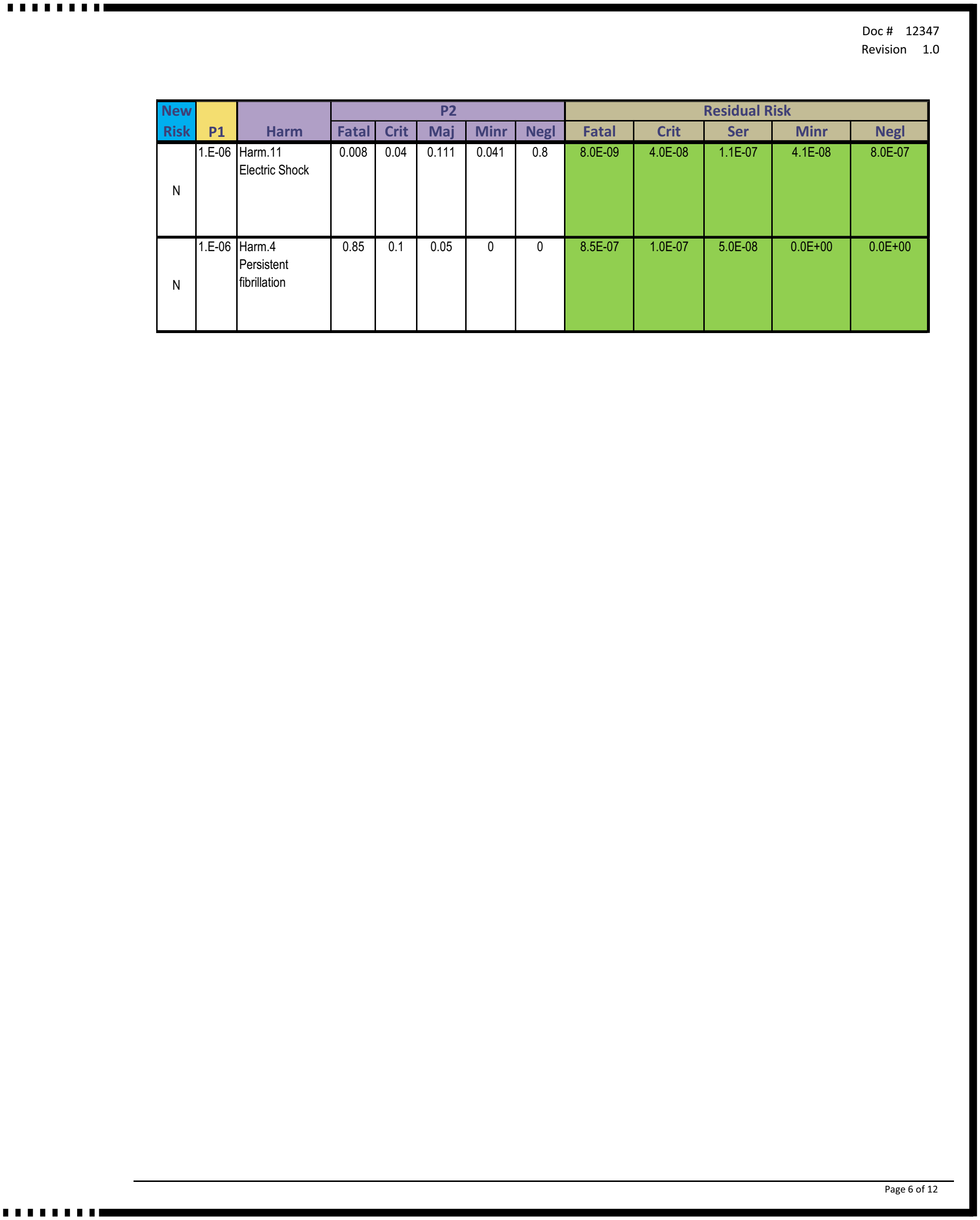
BXM

RACT - Per Hazarous Situation
Vivio AED

	Hazard	Initial cause				Risk Controls		
ID	Source	of hazard	Sequence of Events	Hazard	Hazardous Situations	SD	PM	IS
20	FTA	Insulation breach	Pad wires' insulation is breached → exposure of high-voltage wires	Haz.09 Current Leakage	User is exposed to high voltage during defibrillation	Use of high-integrity components	Use of protective packaging for pads	Use of audio & visual communication to inform user to stand clear
22	UMFMEA ID2	Zipper too tight	Zipper too tight → user has difficulty opening the outer case → slow to setup the AED	Haz.11 Delayed Therapy	Fibrillating patient gets delayed therapy	Use of plastic, self lubricating zipper	N/A	N/A

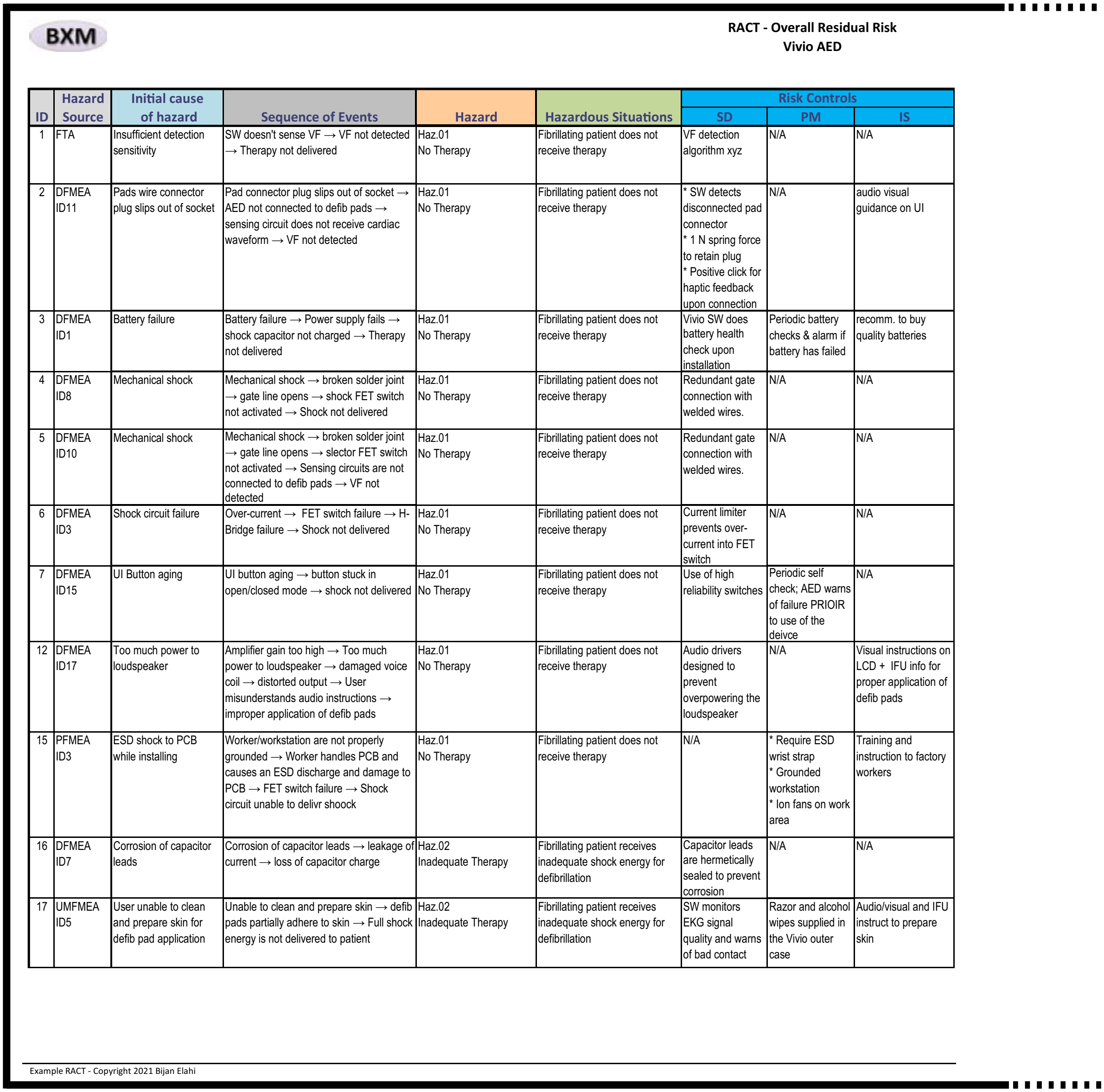
<This example RACT is truncated>

Example RACT - Copyright 2021 Bijan Elahi



Doc # 12347
Revision 1.0

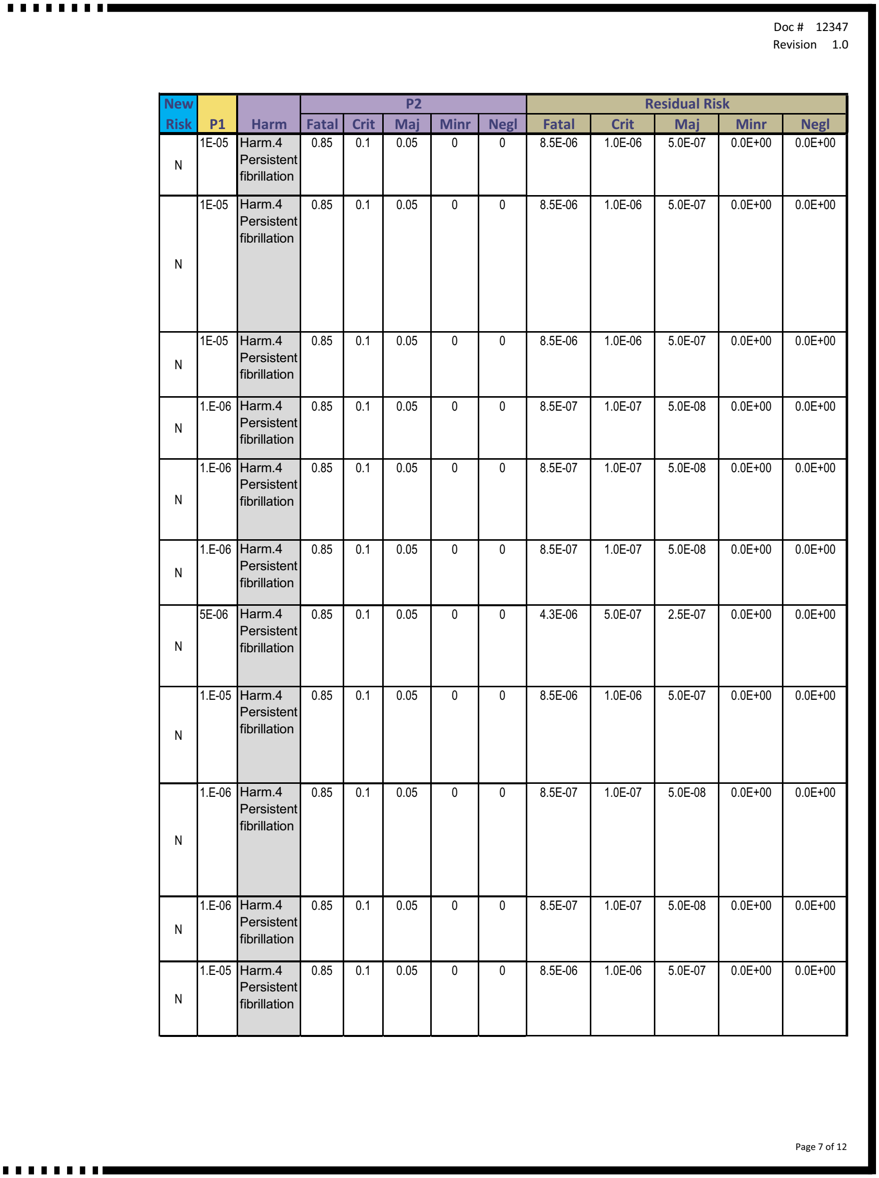
New			P2					Residual Risk				
Risk	P1	Harm	Fatal	Crit	Maj	Minr	Negl	Fatal	Crit	Ser	Minr	Negl
N	1.E-06	Harm.11 Electric Shock	0.008	0.04	0.111	0.041	0.8	8.0E-09	4.0E-08	1.1E-07	4.1E-08	8.0E-07
N	1.E-06	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-07	1.0E-07	5.0E-08	0.0E+00	0.0E+00



RACT - Overall Residual Risk
Vivio AED

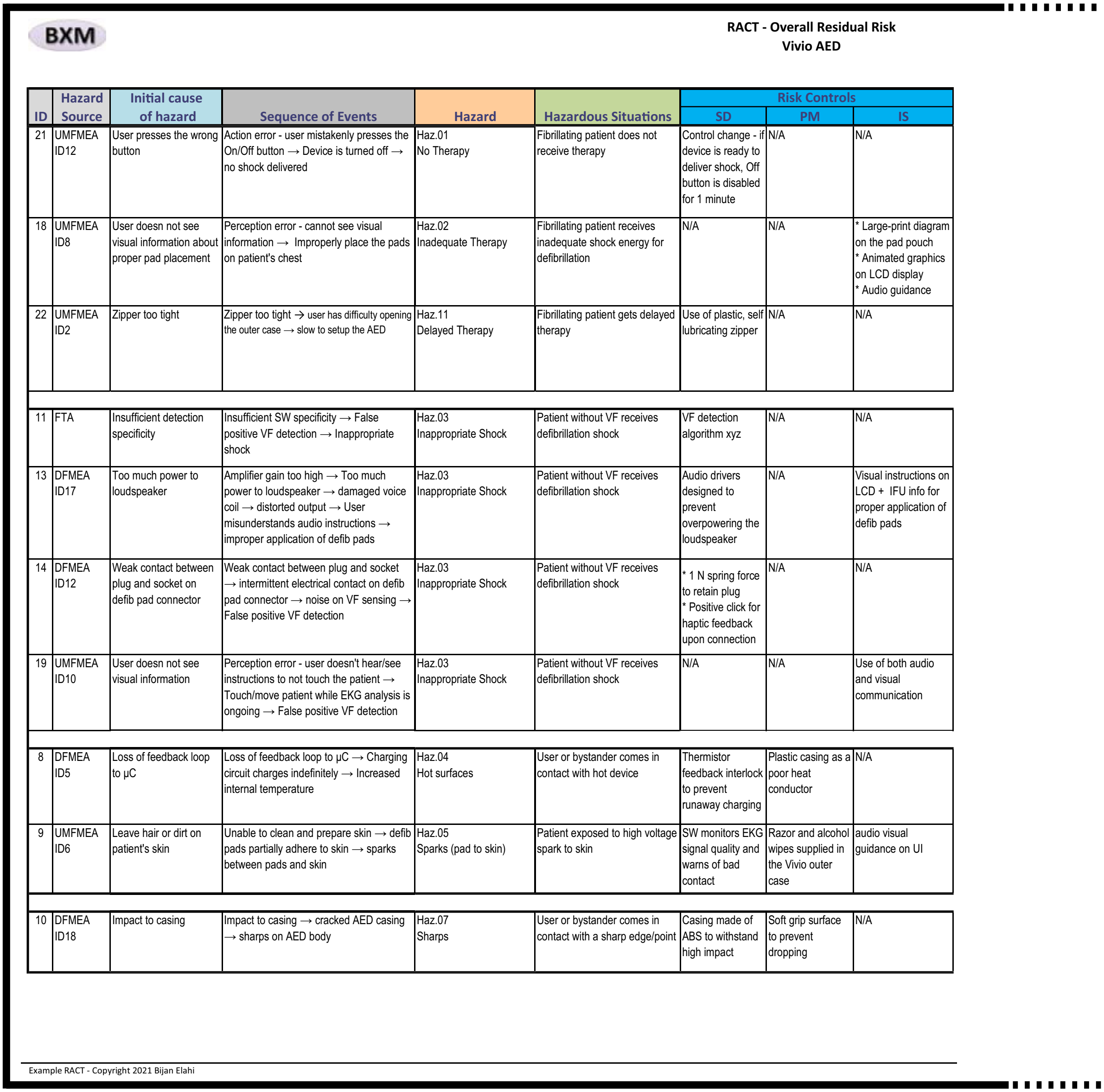
	Hazard	Initial cause				Risk Controls		
ID	Source	of hazard	Sequence of Events	Hazard	Hazardous Situations	SD	PM	IS
1	FTA	Insufficient detection sensitivity	SW doesn't sense VF → VF not detected → Therapy not delivered	Haz.01 No Therapy	Fibrillating patient does not receive therapy	VF detection algorithm xyz	N/A	N/A
2	DFMEA ID11	Pads wire connector plug slips out of socket	Pad connector plug slips out of socket → AED not connected to defib pads → sensing circuit does not receive cardiac waveform → VF not detected	Haz.01 No Therapy	Fibrillating patient does not receive therapy	* SW detects disconnected pad connector * 1 N spring force to retain plug * Positive click for haptic feedback upon connection	N/A	audio visual guidance on UI
3	DFMEA ID1	Battery failure	Battery failure → Power supply fails → shock capacitor not charged → Therapy not delivered	Haz.01 No Therapy	Fibrillating patient does not receive therapy	Vivio SW does battery health check upon installation	Periodic battery checks & alarm if battery has failed	recomm. to buy quality batteries
4	DFMEA ID8	Mechanical shock	Mechanical shock → broken solder joint → gate line opens → shock FET switch not activated → Shock not delivered	Haz.01 No Therapy	Fibrillating patient does not receive therapy	Redundant gate connection with welded wires.	N/A	N/A
5	DFMEA ID10	Mechanical shock	Mechanical shock → broken solder joint → gate line opens → slector FET switch not activated → Sensing circuits are not connected to defib pads → VF not detected	Haz.01 No Therapy	Fibrillating patient does not receive therapy	Redundant gate connection with welded wires.	N/A	N/A
6	DFMEA ID3	Shock circuit failure	Over-current → FET switch failure → H-Bridge failure → Shock not delivered	Haz.01 No Therapy	Fibrillating patient does not receive therapy	Current limiter prevents over-current into FET switch	N/A	N/A
7	DFMEA ID15	UI Button aging	UI button aging → button stuck in open/closed mode → shock not delivered	Haz.01 No Therapy	Fibrillating patient does not receive therapy	Use of high reliability switches	Periodic self check; AED warns of failure PRIOIR to use of the deivce	N/A
12	DFMEA ID17	Too much power to loudspeaker	Amplifier gain too high → Too much power to loudspeaker → damaged voice coil → distorted output → User misunderstands audio instructions → improper application of defib pads	Haz.01 No Therapy	Fibrillating patient does not receive therapy	Audio drivers designed to prevent overpowering the loudspeaker	N/A	Visual instructions on LCD + IFU info for proper application of defib pads
15	PFMEA ID3	ESD shock to PCB while installing	Worker/workstation are not properly grounded → Worker handles PCB and causes an ESD discharge and damage to PCB → FET switch failure → Shock circuit unable to delivr shoock	Haz.01 No Therapy	Fibrillating patient does not receive therapy	N/A	* Require ESD wrist strap * Grounded workstation * Ion fans on work area	Training and instruction to factory workers
16	DFMEA ID7	Corrosion of capacitor leads	Corrosion of capacitor leads → leakage of current → loss of capacitor charge	Haz.02 Inadequate Therapy	Fibrillating patient receives inadequate shock energy for defibrillation	Capacitor leads are hermetically sealed to prevent corrosion	N/A	N/A
17	UMFMEA ID5	User unable to clean and prepare skin for defib pad application	Unable to clean and prepare skin → defib pads partially adhere to skin → Full shock energy is not delivered to patient	Haz.02 Inadequate Therapy	Fibrillating patient receives inadequate shock energy for defibrillation	SW monitors EKG signal quality and warns of bad contact	Razor and alcohol wipes supplied in the Vivio outer case	Audio/visual and IFU instruct to prepare skin

Example RACT - Copyright 2021 Bijan Elahi



Doc # 12347
Revision 1.0

New			P2					Residual Risk				
Risk	P1	Harm	Fatal	Crit	Maj	Minr	Negl	Fatal	Crit	Maj	Minr	Negl
N	1E-05	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-06	1.0E-06	5.0E-07	0.0E+00	0.0E+00
N	1E-05	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-06	1.0E-06	5.0E-07	0.0E+00	0.0E+00
N	1E-05	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-06	1.0E-06	5.0E-07	0.0E+00	0.0E+00
N	1.E-06	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-07	1.0E-07	5.0E-08	0.0E+00	0.0E+00
N	1.E-06	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-07	1.0E-07	5.0E-08	0.0E+00	0.0E+00
N	1.E-06	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-07	1.0E-07	5.0E-08	0.0E+00	0.0E+00
N	5E-06	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	4.3E-06	5.0E-07	2.5E-07	0.0E+00	0.0E+00
N	1.E-05	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-06	1.0E-06	5.0E-07	0.0E+00	0.0E+00
N	1.E-06	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-07	1.0E-07	5.0E-08	0.0E+00	0.0E+00
N	1.E-06	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-07	1.0E-07	5.0E-08	0.0E+00	0.0E+00
N	1.E-05	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-06	1.0E-06	5.0E-07	0.0E+00	0.0E+00

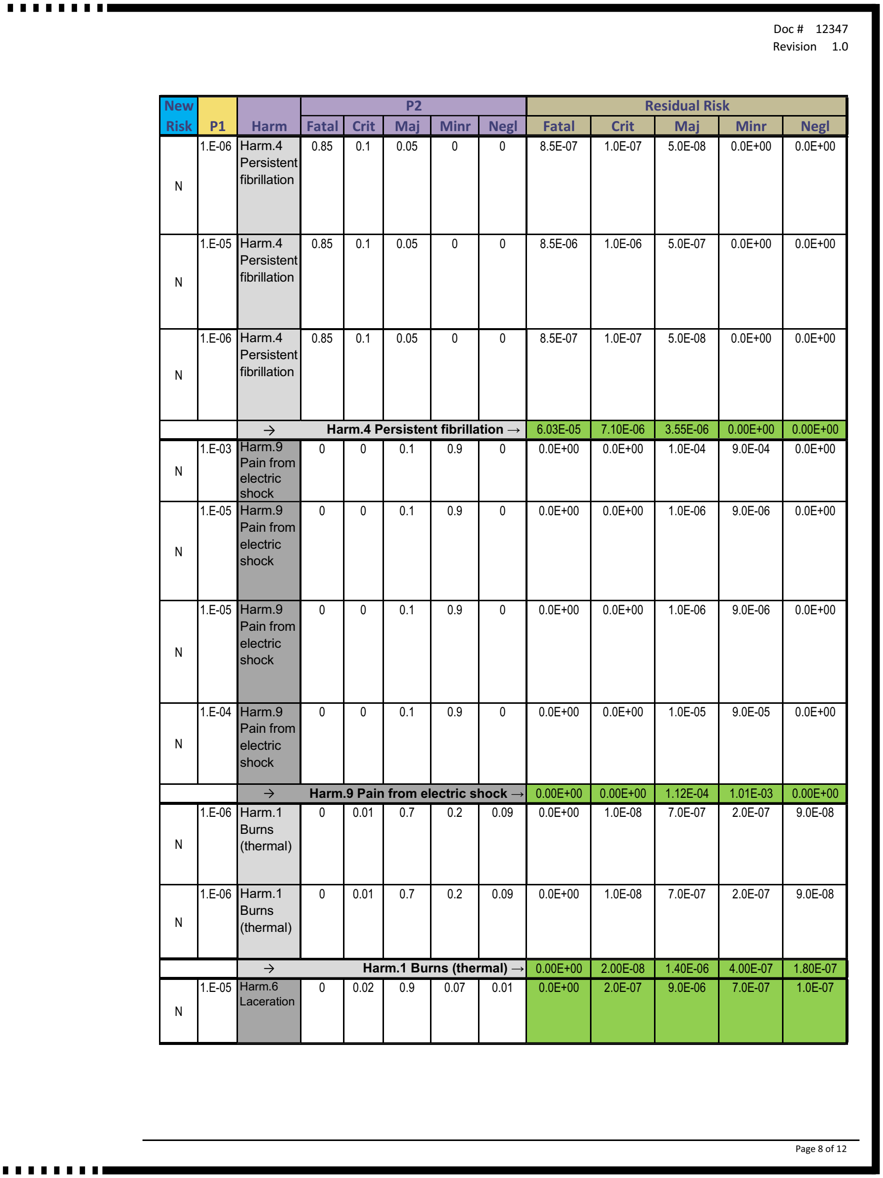


BXM

RACT - Overall Residual Risk
Vivio AED

ID	Hazard Source	Initial cause of hazard	Sequence of Events	Hazard	Hazardous Situations	Risk Controls		
						SD	PM	IS
21	UMFMEA ID12	User presses the wrong button	Action error - user mistakenly presses the On/Off button → Device is turned off → no shock delivered	Haz.01 No Therapy	Fibrillating patient does not receive therapy	Control change - if device is ready to deliver shock, Off button is disabled for 1 minute	N/A	N/A
18	UMFMEA ID8	User doesn not see visual information about proper pad placement	Perception error - cannot see visual information → Improperly place the pads on patient's chest	Haz.02 Inadequate Therapy	Fibrillating patient receives inadequate shock energy for defibrillation	N/A	N/A	* Large-print diagram on the pad pouch * Animated graphics on LCD display * Audio guidance
22	UMFMEA ID2	Zipper too tight	Zipper too tight → user has difficulty opening the outer case → slow to setup the AED	Haz.11 Delayed Therapy	Fibrillating patient gets delayed therapy	Use of plastic, self lubricating zipper	N/A	N/A
11	FTA	Insufficient detection specificity	Insufficient SW specificity → False positive VF detection → Inappropriate shock	Haz.03 Inappropriate Shock	Patient without VF receives defibrillation shock	VF detection algorithm xyz	N/A	N/A
13	DFMEA ID17	Too much power to loudspeaker	Amplifier gain too high → Too much power to loudspeaker → damaged voice coil → distorted output → User misunderstands audio instructions → improper application of defib pads	Haz.03 Inappropriate Shock	Patient without VF receives defibrillation shock	Audio drivers designed to prevent overpowering the loudspeaker	N/A	Visual instructions on LCD + IFU info for proper application of defib pads
14	DFMEA ID12	Weak contact between plug and socket on defib pad connector	Weak contact between plug and socket → intermittent electrical contact on defib pad connector → noise on VF sensing → False positive VF detection	Haz.03 Inappropriate Shock	Patient without VF receives defibrillation shock	* 1 N spring force to retain plug * Positive click for haptic feedback upon connection	N/A	N/A
19	UMFMEA ID10	User doesn not see visual information	Perception error - user doesn't hear/see instructions to not touch the patient → Touch/move patient while EKG analysis is ongoing → False positive VF detection	Haz.03 Inappropriate Shock	Patient without VF receives defibrillation shock	N/A	N/A	Use of both audio and visual communication
8	DFMEA ID5	Loss of feedback loop to µC	Loss of feedback loop to µC → Charging circuit charges indefinitely → Increased internal temperature	Haz.04 Hot surfaces	User or bystander comes in contact with hot device	Thermistor feedback interlock to prevent runaway charging	Plastic casing as a poor heat conductor	N/A
9	UMFMEA ID6	Leave hair or dirt on patient's skin	Unable to clean and prepare skin → defib pads partially adhere to skin → sparks between pads and skin	Haz.05 Sparks (pad to skin)	Patient exposed to high voltage spark to skin	SW monitors EKG signal quality and warns of bad contact	Razor and alcohol wipes supplied in the Vivio outer case	audio visual guidance on UI
10	DFMEA ID18	Impact to casing	Impact to casing → cracked AED casing → sharps on AED body	Haz.07 Sharps	User or bystander comes in contact with a sharp edge/point	Casing made of ABS to withstand high impact	Soft grip surface to prevent dropping	N/A

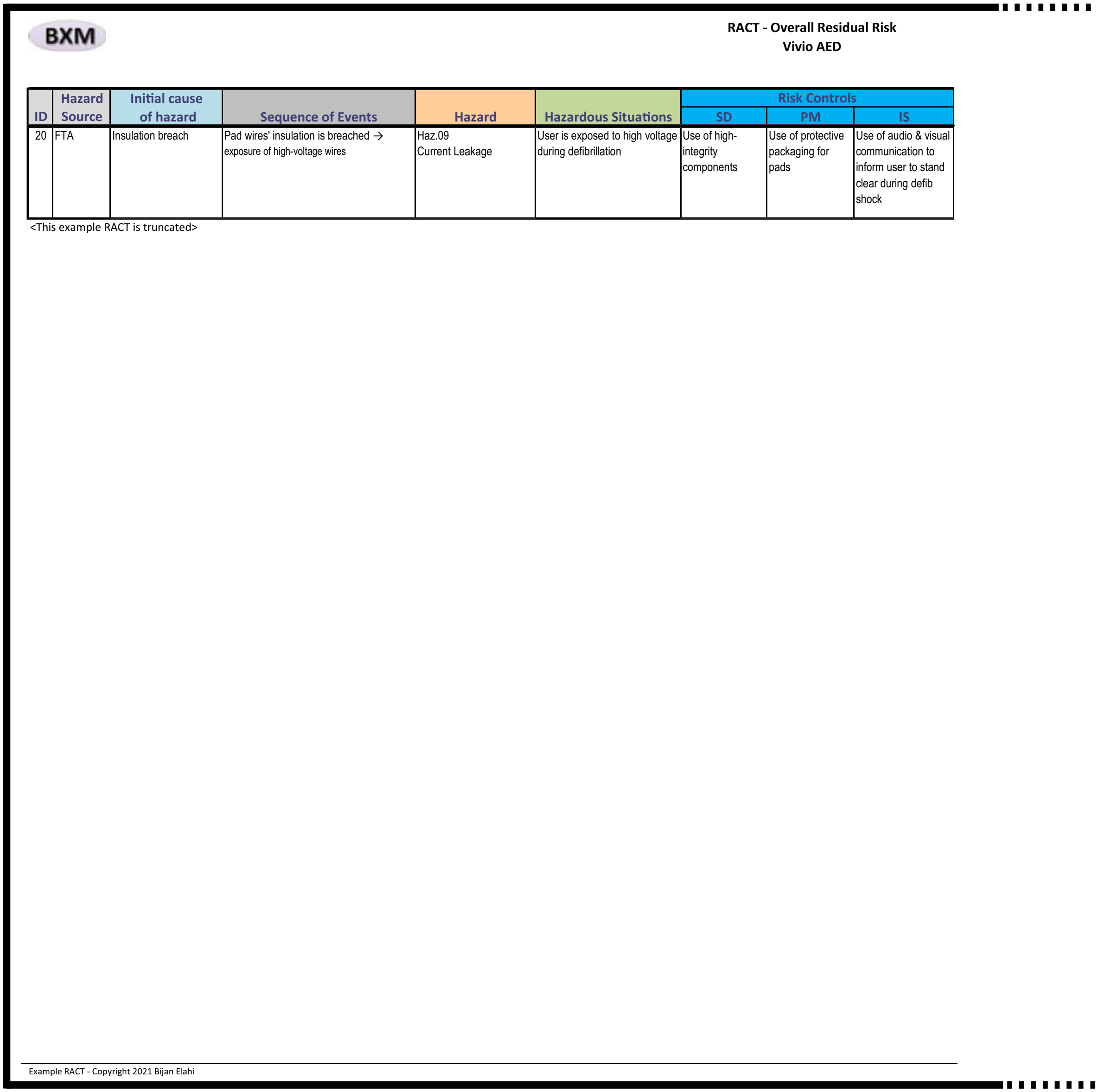
Example RACT - Copyright 2021 Bijan Elahi



Doc # 12347
Revision 1.0

New			P2					Residual Risk				
Risk	P1	Harm	Fatal	Crit	Maj	Minr	Negl	Fatal	Crit	Maj	Minr	Negl
N	1.E-06	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-07	1.0E-07	5.0E-08	0.0E+00	0.0E+00
N	1.E-05	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-06	1.0E-06	5.0E-07	0.0E+00	0.0E+00
N	1.E-06	Harm.4 Persistent fibrillation	0.85	0.1	0.05	0	0	8.5E-07	1.0E-07	5.0E-08	0.0E+00	0.0E+00
		→ **Harm.4 Persistent fibrillation →**						6.03E-05	7.10E-06	3.55E-06	0.00E+00	0.00E+00
N	1.E-03	Harm.9 Pain from electric shock	0	0	0.1	0.9	0	0.0E+00	0.0E+00	1.0E-04	9.0E-04	0.0E+00
N	1.E-05	Harm.9 Pain from electric shock	0	0	0.1	0.9	0	0.0E+00	0.0E+00	1.0E-06	9.0E-06	0.0E+00
N	1.E-05	Harm.9 Pain from electric shock	0	0	0.1	0.9	0	0.0E+00	0.0E+00	1.0E-06	9.0E-06	0.0E+00
N	1.E-04	Harm.9 Pain from electric shock	0	0	0.1	0.9	0	0.0E+00	0.0E+00	1.0E-05	9.0E-05	0.0E+00
		→ **Harm.9 Pain from electric shock →**						0.00E+00	0.00E+00	1.12E-04	1.01E-03	0.00E+00
N	1.E-06	Harm.1 Burns (thermal)	0	0.01	0.7	0.2	0.09	0.0E+00	1.0E-08	7.0E-07	2.0E-07	9.0E-08
N	1.E-06	Harm.1 Burns (thermal)	0	0.01	0.7	0.2	0.09	0.0E+00	1.0E-08	7.0E-07	2.0E-07	9.0E-08
		→ **Harm.1 Burns (thermal) →**						0.00E+00	2.00E-08	1.40E-06	4.00E-07	1.80E-07
N	1.E-05	Harm.6 Laceration	0	0.02	0.9	0.07	0.01	0.0E+00	2.0E-07	9.0E-06	7.0E-07	1.0E-07

Page 8 of 12

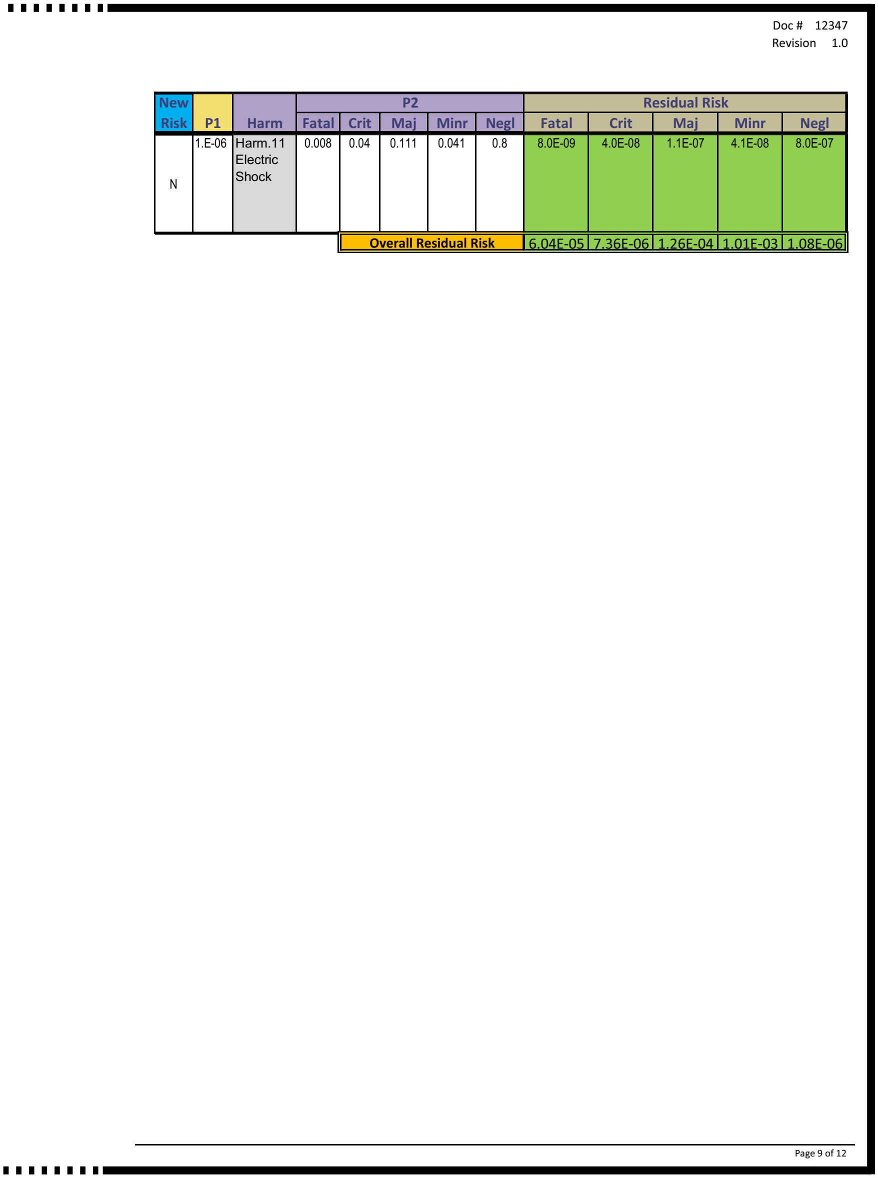


BXM

RACT - Overall Residual Risk
Vivio AED

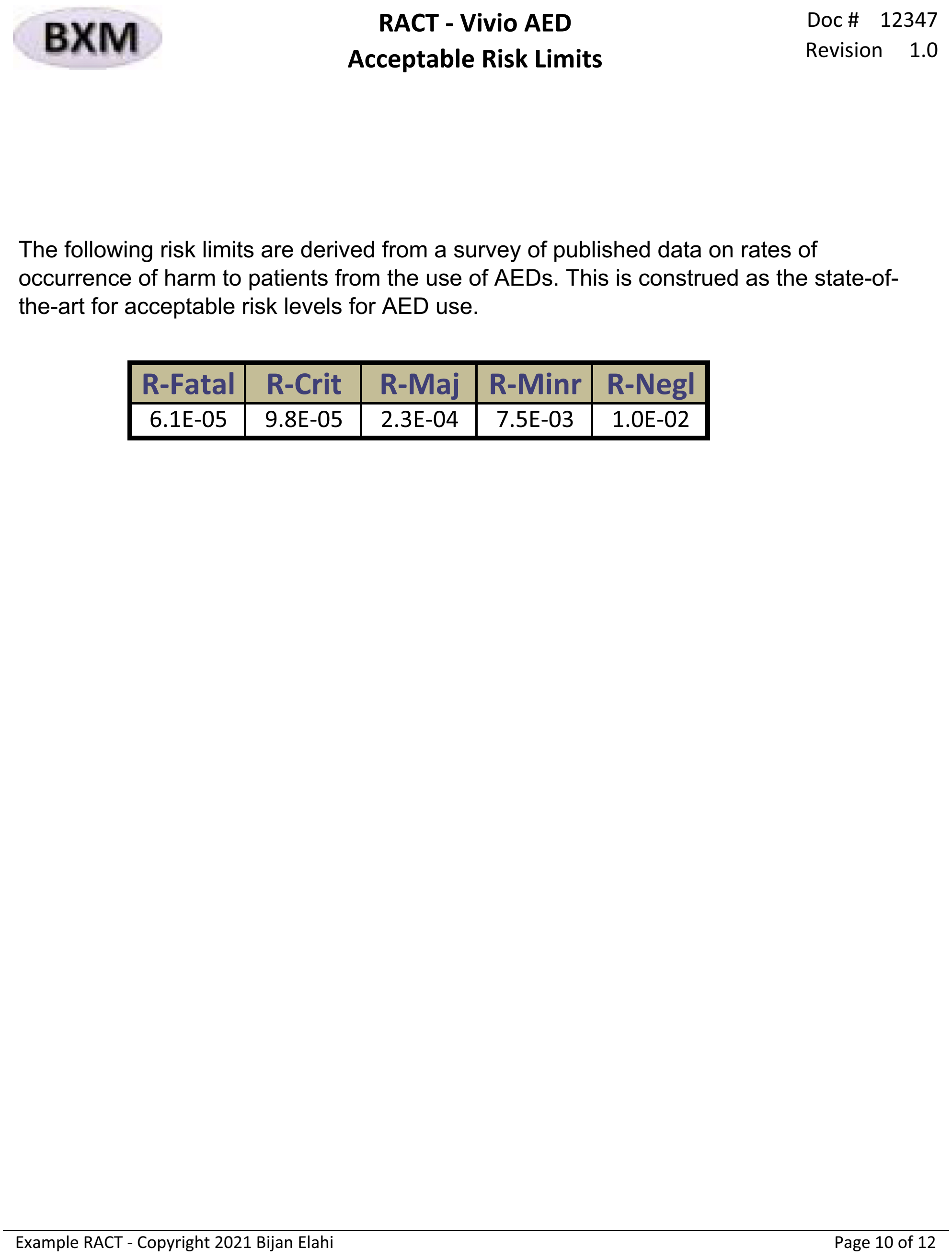
	Hazard	Initial cause				Risk Controls		
ID	Source	of hazard	Sequence of Events	Hazard	Hazardous Situations	SD	PM	IS
20	FTA	Insulation breach	Pad wires' insulation is breached → exposure of high-voltage wires	Haz.09 Current Leakage	User is exposed to high voltage during defibrillation	Use of high-integrity components	Use of protective packaging for pads	Use of audio & visual communication to inform user to stand clear during defib shock

<This example RACT is truncated>



Doc # 12347
Revision 1.0

New			P2					Residual Risk				
Risk	P1	Harm	Fatal	Crit	Maj	Minr	Negl	Fatal	Crit	Maj	Minr	Negl
N	1.E-06	Harm.11 Electric Shock	0.008	0.04	0.111	0.041	0.8	8.0E-09	4.0E-08	1.1E-07	4.1E-08	8.0E-07
				Overall Residual Risk				6.04E-05	7.36E-06	1.26E-04	1.01E-03	1.08E-06



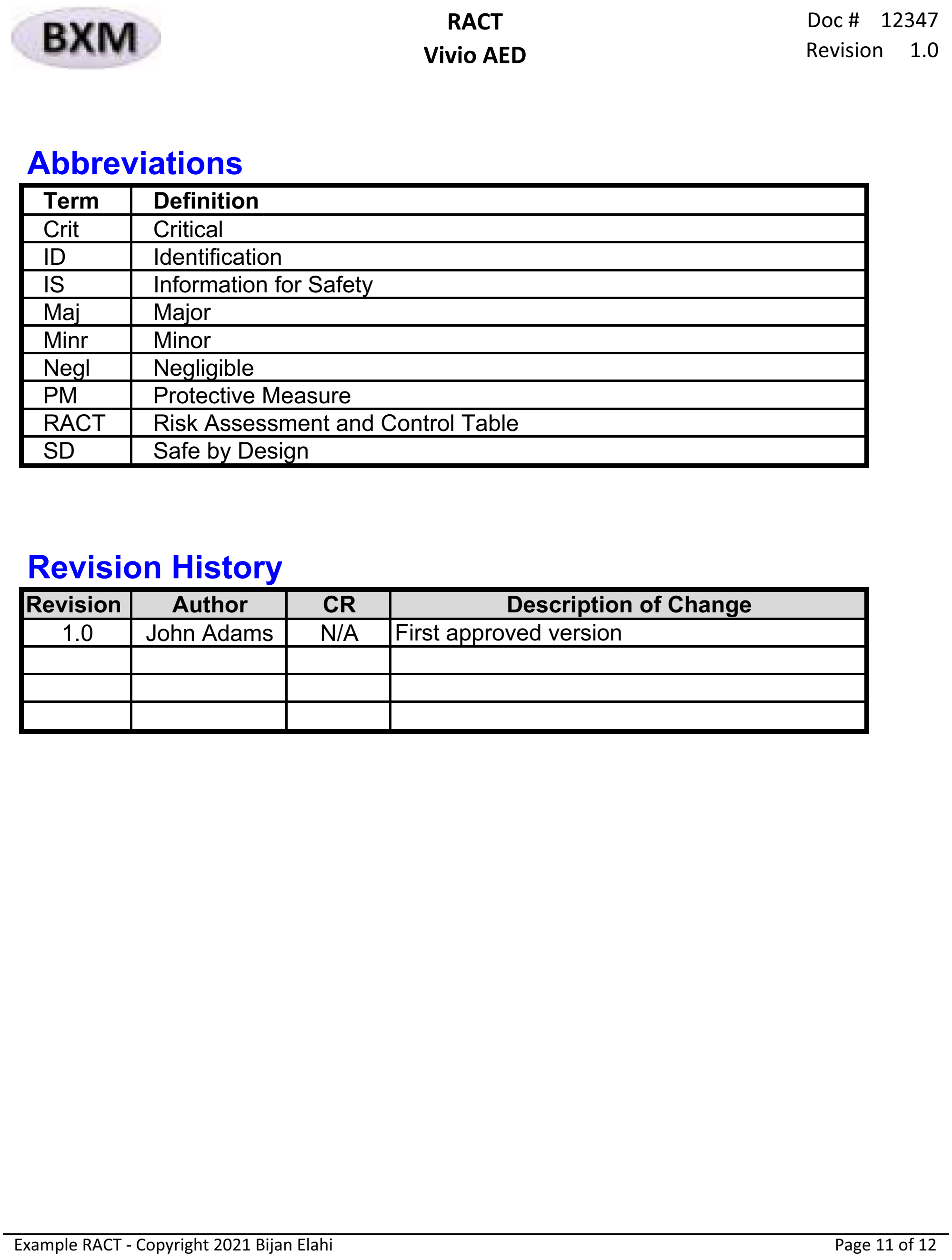
BXM

RACT - Vivio AED
Acceptable Risk Limits

Doc # 12347
Revision 1.0

The following risk limits are derived from a survey of published data on rates of occurrence of harm to patients from the use of AEDs. This is construed as the state-of-the-art for acceptable risk levels for AED use.

R-Fatal	R-Crit	R-Maj	R-Minr	R-Negl
6.1E-05	9.8E-05	2.3E-04	7.5E-03	1.0E-02



BXM

RACT
Vivio AED

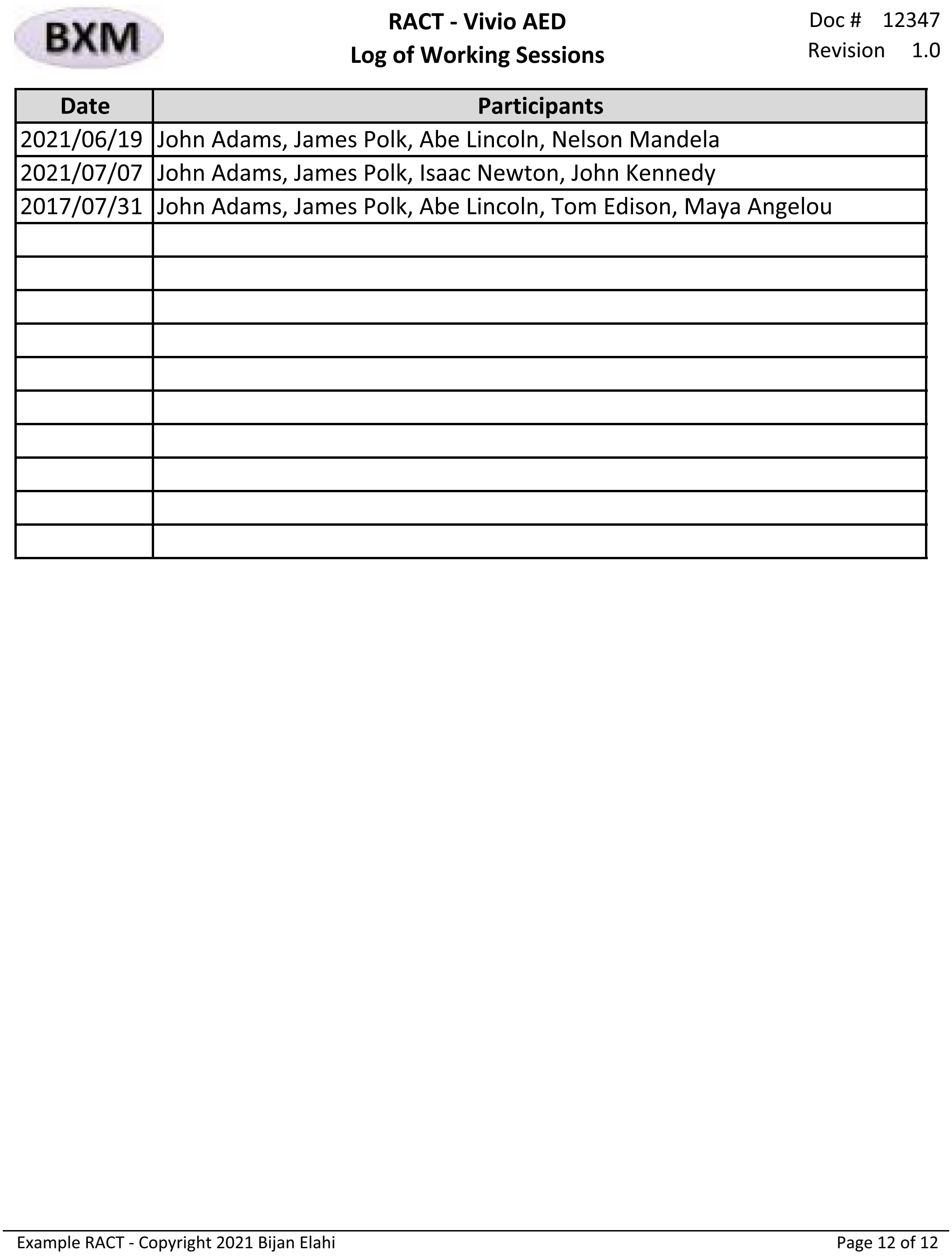
Doc # 12347
Revision 1.0

Abbreviations

Term	Definition
Crit	Critical
ID	Identification
IS	Information for Safety
Maj	Major
Minr	Minor
Negl	Negligible
PM	Protective Measure
RACT	Risk Assessment and Control Table
SD	Safe by Design

Revision History

Revision	Author	CR	Description of Change
1.0	John Adams	N/A	First approved version



RACT - Vivio AED
Log of Working Sessions

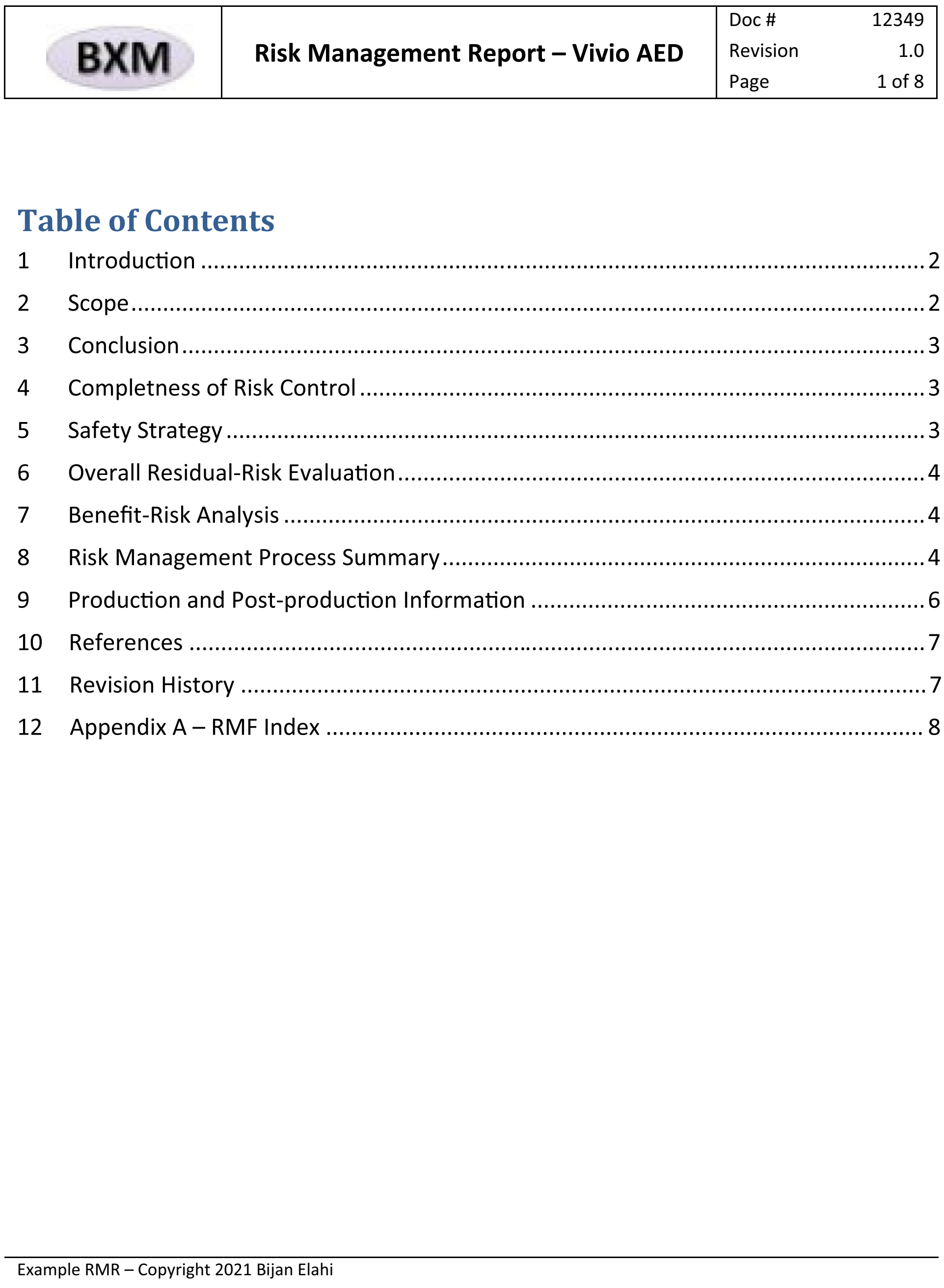
Doc # 12347
Revision 1.0

Date	Participants
2021/06/19	John Adams, James Polk, Abe Lincoln, Nelson Mandela
2021/07/07	John Adams, James Polk, Isaac Newton, John Kennedy
2017/07/31	John Adams, James Polk, Abe Lincoln, Tom Edison, Maya Angelou

Example RACT - Copyright 2021 Bijan Elahi

Page 12 of 12

C.13 RISK MANAGEMENT REPORT



BXM	**Risk Management Report – Vivio AED**	Doc #	12349
		Revision	1.0
		Page	1 of 8

Table of Contents

BXM	Risk Management Report – Vivio AED	Doc # Revision Page	12349 1.0 2 of 8

1 INTRODUCTION

This Risk Management Report (RMR), which fulfills the requirements of ISO 14971:2019 section 9, is intended to provide an overview of the outcome of the Risk Management process for Vivio AED. Details of the Risk Management activities are available in the Risk Management File [RMF].

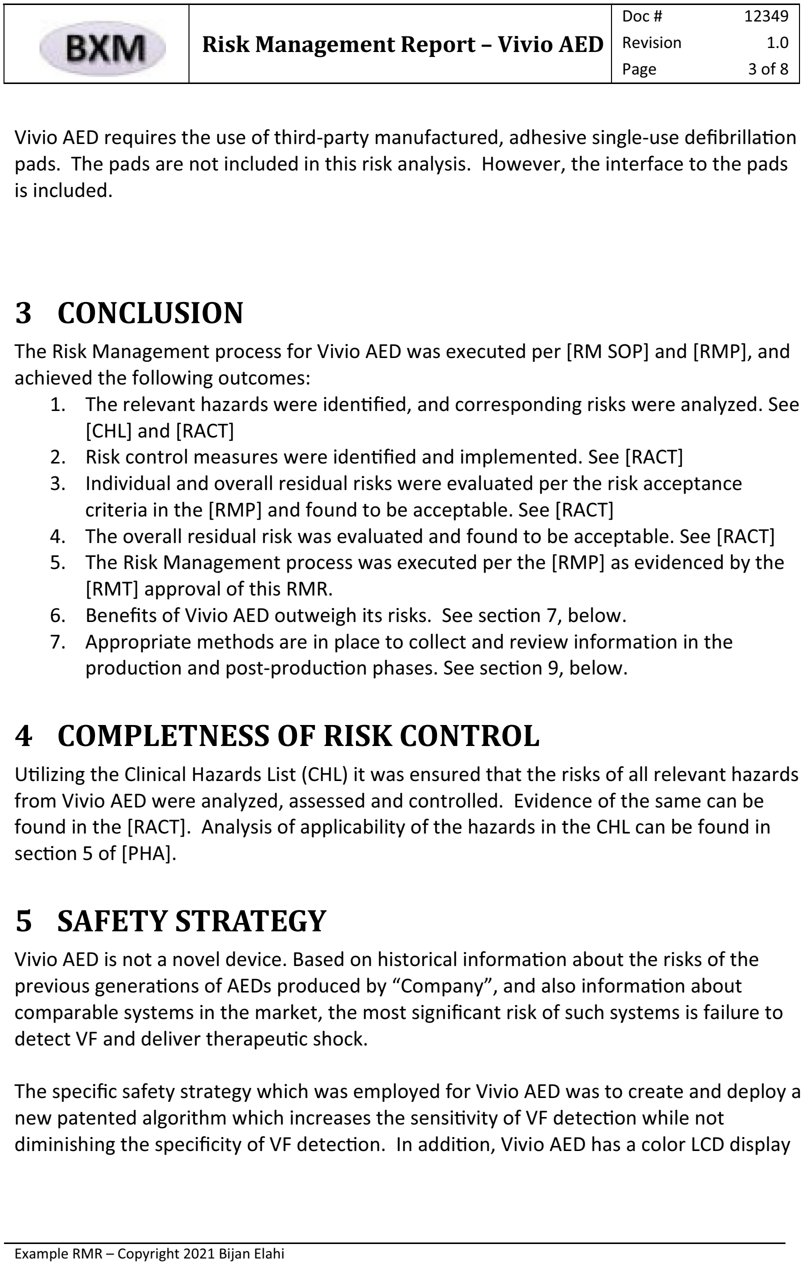
The preliminary residual risks of the Vivio AED are captured in the [PHA], and the final residual risks are captured in the [RACT].

The Risk Management Report is a living document and will be maintained for the lifecycle of Vivio AED.

2 SCOPE

The scope of this analysis is Vivio AED, a portable class III medical device designed for indoor/outdoor storage, and use by minimally trained individuals.

DEFIBRILLATOR



Vivio AED requires the use of third-party manufactured, adhesive single-use defibrillation pads. The pads are not included in this risk analysis. However, the interface to the pads is included.

3 CONCLUSION

The Risk Management process for Vivio AED was executed per [RM SOP] and [RMP], and achieved the following outcomes:

1. The relevant hazards were identified, and corresponding risks were analyzed. See [CHL] and [RACT]
2. Risk control measures were identified and implemented. See [RACT]
3. Individual and overall residual risks were evaluated per the risk acceptance criteria in the [RMP] and found to be acceptable. See [RACT]
4. The overall residual risk was evaluated and found to be acceptable. See [RACT]
5. The Risk Management process was executed per the [RMP] as evidenced by the [RMT] approval of this RMR.
6. Benefits of Vivio AED outweigh its risks. See section 7, below.
7. Appropriate methods are in place to collect and review information in the production and post-production phases. See section 9, below.

4 COMPLETNESS OF RISK CONTROL

Utilizing the Clinical Hazards List (CHL) it was ensured that the risks of all relevant hazards from Vivio AED were analyzed, assessed and controlled. Evidence of the same can be found in the [RACT]. Analysis of applicability of the hazards in the CHL can be found in section 5 of [PHA].

5 SAFETY STRATEGY

Vivio AED is not a novel device. Based on historical information about the risks of the previous generations of AEDs produced by "Company", and also information about comparable systems in the market, the most significant risk of such systems is failure to detect VF and deliver therapeutic shock.

The specific safety strategy which was employed for Vivio AED was to create and deploy a new patented algorithm which increases the sensitivity of VF detection while not diminishing the specificity of VF detection. In addition, Vivio AED has a color LCD display

and a loudspeaker to provide audio/visual guidance in the local language, for proper preparation and attachment of defibrillation pads to the patient chest.
Vivio AED is not vulnerable to cybersecurity threats. There is no wireless connectivity, and SW updates can only be done in the factory under controlled conditions.

6 OVERALL RESIDUAL-RISK EVALUATION

The overall residual risk for Vivio AED was evaluated to be acceptable. The basis of this evaluation was comparison with state-of-the-art risk levels as defined in [ISO 14971], and specified in the [RMP]. Details of the risk evaluation can be found in the [RACT]. Below a summary of overall residual risk vs. acceptable risk limits is presented.

	Risk Class				
	Fatal	**Critical**	**Major**	**Minor**	**Negligible**
Overall Residual Risk	6.04×10^{-5}	7.36×10^{-6}	1.26×10^{-4}	1.01×10^{-3}	1.08×10^{-6}
Acceptable Risk Limits	$\leq 6.1 \times 10^{-5}$	$\leq 9.8 \times 10^{-5}$	$\leq 2.3 \times 10^{-4}$	$\leq 7.5 \times 10^{-3}$	$\leq 1.0 \times 0^{-2}$

7 BENEFIT-RISK ANALYSIS

The residual risks for Vivio AED were evaluated both individually, and overall. In all cases, the residual risk was at or below acceptable thresholds as established in the [RMP].

Vivio AED delivers comparable benefit to state-of-the-art AEDs in the market, at a lower overall residual risk. It is therefore deduced that the benefits of Vivio AED outweigh its risks when the device is used for its intended purpose.

8 RISK MANAGEMENT PROCESS SUMMARY

[RM SOP] prescribes a Risk Management Process, which is compliant to [ISO 14971]. Figure 1 depicts a representation of the risk Management Process. The [RMT] ensured compliance with [RM SOP] by reviewing and approving of the [RMF] work products, including this Risk Management Report.

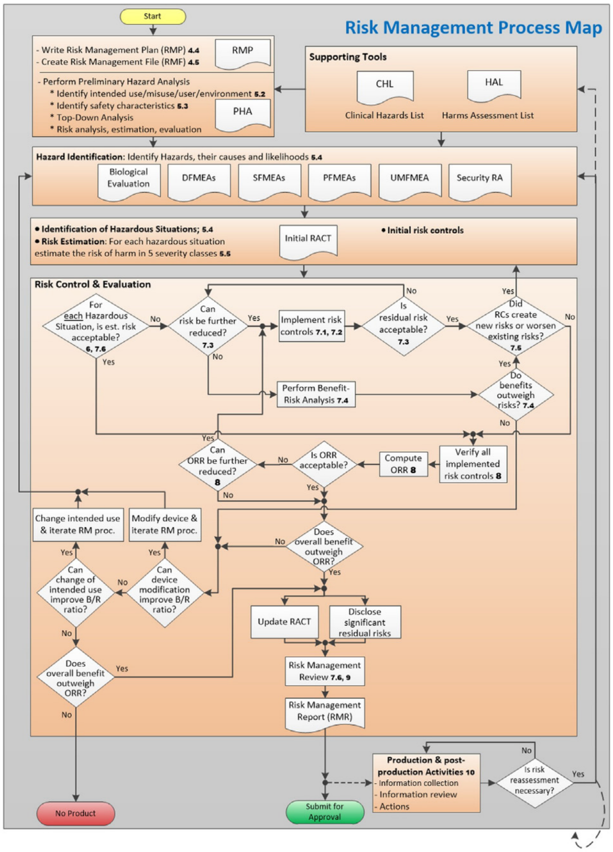
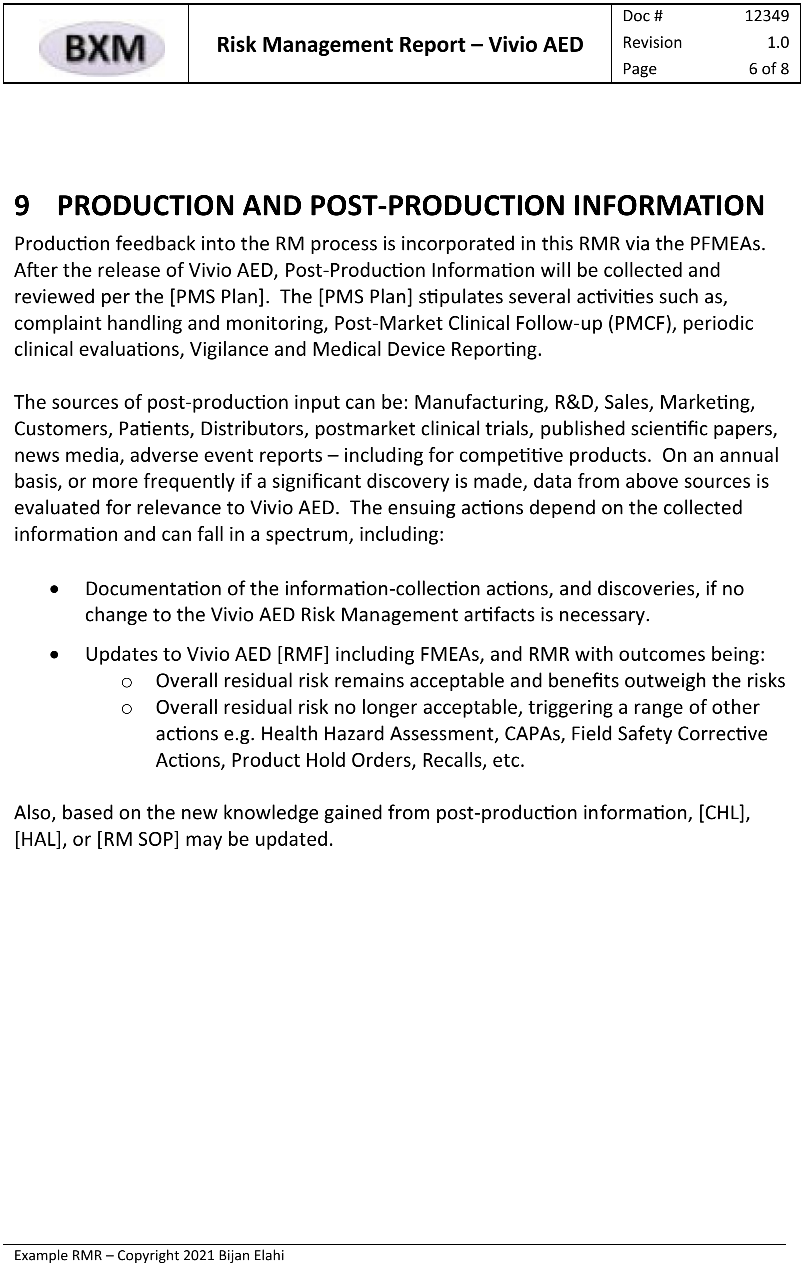

Risk Management Process Map
Start
- Write Risk Management Plan (RMP) 4.4
- Create Risk Management File (RMF) 4.5
RMP
- Perform Preliminary Hazard Analysis
* Identify intended use/misuse/user/environment 5.2
* Identify safety characteristics 5.3
* Top-Down Analysis
* Risk analysis, estimation, evaluation
PHA
Supporting Tools
CHL
Clinical Hazards List
HAL
Harms Assessment List
Hazard Identification: Identify Hazards, their causes and likelihoods 5.4
Biological Evaluation
DFMEAs
SFMEAs
PFMEAs
UMFMEA
Security RA
• Identification of Hazardous Situations; 5.4
• Risk Estimation: For each hazardous situation estimate the risk of harm in 5 severity classes 5.5
Initial RACT
• Initial risk controls
Risk Control & Evaluation
For each Hazardous Situation, is est. risk acceptable? 6, 7.6
No
Yes
Can risk be further reduced? 7.3
Yes
No
Implement risk controls 7.1, 7.2
Is residual risk acceptable? 7.3
No
Yes
Did RCs create new risks or worsen existing risks? 7.5
Yes
No
Perform Benefit-Risk Analysis 7.4
Do benefits outweigh risks? 7.4
Yes
No
Verify all implemented risk controls 8
Compute ORR 8
Is ORR acceptable?
No
Yes
Can ORR be further reduced? 8
Yes
No
Change intended use & iterate RM proc.
Modify device & iterate RM proc.
Yes
Yes
Can change of intended use improve B/R ratio?
No
Can device modification improve B/R ratio?
No
Does overall benefit outweigh ORR?
No
Yes
Does overall benefit outweigh ORR?
Yes
No
Update RACT
Disclose significant residual risks
Risk Management Review 7.6, 9
Risk Management Report (RMR)
No Product
Submit for Approval
Production & post-production Activities 10
- Information collection
- Information review
- Actions
Is risk reassessment necessary?
No
Yes

Figure 1 - Risk Management Process

The Risk Controls that were implemented via safety requirements were verified for implementation as part of the normal formal verification testing process. Risk Controls were also verified for effectiveness. The verification test protocols and results are stored in the RMF per the QMS procedures. The Traceability Analysis Report documents the linkages between the risk controls, and their associated verification test protocols and test results.



BXM	**Risk Management Report – Vivio AED**	Doc # Revision Page	12349 1.0 6 of 8

9 PRODUCTION AND POST-PRODUCTION INFORMATION

Production feedback into the RM process is incorporated in this RMR via the PFMEAs. After the release of Vivio AED, Post-Production Information will be collected and reviewed per the [PMS Plan]. The [PMS Plan] stipulates several activities such as, complaint handling and monitoring, Post-Market Clinical Follow-up (PMCF), periodic clinical evaluations, Vigilance and Medical Device Reporting.

The sources of post-production input can be: Manufacturing, R&D, Sales, Marketing, Customers, Patients, Distributors, postmarket clinical trials, published scientific papers, news media, adverse event reports – including for competitive products. On an annual basis, or more frequently if a significant discovery is made, data from above sources is evaluated for relevance to Vivio AED. The ensuing actions depend on the collected information and can fall in a spectrum, including:

- Documentation of the information-collection actions, and discoveries, if no change to the Vivio AED Risk Management artifacts is necessary.
- Updates to Vivio AED [RMF] including FMEAs, and RMR with outcomes being:
    - Overall residual risk remains acceptable and benefits outweigh the risks
    - Overall residual risk no longer acceptable, triggering a range of other actions e.g. Health Hazard Assessment, CAPAs, Field Safety Corrective Actions, Product Hold Orders, Recalls, etc.

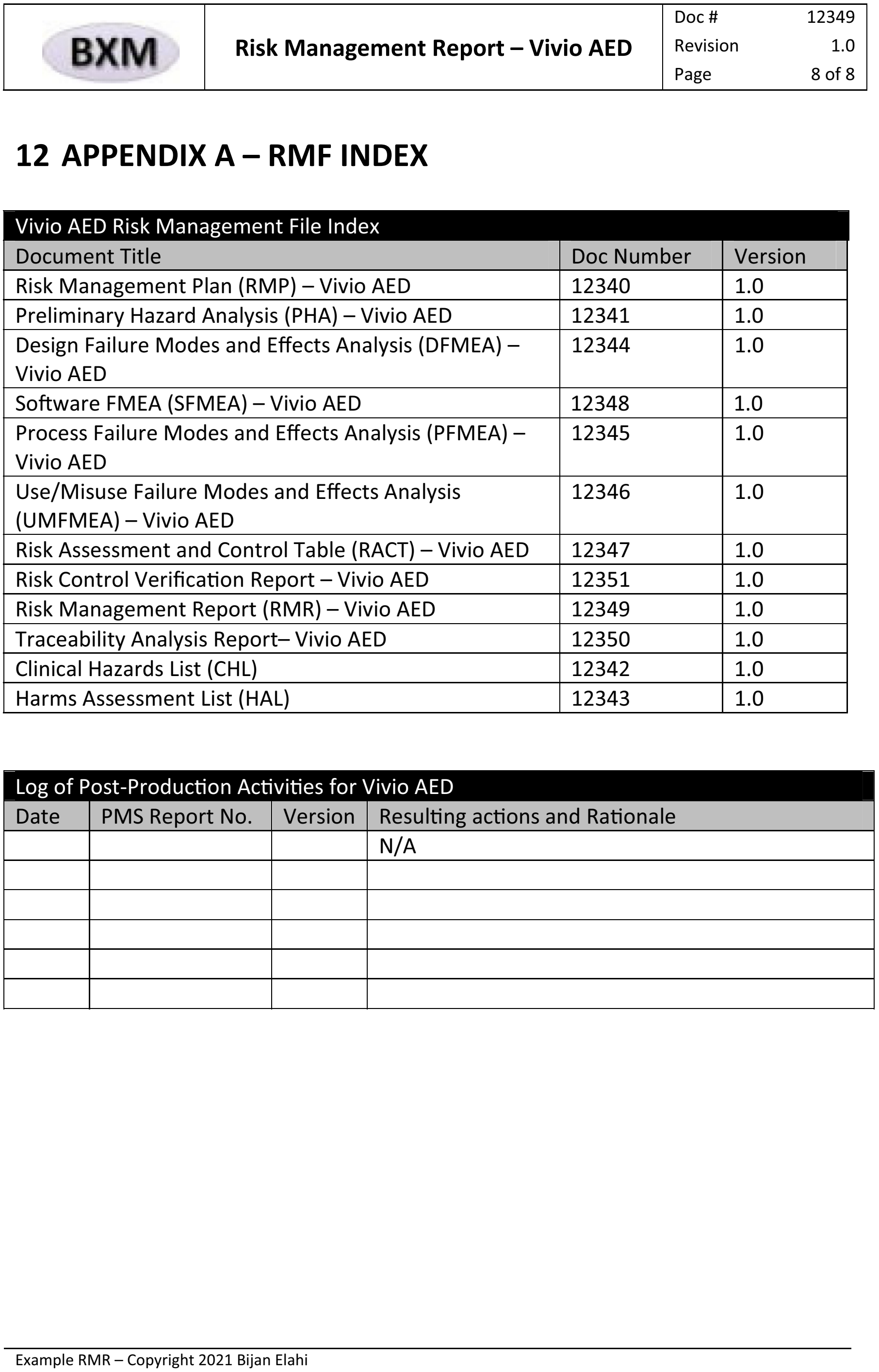
Also, based on the new knowledge gained from post-production information, [CHL], [HAL], or [RM SOP] may be updated.

10 REFERENCES

Reference	Document Number	Title / additional remarks
[RMP]	12340	Risk Management Plan – Vivio AED
[CHL]	12342	Clinical Hazards List
[PHA]	12341	Preliminary Hazard Analysis – Vivio AED
[PMS Plan]	12360	Post-Market Surveillance Plan – Vivio AED
[RACT]	12347	Risk Assessment and Control Table – Vivio AED
[RMF]	N/A	Risk Management File. See Appendix A in this document.
[RMT]	N/A	Risk Management Team. Identified in [RMP].
[RM SOP]	xxxxxx	Risk Management Process
[ISO 14971]	ISO 14971:2019	Application of Risk Management to Medical Devices

11 REVISION HISTORY

Revision	Author	CR	Description of changes
1.0	John Adams	N/A	First approved version



BXM	**Risk Management Report – Vivio AED**	Doc #	12349
		Revision	1.0
		Page	8 of 8

12 APPENDIX A – RMF INDEX

Vivio AED Risk Management File Index		
Document Title	Doc Number	Version
Risk Management Plan (RMP) – Vivio AED	12340	1.0
Preliminary Hazard Analysis (PHA) – Vivio AED	12341	1.0
Design Failure Modes and Effects Analysis (DFMEA) – Vivio AED	12344	1.0
Software FMEA (SFMEA) – Vivio AED	12348	1.0
Process Failure Modes and Effects Analysis (PFMEA) – Vivio AED	12345	1.0
Use/Misuse Failure Modes and Effects Analysis (UMFMEA) – Vivio AED	12346	1.0
Risk Assessment and Control Table (RACT) – Vivio AED	12347	1.0
Risk Control Verification Report – Vivio AED	12351	1.0
Risk Management Report (RMR) – Vivio AED	12349	1.0
Traceability Analysis Report– Vivio AED	12350	1.0
Clinical Hazards List (CHL)	12342	1.0
Harms Assessment List (HAL)	12343	1.0

Log of Post-Production Activities for Vivio AED			
Date	PMS Report No.	Version	Resulting actions and Rationale
			N/A

Appendix D: Useful References

In this Appendix a number of useful references are presented for use in risk management.

Directives, guidelines, and standards:

- *European Commission Medical Device Sector* – https://ec.europa.eu/health/md_sector/current_directives_en
- *Official Journal of the European Union* – https://eur-lex.europa.eu/oj/direct-access.html
- *European Commission Guidance MDCG endorsed documents* – https://ec.europa.eu/health/md_sector/new_regulations/guidance_en
- *European Medicines Agency (EMA) Human regulatory Medical devices* – https://www.ema.europa.eu/en/human-regulatory/overview/medical-devices
- *Eur-Lex Regulation (EU) 2017/745 (MDR)* – https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R0745
- *EUR-Lex Regulation (EU) 2017/746 (IVDR)* – https://eur-lex.europa.eu/eli/reg/2017/746/oj
- *MEDDEV guidance list and downloads* – https://ec.europa.eu/health/sites/health/files/md_sector/docs/md_guidance_meddevs.pdf https://www.medical-device-regulation.eu/meddev-guidance-list-download/
- *International Standards Organization (ISO) – List of standards related to medical devices* – https://www.iso.org/search.html?q=medical%20device
- *Emergo by UL* – https://www.emergobyul.com/
- *The International Medical Device Regulators Forum (IMDRF)* – http://www.imdrf.org/

Databases for clinical trials, surveillance, and literature reviews:

- *EU Clinical Trials Register* – https://www.clinicaltrialsregister.eu/
- *The World Health Organization (WHO) International Clinical Trials Registry Platform (ICTRP)* – https://www.who.int/ictrp/en/
- *US NIH database of clinical studies* – https://www.clinicaltrials.gov/
- *Cochrane Central Register of Controlled Trials (CENTRAL)* – https://www.cochranelibrary.com/central/about-central
- *European Commission EUDAMED* – https://ec.europa.eu/health/md_eudamed/overview_en
- *US FDA Manufacturer and User Facility Device Experience (MAUDE)* – https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfmaude/search.cfm
- *US FDA Total Product Life Cycle (TPLC)* – https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfTPLC/tplc.cfm

- *Australian Medical device incident reporting & investigation scheme (IRIS)* – https://www.tga.gov.au/medical-device-incident-reporting-investigation-scheme-iris
- *Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA)* – http://www.prisma-statement.org/
- *Cochrane Handbook for Systematic Reviews of Interventions* – https://training.cochrane.org/handbook
- *Cochrane PICO search*^{BETA} – https://www.cochranelibrary.com/about/pico-search
- *US NIH PubMed* – https://pubmed.ncbi.nlm.nih.gov/
- *US NIH MEDLINE* – https://www.nlm.nih.gov/bsd/medline.html
- *Elsevier Embase* – https://www.embase.com
- *Elsevier ScienceDirect* – https://www.sciencedirect.com/

Sources of data on medical device alerts, safety notices, and recalls:

United Kingdom: https://www.gov.uk/drug-device-alerts
France: https://ansm.sante.fr/informations-de-securite/
Germany: https://www.bfarm.de/EN/Home/_node.html
The Netherlands: https://www.igj.nl/onderwerpen/waarschuwingen-medische-hulpmiddelen/documenten
Spain: https://www.aemps.gob.es/acciones-informativas/notas-informativas-productos-sanitarios/?lang=en
Italy: https://www.salute.gov.it/portale/news/p3_2_1_3_1.jsp?lingua=italiano&menu=notizie&p=avvisi&tipo=dispo&dataa=2021/12/31&datada=2016/01/01
Ireland: http://www.hpra.ie/homepage/medical-devices/safety-information/safety-notices
Switzerland: https://www.swissmedic.ch/swissmedic/en/home/medical-devices/overview-medical-devices/information-on-specific-medical-devices.html
Hong Kong: https://www.mdd.gov.hk/en/safety-alerts-communications/important-safety-alerts/index.html
Australia: http://apps.tga.gov.au/prod/DEVICES/daen-entry.aspx
New Zealand: https://www.medsafe.govt.nz/safety/safety-landing.asp
Canada: https://healthycanadians.gc.ca/recall-alert-rappel-avis/search-recherche/simple/en?s=&plain_text=&f_mc=3&js_en=&page=5&f_mc=3&f_sc=41
United States: http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfMAUDE/TextSearch.cfm

CHAPTER 1

Introduction

Abstract

This book is about the management of safety risks for medical devices. You will learn how to answer difficult questions such as: Is my medical device safe enough? What are the safety-critical aspects of my device, and which are the most important ones? Have I reduced the risks as far as possible? A sound and properly executed risk management process does not render a risk-free medical device. It does imply that the best efforts were made to produce a device that is adequately safe—a device that provides benefits which outweigh its risks.

Keywords: Risk management; medical device

> *Art without engineering is dreaming. Engineering without art is calculating.*
>
> ***Steven K. Roberts***

This book is about the management of safety risks for medical devices. You will learn how to answer difficult questions such as: Is my medical device safe enough? What are the safety-critical aspects of my device, and which are the most important ones? How far do I need to reduce the risks of my medical device?

One of the main challenges for medical device companies is to be able to tell a clear and understandable story in their medical device submissions which demonstrates that their medical device is safe enough for commercial use. The methodology offered in this book, which we call the 'BXM Method,' offers a simple, understandable, and integrated process that is scalable and efficient. The BXM method is suitable for automation, which is a huge benefit to the practitioners of risk management in an environment of dynamic and complex medical technology.

The methodology offered in this book is in conformance with ISO 14971 and has been used and tested numerous times in real products that have been submitted and approved by the FDA and European notified bodies.

Risk management is a truly interdisciplinary endeavor. A successful risk manager employs skills from engineering, physics, chemistry, mathematics, logic, statistics, behavioral science, psychology and communications, all underpinned by critical thinking. In this book, we touch upon ways in which the various disciplines are employed at the service of risk management. Practitioners of risk management can at times

Safety Risk Management for Medical Devices
DOI: https://doi.org/10.1016/B978-0-323-85755-0.00001-1

encounter perplexing situations that fall in gray areas, and for which there is no clear answer. These are the times when the *art* of engineering must be deployed. Equipped with the knowledge of risk management fundamentals, using logical, critical thinking, and maintaining an attitude of reasonableness the practitioner of risk management will successfully navigate through challenges.

This book is designed to serve both university students who are new to risk management, as well as industry professionals who need a reference handbook. Step-by-step instructions are provided on how to perform the techniques of risk management. For further elucidation, Appendix C provides an example of a Risk Management File for a fictitious medical device.

Although the techniques, information, and tips that are offered in this book are intended for medical technology and medical devices, other safety-critical fields can also benefit from the knowledge gained herein.

One of the factors that should be kept in mind in the analysis of risks, is that the risk is not a deterministic outcome, but rather a probabilistic phenomenon. The same therapy from a given device could have different consequences for different patients. Variations in patient physiology and environmental conditions can contribute to vastly different severities of Harm, from patient to patient.

Risk management before a product is launched is about predictive engineering – to forecast risks, and to attempt to reduce and control the risks to acceptable levels. This is in contrast to Post-Market risk management which takes the retrospective, and at times the reactionary approach of root cause analysis, and Corrective and Preventive Actions (CAPA) after an adverse event has happened in the field.

The goal of medical device manufacturers is to produce effective, safe, reliable, and affordable products to promote health. Manufacturers are not expected to be error-free, flawless, or perfect. They are expected to use sound processes and good judgement to reduce the probability of Harm to people.

A sound and properly executed risk management process does not render a risk-free medical device. It does imply that the best efforts were made to produce a device that is adequately safe – a device that provides Benefits which outweigh its risks. Human beings are prone to errors and poor judgement. This is called misfeasance in legal terms. It is different from malfeasance, which is deliberate or deceptive actions with the intention to release a device that is not adequately safe.

Safety risk management is applicable to the entire lifecycle of medical devices, including design, production, distribution, installation, use, service, maintenance, obsolescence, decommissioning, and even destruction or disposal.

Although Harm is defined as "injury or damage to the health of people, or damage to property or the environment" [1], in this book we focus on injury or damage to the health of people. Damage to property or the environment that has a direct impact on the health of people is also within the scope of this book.

The words: System, Product, and medical device are used interchangeably in this book to refer to the target of the risk management process.

Styling – In this book words that have specific meaning in the world of risk management are capitalized to distinguish them from the ordinary dictionary meanings. Examples are Cause, End Effect, and Risk Control.

Glossary – Many acronyms are used in this book. A glossary of acronyms is provided in Appendix A for your reference.

1.1 HISTORY OF RISK MANAGEMENT

Risk management has been a part of human life for thousands of years. Long ago people recognized that sometimes they had good luck and sometimes they had bad luck. In order to avoid bad luck, they would consult oracles, astrologers, and the like. This was an early form of risk management. Mitigations included rituals, sacrifices to the gods, penitence, etc.

Gradually attention was paid to the causation of adverse events. What did we do to cause this earthquake? Is this famine a punishment for something we did? Slowly, people started considering the physical causes of adverse events, things that could actively be done to prevent the adverse events, and things that could be done to ameliorate the harms from those adverse events. However, the concept of risk was not yet understood. To this day, human beings are inherently not good at risk estimation. Our psychology tricks us to perceive some small risks as large, and vice versa.

In the 17th century, the mathematics of probability was worked out. But it wasn't until after World War II that structured and systematic methods for Risk Analysis, evaluation and control came into existence. The aviation, space, railway, and nuclear industries were pioneers in the development and evolution of these methodologies.

Risk management is paramount in any endeavor where there are high consequences, such as human or environmental health. The most effective means of risk reduction is to implement an organized and systematic approach to system safety from early in the development stage.

CHAPTER 2

What Is a Medical Device?

Abstract

Determination of what is a medical device is not always clear. The same device would be considered a medical device in one jurisdiction, and not a medical device in another jurisdiction. New technologies can challenge the established concepts of what constitutes a medical device. Certain kinds of software are now considered to be medical devices.

Keywords: Medical device; accessory; software; apparatus; appliance

Determination of what constitutes a medical device is not always so straightforward. There are many definitions, depending on the jurisdiction of operation. Below are some excerpts from the definitions in various jurisdictions:

United States – Section 201(h) of the Federal Food Drug & Cosmetic (FD&C) Act: an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory which is:

- recognized in the official National Formulary, or the United States Pharmacopoeia, or any supplement to them,
- intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or
- intended to affect the structure or any function of the body of man or other animals, and
- which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals, and
- which is not dependent upon being metabolized for the achievement of its primary intended purposes.

Europe – 2017/745 Medical Device Regulation: 'medical device' means any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes:

- diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease,
- diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability,

DOI: https://doi.org/10.1016/B978-0-323-85755-0.00002-3

- investigation, replacement or modification of the anatomy or of a physiological or pathological process or state,
- providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations,

and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means.

The following products shall also be deemed to be medical devices:

- devices for the control or support of conception;
- products specifically intended for the cleaning, disinfection or sterilisation of devices

China – National Medical Products Administration (NMPA) any instrument, apparatus, appliance, material, or other article whether used alone or in combination, including the software necessary for its proper application. It does not achieve its principal action in or on the human body by means of pharmacology, immunology or metabolism, but may be assisted in its function by such means; the use of which is to achieve the following intended objectives:

1. Diagnosis, prevention, monitoring, treatment, or alleviation of disease;
2. Diagnosis, monitoring, treatment, alleviation of, or compensation for an injury or handicap conditions;
3. Investigation, replacement, or modification for anatomy or a physiological process;
4. Control of conception.

Brasil – Agência Nacional de Vigilância Sanitária (ANVISA) healthcare product, such as equipment, devices, materials, articles, or systems for medical, odontological, or laboratory use or application, intended for prevention, diagnosis, treatment, rehabilitation, or anticonception and that does not use pharmacological, immunological, or metabolic means to fulfill its main function in human beings, but can have its functions assisted by such means

Australia – Therapeutic Goods Administration (TGA)

1. A medical device is:
   a. any instrument, apparatus, appliance, material or other article (whether used alone or in combination, and including the software necessary for its proper application) intended, by the person under whose name it is or is to be supplied, to be used for human beings for the purpose of one or more of the following:
      i. diagnosis, prevention, monitoring, treatment, or alleviation of disease;
      ii. diagnosis, monitoring, treatment, alleviation of, or compensation for an injury or disability;

iii. investigation, replacement, or modification of the anatomy or of a physiological process;

iv. control of conception;

and that does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, but that may be assisted in its function by such means; or

(aa) any instrument, apparatus, appliance, material or other article specified under subsection (2A); or

(ab) any instrument, apparatus, appliance, material or other article that is included in a class of instruments, apparatus, appliances, materials or other articles specified under subsection (2B); or

b. an accessory to an instrument, apparatus, appliance, material, or other article covered by paragraph (a), (aa) or (ab).

Note: Declarations under subsection (3) exclude articles from the scope of this definition. Declarations under section 7 can also have this effect: see subsection 7(4).

2. For the purposes of paragraph (1)(a), the purpose for which an instrument, apparatus, appliance, material or other article (the *main equipment*) is to be used is to be ascertained from the information supplied, by the person under whose name the main equipment is or is to be supplied, on or in any one or more of the following:

a. the labelling on the main equipment;

b. the instructions for using the main equipment;

c. any advertising material relating to the main equipment;

d. technical documentation describing the mechanism of action of the main equipment.

(2A) The Secretary may, by notice published in the *Gazette* or on the Department's website, specify a particular instrument, apparatus, appliance, material, or other article for the purposes of paragraph (1)(aa). The notice is not a legislative instrument.

(2B) The Secretary may, by legislative instrument, specify a particular class of instruments, apparatus, appliances, materials, or other articles for the purposes of paragraph (1)(ab).

3. The Secretary may, by order published in the *Gazette* or on the Department's website, declare that a particular instrument, apparatus, appliance, material, or other article, or that a particular class of instruments, apparatus, appliances, materials, or other articles, are not, for the purposes of this Act, medical devices.

Note: A declaration under this section does not stop articles from being therapeutic goods.

Some interesting observations from the above definitions are:

- Software can be considered to be a medical device in the EU, Chinese, and Australian regulations, but not in the United States or Brazilian regulations.
- A condom used for birth control is a medical device in the EU, China, Australia, and Brazil, but not in the United States.
- Veterinarian devices are medical devices in the United States, but not in Europe, China, Australia, or Brazil.

Other noteworthy instances:

- Cryogenic gases used in therapy are treated as medical devices.
- Vacuum which is used to operate a medical device is an accessory which would be treated as a medical device.
- Software which is used to interpret ECG or X-rays is a medical device.
- A syringe is a medical device, but a prefilled syringe is a combinational device with a drug as Primary Mode of Action (PMOA).
- An anti-bacterial vaginal ointment which achieves its therapeutic purpose by mechanical prevention of attachment of bacteria to vaginal walls is a medical device.

This is important because medical device risk management is required if the subject device is considered a medical device in the geography in which it will be sold.

Sometimes the manufacturer has a choice. For instance, a treadmill can be exercise equipment, or a medical device depending on the declared Intended Use.

~ ~ ~

Accessories are another class of devices which are of interest for risk management. The distinction between a medical device and an accessory is not always clear. For example, the cable that connects a generator to a laparoscope is an accessory because it is intended to enable the performance of a clinical function. But, if it was possible to use a generic audio cable to make the same connection, that audio cable would not be an accessory because it was not intended to enable the performance of a clinical function.

To help with the distinction of medical device accessories, two definitions from the United States and Europe are presented below:

Europe – 2017/745 Medical Device Regulation [2]:

Accessory: an article which, whilst not being itself a medical device, is intended by its manufacturer to be used together with ... medical device(s) to specifically enable or assist the medical device(s) to be used in accordance with their intended purpose(s)...

U S FDA – Section 513(f) of the Federal Food Drug & Cosmetic (FD&C) Act

An accessory is a finished device that is intended to support, supplement, and/or augment the performance of one or more parent devices.

To help distinguish whether an item is an accessory, ask two questions:

Q1 – Is it intended to be used with one/more parent medical devices?

Example: an off-the-shelf computer monitor that is used with a medical device is not an accessory.

Q2 – Is the subject intended to support, supplement, and/or augment the performance of a parent medical device?

- Support – does it support, enable, or facilitate the performance of the clinical function of a parent medical device according to its Intended Use?
  Example: an infusion pump stand; a trocar for laparoscopy.
- Supplement – does it supplement the performance of the clinical function of a parent medical device by adding a new function, or making possible the use of a parent medical device in new ways, without changing the Intended Use of the parent medical device?
  Example: an adapter that allows the connection of a pulse oximeter to a multiparameter monitor, so it can now display blood oxygen levels.
- Augment – does it augment the performance of a parent medical device by enabling the parent medical device to perform its intended use more safety/effectively?
  Example: bone cutting guide to enable more precise cutting of bone in orthopedic operations.

If the answers to both Q1 and Q2 are yes, then the item can be classified as an accessory.

Software could be an accessory when it supports, supplements, or augments the performance of a medical device. Sometimes software is a medical device in and of itself.

An accessory is treated as a medical device and is subject to risk management requirements.

CHAPTER 3

Why Do Risk-Management?

Abstract

There are many good reasons to do risk management. In addition to making safer products, risk management can help reduce the cost of design and development by identifying the safety-critical aspects of the design early in the product life cycle. Risk management is a legal requirement in most countries, without which it would not be possible to obtain approval for commercialization of medical devices. In the unfortunate situations when people are injured by medical devices, the first place that lawyers would look is the risk management file of the device.

Keywords: Legal; regulatory; harmonized standards; risk-based; recall; field corrective action; moral; ethical

Whether you are aware of it or not, you are constantly managing risk in your daily life. For almost every action that we take, we internally evaluate the benefit of that action vs. the risks (or cost) of that action. If we believe the benefits outweigh the risks, we take that action. Else, we don't. Consider the simple action of driving to work in your car. You consider the benefit of comfort and speed of getting from home to work vs. the risks of getting injured or killed in a car crash. In general, the chances of getting into a serious accident are fairly small, compared to the benefit of commuting in your car. But now imagine you are in a war-torn country where there are explosive devices buried in the roadway. Now the calculus changes. The risks are higher than the benefits, and you would likely choose to walk off-road instead.

The medical device industry is required to evaluate the potential safety risks due to the use of a medical device against the potential Benefits of that device. Regulatory approval of a medical device requires demonstrating that the risks of the device are outweighed by its Benefits. Formal and systematic methods are used to make this determination.

Another important reason to do risk management is the progressive shift in the industry where more and more decisions are risk-based. For example, decisions on Field Safety Corrective Actions, decisions on Corrective and Preventive Actions, and Product Hold Orders. Risk-based decisions are rational and defensible. In many aspects of product development, e.g., design choices, or test sample-size determination, risk is a good discriminator and basis for decision-making. Moreover, the European Medical Device Regulation (EU MDR) [2] takes a preference for a risk-based approach to evaluation of manufacturer's technical documentation, and oversight and monitoring of the manufacturers. How can one make risk-based decisions, if one doesn't know the risks? Risk management offers the answer.

Safety Risk Management for Medical Devices
DOI: https://doi.org/10.1016/B978-0-323-85755-0.00003-5

3.1 LEGAL AND REGULATORY REQUIREMENTS

3.1.1 United States

In the United States, the governing law is United States CFR Title 21, part 820. Title 21 is about foods and drugs, and part 820 is about Quality System Regulations. This law requires that all finished medical devices be safe and effective. The burden of proof is on the manufacturer. Prior to ISO 14971, there were many methods used by manufacturers to provide evidence of safety. There was no consistency and the quality of the evidence varied widely.

On January 14, 2020 the FDA recognized ISO 14971:2019 [9]. However, the FDA will continue to accept declarations of conformity to the previous version, ISO 14971:2007, in support of pre-market submissions until December 25, 2022. As a recognized standard, conformance to ISO 14971 is sufficient proof of medical device safety for the FDA.

3.1.2 European Union

In the European Union, until May 25, 2021 manufacturers can choose either of two regulatory channels for the approval of their medical devices.

Channel 1 – MDD/AIMDD

Directive 93/42/EEC, also known as the Medical Device Directive (MDD) [3] compelled the member States to pass laws that were consistent with the MDD. Article 3 of the MDD required that medical devices must meet the essential requirements set out in Annex I. Stated briefly and simply, the Essential Requirements of *Annex I* stipulate that medical devices:

1. Be safe when used as intended by the manufacturer.
2. Have benefits that outweigh their risks.
3. Reduce risks as far as possible.

There was also a counterpart to MDD [3] for active implantable medical devices. It was called Active Implantable Medical Device Directive (AIMDD) [4]. AIMDD was similar to MDD, but was focused on Active Implantable Medical Devices.

Article 5 of the MDD stated that compliance with the Essential Requirements of *Annex I* could be presumed, if a medical device was conformant with relevant harmonized standards that are published in the *Official Journal of the European Communities* [5].

Channel 2 – Medical Device Regulation (MDR)

The EU MDR [2] is a regulation which applies to all member states in the European Union. Unlike the MDD, it does not compel member states to interpret it and pass laws that are consistent with it. The MDR is a Regulation which is applicable as is, hence not subject to varying interpretations by member states.

Annex I, Chapter I of EU MDR [2] has similar requirements to MDD [4]. Stated briefly and simply, the General Safety and Performance Requirements stipulate that medical devices:

1. Be safe and effective when used as intended by the manufacturer.
2. Their risks be acceptable when weighed against the Benefits to patients.
3. The risks be reduced as far as possible without adversely affecting the Benefit-risk ratio.

Similar to the MDD/AIMDD, the EU MDR confers a presumption of compliance with the MDR requirements if a manufacturer is in conformance with the relevant harmonized standards.

> **Harmonized Standards** – According to MDCG 2021-5 [6], Harmonized European standards in the field of healthcare engineering, including medical devices, are developed by the two relevant European standardization organizations: the European Committee for Standardization (CEN) for most types of medical devices, and the European Committee for Electrotechnical Standardization (CENELEC) for medical electrical equipment.
>
> According to Article 10 of the Standardization Regulation (EU) 1025/2012, the European Commission may request one or several European standardization organizations to draft European standards. This is the necessary legal basis for the development of harmonized European standards in support of the requirements of EU legislation, and to allow publication in the *Official Journal of the European Union* (OJEU) [5].
>
> During the standardization process, specific assessment of the draft standards under development is carried out by the "Harmonized Standards (HAS) consultants," as technical experts supporting the European Commission, to ensure the compliance of the draft harmonized standards with the relevant EU legislative framework and with the relevant standardization request (mandate).
>
> CEN and CENELEC propose to the European commission the publication of references to such standards in the OJEU [5]. The Commission carries out the final assessment on compliance of these proposed standards with the requirements of the legislation, as well as the relevant standardization mandate or request, taking into account the assessment reports by the HAS consultants to decide whether to publish references to the European standards in the OJEU [5]. Publication in the OJEU [5] makes the standard harmonized.

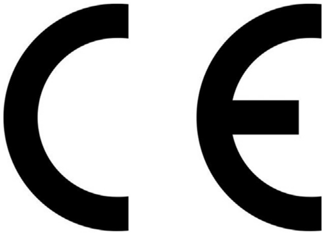
Conformance to harmonized standards is voluntary. Products designed and manufactured according to applicable harmonized standards benefit from a presumption of conformity with the relevant regulations. This creates an advantage for the manufacturers in demonstrating compliance with regulations, and a similar advantage for the Notified Bodies and

Competent Authorities in assessing compliance with the regulations, thereby leading to quicker and easier regulatory approvals of medical devices.

Notified Bodies are accredited entities who assess conformity to harmonized standards. For a list of the Notified Bodies refer to the website: https://ec.europa.eu/.

Directive 98/79/EC on in vitro diagnostic medical devices (IVDMDD), is applicable from June 7, 2000 until May 25, 2022. From May 26, 2022, Regulation (EU) 2017/746 on in vitro diagnostic medical devices (IVDR), is fully applicable.

Each country in the European Union has a Competent Authority who approves medical devices for commercialization. Upon approval by a Competent Authority, a medical device can be CE (Conformité Européenne) marked.



3.1.3 MDD/AIMDD and Transition to EU MDR

EU MDR [2] was promulgated on May 26, 2017. There was a 3-year transition period after which AIMDD [4] and MDD [3] would no longer be effective and only MDR certification would be possible. This transition period was to end on May 26, 2020. But for a variety of reasons, the date of application was postposed to May 26, 2021. The date of application for IVDR is May 26, 2022. From May 26, 2017 to November/December 2018 only MDD/AIMDD certification was possible. Thereafter, until May 26, 2021, it was possible to choose MDD/AIMDD or MDR [2] certification.

There is a 3-year grace period after May 26, 2021 during which products that were certified to MDD/AIMDD can be still manufactured and sold – until May 26 2024. Thereafter, there is only a 1-year period until May 26, 2025 to sell off any inventory of MDD/AIMDD certified products.

3.2 BUSINESS REASONS

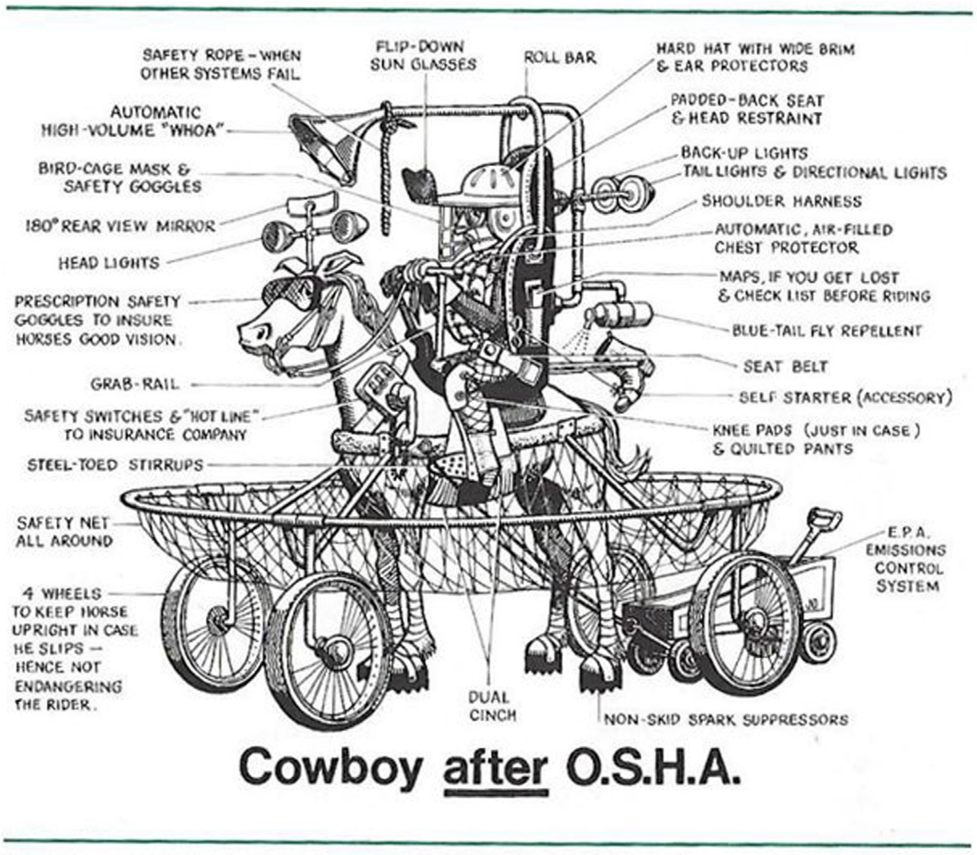
3.2.1 Cost Efficiency

One of the main benefits of risk management is gaining knowledge of what the risks of a medical device are, where they are, and how big they are. With this knowledge, the product development team can focus their engineering resources on the areas of highest risk. Furthermore, good risk management practices can help detect design-flaws that have a safety impact, early in the product development process. The sooner a design-flaw is corrected, the less expensive it is to fix it.

Competition and economic incentives drive the industry for speed to market. But history suggests that speed does not justify compromise on the safety of programs. For example, excess focus on schedule resulted in the Space Shuttle Challenger disaster in 1986.

Manufacturers want to make their products as safe as possible. But without clear knowledge of the risks of a device, the tendency is to operate based on fear and to over-engineer in an abundance of caution. This is costly, especially when the over-engineering is done in areas that are of low/no risk.

The cartoon in Fig. 1 was drawn by J.N. Devin in 1972. Although it gives a comical view of over-engineering, there are some lessons hidden in there. It shows when a good intention can go awry to the point of making a product useless.


SAFETY ROPE - WHEN OTHER SYSTEMS FAIL
FLIP-DOWN SUN GLASSES
ROLL BAR
HARD HAT WITH WIDE BRIM & EAR PROTECTORS
AUTOMATIC HIGH-VOLUME "WHOA"
PADDED-BACK SEAT & HEAD RESTRAINT
BIRD-CAGE MASK & SAFETY GOGGLES
BACK-UP LIGHTS TAIL LIGHTS & DIRECTIONAL LIGHTS
SHOULDER HARNESS
180° REAR VIEW MIRROR
AUTOMATIC, AIR-FILLED CHEST PROTECTOR
HEAD LIGHTS
MAPS, IF YOU GET LOST & CHECK LIST BEFORE RIDING
PRESCRIPTION SAFETY GOGGLES TO INSURE HORSES GOOD VISION.
BLUE-TAIL FLY REPELLENT
SEAT BELT
GRAB-RAIL
SELF STARTER (ACCESSORY)
SAFETY SWITCHES & "HOT LINE" TO INSURANCE COMPANY
KNEE PADS (JUST IN CASE) & QUILTED PANTS
STEEL-TOED STIRRUPS
SAFETY NET ALL AROUND
E.P.A. EMISSIONS CONTROL SYSTEM
4 WHEELS TO KEEP HORSE UPRIGHT IN CASE HE SLIPS — HENCE NOT ENDANGERING THE RIDER.
DUAL CINCH
NON-SKID SPARK SUPPRESSORS
Cowboy after O.S.H.A.

Mr. James N. Devin, Independence, Missouri. © 1972. Reproduced with permission.

Figure 1 Over-Engineered Cowboy.

3.2.2 Avoiding Recalls and Field Corrective Actions

Safety violations are the main reason for Field Safety Corrective Actions (FSCA), such as product recalls. Product recalls are very expensive, and expose manufacturers to lawsuits and potentially large fines, settlement costs, and legal fees. Moreover, the reputation of a manufacturer may become tarnished and future sales hampered.

Good risk management practices can reduce the probability of harming people or the environment, and thus avoid recalls.

One of the most important benefits of risk management is that it provides leading indicators for potential future problems. In many cases a manufacturer realizes only after an Adverse Event, that they are in trouble and facing a lawsuit or punishment by Regulatory bodies. Risk management enables manufacturers to identify the highest risks associated with their products and be able to forecast the probability of Serious Adverse Events.

3.2.3 Better Communications

An unexpected side benefit of risk management is improved communication. In most companies the product development teams become siloed, which means poor communication among the various disciplines, such as electrical engineering, mechanical engineering, clinical, sterilization, etc. Because risk management is a team effort, it tends to bring the various disciplines to the table to work together toward safer products. Many very useful and enlightening discussions happen during the risk management work meetings.

3.3 MORAL AND ETHICAL REASONS

Our patients trust us with their lives. They expect that we do our utmost to make devices that are safe and effective. It is our moral and ethical duty to apply good risk management practices so we deliver the safest possible products to our patients. Effective and safe devices earn the trust of medical device makers' customers.

CHAPTER 4

The Basics

Abstract

As in any other discipline, risk management also has its own jargon, or special vocabulary. It is imperative that you learn this vocabulary and use it correctly and consistently. Without this common language, it is not possible to reliably convey meaning. This increases the probability of miscommunication, confusion, and the potential for errors.

Keywords: Vocabulary; jargon; hazard; safety; risk; hazard theory; integral system; distributed system

4.1 VOCABULARY OF RISK MANAGEMENT

As in any other discipline, risk management also has its own jargon, or special vocabulary. It is imperative that you learn this vocabulary and use it correctly and consistently. Just as important, you should teach this vocabulary to others who participate in producing risk management work products. Without this common language, it is not possible to reliably convey meaning.

Note that this vocabulary is not colloquial English. For instance, to a normal English-speaker the words: hazard, risk, or danger may sound synonymous. But in the jargon of risk management specific meanings are assigned to words.

Sloppy usage of the jargon increases the probability of miscommunication, confusion, and the potential for errors. Table 1 lists some of the most commonly used terms in medical device risk management.

Table 1 Special Vocabulary of Risk Management

Term	Definition
Basic Safety	freedom from unacceptable risk directly caused by physical hazards when ME equipment is used under normal condition and single fault condition [7]
Essential Performance	performance of a clinical function, other than that related to basic safety, where loss or degradation beyond the limits specified by the manufacturer results in an unacceptable risk [7]

(*Continued*)

DOI: https://doi.org/10.1016/B978-0-323-85755-0.00004-7

Table 1 (Continued)

Term	Definition
Expected Service Life	time period specified by the manufacturer during which the medical electrical equipment or medical electrical system is expected to remain safe for use (i.e., maintain basic safety and essential performance) Note – Maintenance can be necessary during the expected service life [7]
Failure	the inability of an entity to achieve its purpose
Fault	an anomalous condition for a part
Harm	injury or damage to the health of people, or damage to property or the environment [8]
Hazard	potential source of harm [8]
Hazardous Situation	circumstance in which people, property, or the environment are exposed to one or more hazards [8]
Instruction for Use	information provided by the manufacturer to inform the user of the device's intended purpose and proper use and of any precautions to be taken [2] article 2, (14)
Intended Purpose	use for which a device is intended according to the data supplied by the manufacturer on the label, in the instructions for use or in promotional or sales materials or statements and as specified by the manufacturer in the clinical evaluation [2] Article 2 (12)
Intended Use	use for which a product, process. or service is intended according to the specifications, instructions, and information provided by the manufacturer [8] Note – ISO 14971:2019 [1] equated Intended Use and Intended Purpose in [1] Section 3.6
Label	written, printed, or graphic information appearing either on the device itself, or on the packaging of each unit or on the packaging of multiple devices [2] Article 2 (13)
Reasonably Foreseeable Misuse	use of a product or system in a way not intended by the manufacturer, but which can result from readily predictable human behavior [8]
Residual Risk	risk remaining after risk control measures have been implemented [8] including actions to avoid, or limit the harm
Risk	combination of the probability of occurrence of harm and the severity of that harm [2] article 2, (23)

(*Continued*)

Table 1 (Continued)

Term	Definition
Risk Analysis	systematic use of available information to identify hazards and to estimate the risk [9]
Risk Assessment	overall process comprising a risk analysis and a risk evaluation [9]
Risk Control	process in which decisions are made and measures implemented by which risks are reduced to, or maintained within, specified levels [9]
Risk Estimation	process used to assign values to the probability of occurrence of harm and the severity of that harm [8]
Risk Evaluation	process of the estimated risk against given risk criteria to determine the acceptability of the risk [8]
Risk Management	systematic application of management policies, procedures and practices to the tasks of analyzing, evaluating, controlling, and monitoring risk [8]
Risk Management File	set of records and other documents that are produced by risk management [1]
Safety	freedom from unacceptable risk [1]
Serious Injury	injury or illness that: [10] a) is life threatening, b) results in permanent impairment of a body function or permanent damage to a body structure, or c) necessitates medical or surgical intervention to prevent permanent impairment of a body function or permanent damage to a body structure Note – Permanent impairment means an irreversible impairment or damage to a body structure or function excluding trivial impairment or damage.
System	a combination of products, either packaged together or not, which are intended to be inter-connected or combined to achieve a specific medical purpose [2] article 2 (11)
User	any healthcare professional or lay person who uses a device [2] article 2, (37)

Further elaborations:

Hazard – A Hazard is something, exposure to which could potentially cause Harm. Sometimes the Harm is directly caused, e.g., a sharp knife. But sometimes the Harm is caused indirectly. For example, if a medical device is expected to sustain life, and it fails, the patient could die not because the device did something to the patient, but because there was an expectation of performance that was not delivered. This is also a Hazard.

Harm – Although not explicitly stated in the official definition, the authors of the standard have a broad interpretation of the term "Harm" including unreasonable psychological stress, and unwanted pregnancy. The intention behind including damage to property and the environment in the scope of Harm, is to consider the type of damage that could have safety consequences. For example, improper disposal of radioactive isotopes in a brachytherapy device may endanger sanitation workers. In addition, with today's environment of cybersecurity concerns, data should be included in the scope of 'property.' For example, loss of X-ray images could lead to retaking the X-ray images and exposure to additional radiation.

Safety – Ref. [8] advises that the term "safety" be used as a noun, rather than as a descriptive adjective, to avoid misinterpretation of "safety" as an assurance of freedom from risk. Ref. [8] further advises that wherever possible, the term "safety" be replaced with an indication of objective. For example, "Protective helmet" instead of "safety helmet"; "protective impedance device" instead of "safety impedance“. The word "safety" is used as a noun in these phrases: "safety and reliability," "degree of safety." Note that this is an advisory, not a requirement.

All medical devices carry a certain amount of Residual Risk, and the users should be made aware of such Residual Risks.

Risk – Although the definition of risk is simply "combination of the probability of occurrence of Harm and the severity of that Harm," there are many factors that play a role in the level of risk which is experienced by people. For example, exposure to a hot object causes burns. But it matters how hot the object is, how long the hot object contacts the person, where on/in the body the hot object contacts the person, and the physical properties of the hot object – compare a hot spoon vs. hot oil. Also, typically when a Harm happens, actions are taken to ameliorate the Harm. ISO/IEC Guide 63 [8], 3.10, Note 1, advises that in risk calculation the possibility to avoid or limit the Harm should be included.

Hazard Analysis vs. Risk Analysis – Sometimes, the terms 'Hazard Analysis' and 'Risk Analysis' are used interchangeably. This is incorrect. The purpose of Hazard Analysis is the identification of Hazards and the foreseeable sequence of events that could realize those Hazards. In contrast, Risk Analysis is about estimation of the potential risks due to the identified Hazards. Hazard analysis precedes Risk Analysis and identifies the Hazards. Risk Analysis estimates the risks of Harms that could ensue from the identified Hazards.

Intended Use vs. Intended Purpose – The guidance document: MDCG 2020-6 [11], Section 1 states that 'intended use' and 'intended purpose' should be considered to have the same meaning. This is an evolutionary conflation of the semantics of these two terms. To understand the distinction, we can examine the definition of Intended Purpose in the EU MDR [2]: "use for which a device is intended according to the data supplied by the manufacturer on the label, in the instructions for use or in promotional or sales materials or statements and as specified by the manufacturer in the clinical evaluation." Historically, Intended Use meant how a device was meant to be used, e.g., single use vs. multi-use, by what type of user, e.g., clinician vs. lay person, and in what way, e.g., a rectal thermometer is intended for insertion in the anus, but the Intended Purpose is to measure body temperature.

Intended Purpose/use vs. Indication (for use) – The guidance document: MDCG 2020-6 [11] Section 1 states that an Indication is a clinical condition that is to be diagnosed, prevented, monitored, treated, alleviated, compensated for, replaced, modified or controlled by the medical device, while Intended Purpose/use describes the effect of a device.

All devices have an Intended Purpose/use, but not all devices have an Indication. For example, a sterilizer has a purpose, but not an Indication.

4.1.1 Reasonably Foreseeable Misuse

ISO 14971 [1] requires that the manufacturer identify and document the Hazardous Situations related to the Intended Use, and Reasonably Foreseeable Misuses of the medical device. The risks associated with each Hazardous Situation must be estimated, evaluated, and controlled.

The definition for the term "Reasonably Foreseeable Misuse" was introduced in the 3rd edition of ISO 14971 [1]. The definition originates in ISO/IEC Guide 63 [8].

The definition is: "use of a product or system in a way not intended by the manufacturer, but which can result from readily predictable human behavior." Although this definition helps, there is still confusion and debate about what constitutes a Reasonably Foreseeable Misuse. First, what is 'reasonable'? In whose judgement? Second, what is 'readily predictable'? Predictable by who? Should every wild and imaginative idea about misuse be considered as *reasonably foreseeable*?

Note 2 of the definition in [1,8] says "Reasonably foreseeable misuse can be intentional or unintentional." This confuses use-errors, which are unintentional, with off-label uses, which are intentional. In the opinion of this author, it is better to distinguish intentional vs. unintentional misuses. Intelligent and proper design of a medical device can help reduce use-errors when using a medical device. But healthcare professionals can intentionally and successfully apply a medical device for a use that was not intended by the manufacturer.

Risks from use-errors can be managed within usability engineering and included within the normal product risk management. Off-label uses are circumstances in which the user and the device are both successful in performing their functions. Your risk management team may imagine a large number of ways in which your medical device could be used off-label. The question is: which imagined off-label uses (misuses) should be included in the Risk Analysis?

The following six tests are offered as a means to determine if a misuse should be included in the Risk Analysis as a *Reasonably Foreseeable Misuse*.

1. Deliberate

   There is a deliberate decision by the user to use the device in the manner that they want.
2. Well-intentioned

   The User intends to do well by the patient, i.e., no harm is intended.
3. Beneficial

   The User believes a Benefit can be derived for the patient from the misuse.
4. Feasible

   The misuse is feasible, i.e., it is technically, financially, and skill-wise within the capability of the user to do the misuse.
5. Safe

   The user can safely use the device for the purpose that they wish to use the device.
6. Ethical

   The user is acting ethically. They have disclosed the truth about the intended misuse and have the consent of the patient and the hospital. (This is not relevant when a patient is using the device on him/herself.)

If a foreseen misuse meets the above six tests, then it can be construed as a Reasonably Foreseeable Misuse. Malice is excluded from the analysis. That is, if the user intends to harm a patient, such action is not included in the risk management of the medical device.

It is a very good idea to consult with other departments such as sales, marketing, and clinical staff to get insights into how the device might get misused in the field.

Tip Consider the situation when multiple generations of the same medical device are used simultaneously, e.g., in a hospital. Could that create a Hazard?

4.2 HAZARD THEORY

In order to receive Harm, there must be exposure to Hazard(s). Fig. 2 illustrates a model that is called Hazard Theory. Hazards either naturally exist, such as UV rays in sunlight, or they are created through a sequence of events. Let's examine the created hazards. Hazard Theory states that an initiating event starts a progression of events that culminate in a Hazard. The Hazard is the last stop in the chain of events that lead to the Hazard. The chain of events could be long, or very short.

Once the Hazard is created, or when it naturally exists, it takes exposure to that Hazard to create a Hazardous Situation. Some exposures are automatic. For example, if an implanted device presents a Hazard, exposure is automatic since the device is already in the patient's body. Other exposures require a chain of events. For instance, imagine a worker in a radioactive environment is wearing protective clothing. The worker scratches the protective clothing, which leads to a tear in the fabric, which leads to exposure to radioactive particles.

A Hazardous Situation may arise as a result of external circumstances. For example, a surgical robot may rely on navigational data from a third-party device to guide the cutting instruments inside a patient's body. A failure in the third-party navigational input would result in a Hazardous Situation due to no failure of the robot itself.

Circumstances surrounding the Hazard and exposure affect the Severity of the Harm. For example, falling down could lead to injuries. But the height of the fall, and the softness of the surface onto which a person falls have an influence on the Severity of the Harm received.

In the BXM method the complete spectrum of Harm severities is considered. That is, given a Hazardous Situation, everything from nothing to death is considered. Therefore, it can be said that once the Hazardous Situation has been achieved, the probability of receiving Harm is 100%.

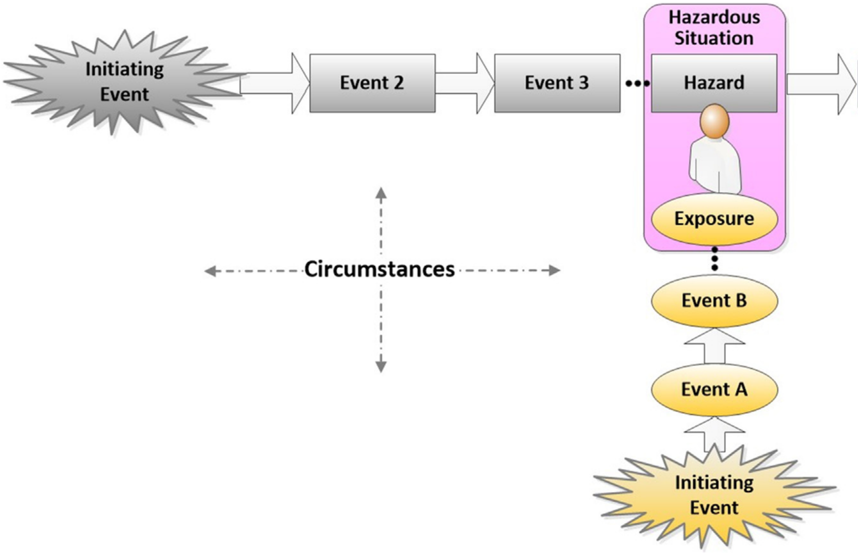


Figure 2 Hazard Theory.

4.3 SYSTEMS AND SYSTEM TYPES

The systems that are under consideration are engineered system, not natural systems such as an ecosystem, or social/governmental systems. The definition of engineered systems per INCOSE is "An engineered system is a system designed or adapted to interact with an anticipated operational environment to achieve one or more intended purposes while complying with applicable constraints."

More generally, INCOSE defines: "A system is an arrangement of parts or elements that together exhibit behavior or meaning that the individual constituents do not."

Systems have functions, behaviors, characteristics, physical structures and connectivity, both internal to the system, and external to the system. Sometimes systems exhibit unintended behaviors that were not recognized in advance, e.g., sneak paths. These could present hazards under non-failure conditions.

The Systems that are subjected to the risk management process can be classified into two categories:

a. Integral Systems
These are Systems that are observable as one integral piece from the perspective of the user. They do not require any assembly or integration by the user. Example: a blood glucose monitor.

b. Distributed Systems
These are Systems that comprise multiple components from the perspective of the user and require integration by the user. Example: a spinal cord stimulation System shown below with six individually integral components. Each integral component is separately approved, packaged and delivered to the user. Final assembly and integration into a working System is done by the user.

Reprinted with the permission of Medtronic ©.

CHAPTER 5

Understanding Risk

Abstract

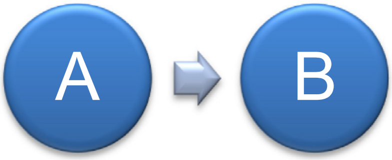
The word “risk” derives from the early Italian risicare, which means “to dare.” The modern concept of risk and the associated mathematics of probability and statistics were driven first by an interest in gambling. In the 17th century Blaise Pascal, a French mathematician was one of the first to address the puzzle of probability of the outcomes of a game of chance. There are many types of risk. This book is focused on safety risks, and contributors to risk. A major contributor to risk is the human, be it the designer, builder, maintainer, or the user of the System. Assuming good intention, the main cause of human influence on risk is inconsistency between reality, and the mental model of reality that the human holds.

Keywords: Risk; contributors to risk; risk perception; risk computation; mental models

The word ‘risk’ derives from the early Italian *risicare*, which means ‘to dare’ [12]. Centuries ago people had some awareness of risk — that sometimes things went wrong, and sometimes they went right. They attributed this to good and bad luck. Not understanding risk, they attributed the cause of their bad luck to the displeasure of the gods. Consulting with priests and shamans, they sacrificed animals and sometimes humans, thinking that would please the gods and improve their luck. This was an early form of risk control. The modern concept of risk and the associated mathematics of probability and statistics were driven first by an interest in gambling. In the 17th century Blaise Pascal, a French mathematician was one of the first to address the puzzle of probability of the outcomes of a game of chance. Pascal turned to Pierre de Fermat and together they created the theory of probability [12]. This meant that for the first-time people could make decisions based not on superstition, but on numbers.

Another interesting consequence of this discovery was the invention of insurance, which itself promoted risk-taking in business and advanced international commerce.

Risk answers the question: if A happens, what is the probability of B happening? We employ statistics as a tool to leverage our knowledge of the past to predict the future.



In many cases risk implies *choice*. That is, with a prediction of the probability of B, we choose whether to take action A. Take the example of investments. We choose

DOI: https://doi.org/10.1016/B978-0-323-85755-0.00005-9

whether to make an investment (Action A) based on our estimate of the probability of making a profit (Outcome B).

Ultimately, risk is about balancing Benefit vs. cost. Cost in the context of medical device risk management is injury or damage to health.

It's important to understand that risk cannot be eliminated – risk is managed. We cannot build a 'safe' device; that is, a device with zero risk. But we can manage the risk. Management of risk involves creating boundaries, and then engineering products such that they do not pose unacceptable levels of risk within those boundaries. Boundaries include Intended Use, intended user, intended use environment, and indicated therapy. According to [9], in the absence of a specific declaration of Intended Use by the manufacturer, generally understood patterns of usage can construe the Intended Use.

Safety is an emergent system property. That is because users interact with the system, not with just parts of the system. For example, a car is a system. Users interact with a car-system for the benefit of transportation. A tire is a component of the car-system. A tire disintegration does not pose a safety risk, if it is sitting in storage. But a tire disintegration does pose a safety risk if it is part of the car-system.

5.1 RISK DEFINITIONS

There are a number of definitions for 'risk.' Let's examine some:

1. Combination of the probability of occurrence of Harm & the Severity of that Harm [2]
2. The objectified uncertainty regarding the occurrence of an undesirable event [13]
3. The probability of occurrence of something undesirable
4. Probability of sustaining Harm in a Hazardous Situation

To provide beneficial information, risk needs to be measurable – quantitatively or qualitatively. Simply knowing there is a risk of Harm is not very useful. One needs to know the magnitude of risk to be able to make a sound decision. Consider disclosure of risk by pharmaceuticals. Pfizer describes the following risks for taking Lipitor®, a common statin drug for fighting cholesterol:

- Diarrhea
- Upset stomach
- Muscle and joint pain
- Feel tired or weak
- Loss of appetite

- Upper belly pain
- Dark, amber-colored urine
- Yellowing of your skin or the whites of your eyes
- . . .

There is no citation of the probability of occurrence for any of the above harms. Without that information, it is not possible to make a sound decision as to whether to take Lipitor® or not. Consider if the probability of occurrence of a Harm were 99% vs. 0.01%; wouldn't your decision be affected by that knowledge?

If quantitative data is not available, relative, qualitative information would also be helpful. For example, if Crestor®, which is another popular statin drug, claimed that relative to Lipitor® their risks of side-effects are lower, a patient might choose Crestor® over Lipitor®.

5.2 TYPES OF RISK

The word risk can conjure up many thoughts in people's minds, depending on the point of view of the listener. A project manager may think of risk to on-time completion of the project. A CEO may think of the business risk. An engineer may think of technical risk of not meeting requirements. A lawyer may think of infringing on someone else's Intellectual Property (IP).

Some examples of types of risk:

- Project risk
- Financial risk
- IP Risk
- Security risk
- Technical risk
- Schedule risk
- Regulatory risk
- Safety risk

In this book, we focus only on safety risk. It is important that when you use the term: 'risk management' to make sure your audience understands which type of risk you are talking about.

Due to inadequate understanding of risk, Harm and risk are frequently confused. The manufacturers are required to disclose Residual Risks of medical devices, or pharmaceuticals. As seen in the example of Lipitor® in Section 5.1 above, typically a list of Harms is presented to fulfill this requirement. This book helps to provide more clarity and distinctions on these terms to help reduce or prevent such confusions.

Safety risks of a medical device should be managed separately from project or business risks in order to avoid dilution of attention to patient safety.

5.3 CONTRIBUTORS TO RISK

A major contributor to risk is the human, be it the designer, builder, maintainer, or the user of the System. Assuming good intention, the main cause of human influence on risk is inconsistency between reality, and the mental model of reality that the human holds. Mental models are necessary to function in life. Consider this model: putting your hand in boiling water will cause a burn. Imagine if you lost this mental model and had to relearn this every time.

Leveson [14] says all models are abstractions; they simplify the thing being modeled by abstracting away what are assumed to be irrelevant details and focusing on the features of the phenomenon that are judged to be the most relevant. Selecting some factors as relevant and others as irrelevant is, in most cases, arbitrary and entirely the choice of the modeler. That choice, however, is critical in determining the usefulness and accuracy of the model in predicting future events.

The mental models that we hold are hypotheses based on theories or empirical observations. Their usefulness depends on how accurately they model reality. If the models that we employ in risk management are incorrect, the safety Risk Controls that we devise may not be effective in reducing risk.

The event-chain model of causation is one of the most common ways of modeling accidents. This was depicted in Fig. 2 above. Extending the event-chain model to risk management suggests that the most obvious countermeasure for preventing Harm is to break the chain of events before the Harm happens. While this is a useful model, care should be taken to consider factors that could indirectly affect the model. For example, in the 1970s if you wanted to safely stop a car while driving on ice, the advice was to pump the brake pedal, so as to avoid locking the wheels and skidding. Modern cars are equipped with anti-lock brakes. When driving a car with anti-lock brakes, the way to stop the car most quickly is to step on the brake pedal as hard as you can, because the brake system does the pumping automatically. Using the model of braking from older cars, on a modern car, actually reduces the braking capability of the car and increases the stopping distance, hence increasing the risk of a car crash.

5.4 RISK PERCEPTION

ISO/TR 24971 [15] says “It is important to consider that the perception and understanding of risk acceptability can vary between different groups of stakeholders and can be influenced by their background and the nature of their interest.” To meet the expectations of public opinion, it might be necessary to give additional weighting to some risks. In some cases, it might be necessary to consider that the identified stakeholder concerns represent the values of society and that these concerns have been taken into account.

Risk perception and tolerance are strongly influenced by human psychology. The same circumstance would be perceived differently by different people. In fact, this is why stock markets work – some people think that the risk of losing money is high, so they sell, while others think the risk of losing money is low and they buy.

When an adverse event happens, the public perception of the risk of that event suddenly jumps up. In the early 1980s Aeroflot, the Russian airlines, had a string of airplane crashes. All the airplanes involved in the crashes were Tupolev model Tu-154. At that time, there were people who would refuse to get on their flight if the brand of aircraft for the flight was Tupolev. We see this in any industry, including the medical device industry. When a particular medical device is involved in an adverse event, all other devices of the same type become suspect. You may remember adverse events related to silicone gel breast-implants ruptures, that terrified many women, even if nothing happened to them.

Risk perception is also influenced by other factors. For example, whether exposure to the Hazard seems to be involuntary, avoidable, from a man-made source, due to negligence, arising from poorly understood causes, or directed at a vulnerable group within society. People tend to be more tolerant of natural risks than risks due to man-made sources. Risk to children is less tolerated than risk to adults.

Michael Lewis says in the Undoing Project [16] "What people call risk aversion is tantamount to a fee that people pay, willingly, to avoid regret – a regret premium." Let's say you are at a horse race, and you have $5 to bet. They give you 10 to 1 odds on a horse. That is, there is a chance that in a short amount of time you can get 1000% return on your money. Or, you can lose your $5. Avoiding taking this risk means you are willing to pay a $50 premium not to feel the regret of losing $5, if your horse didn't win. How this plays out in medical devices is that people are willing to forego a high chance of Benefit from a device, to avoid a low chance of receiving health damage from the device. This calculus changes if a person is desperate. For example, terminal patients are willing to accept higher risk devices for a lower Benefit.

5.5 RISK COMPUTATION

Clause 5.5 of ISO 14971 [1] requires that the manufacturers estimate the risks associated with each identified Hazardous Situation. The Standard [1] offers a figure in its annex C, which is replicated below in Fig. 3. The interpretation of this figure is that after a Hazard has manifested, through the progression of a sequence of events, a Hazardous Situation is realized, where people, property, or the environment are exposed to the Hazard(s). The probability of occurrence of the Hazardous Situation is called P1. Given the Hazardous Situation, there is a probability that the subject

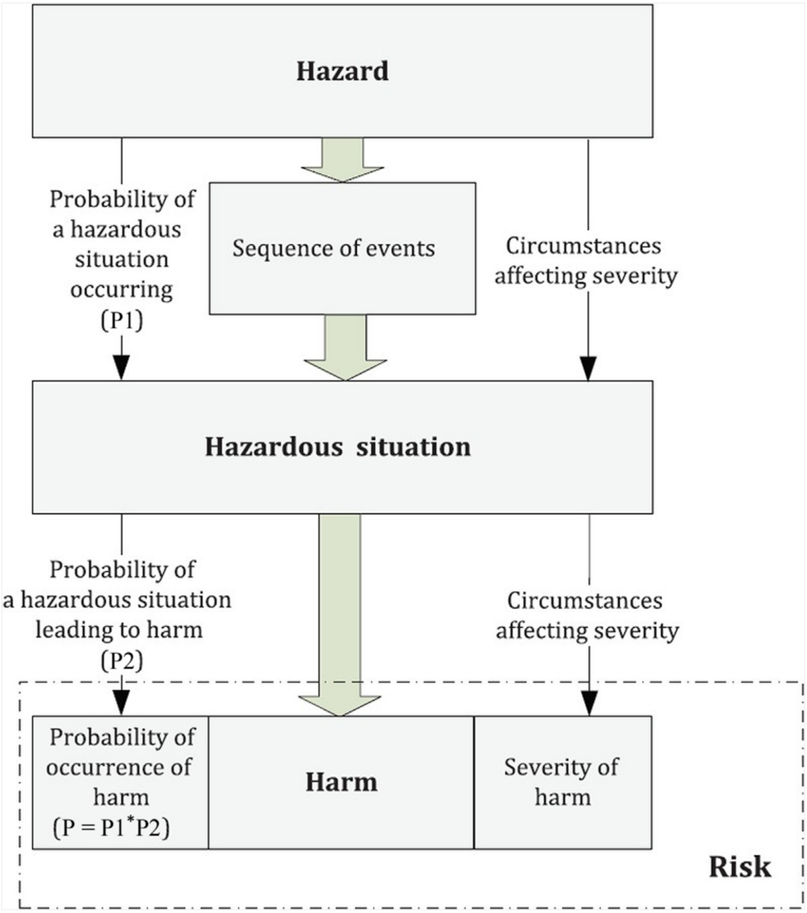

Hazard
Probability of a hazardous situation occurring (P1)
Sequence of events
Circumstances affecting severity
Hazardous situation
Probability of a hazardous situation leading to harm (P2)
Circumstances affecting severity
Probability of occurrence of harm (P = P1*P2)
Harm
Severity of harm
Risk

Figure 3 Risk Estimation — ISO 14971.

(people/property/the environment) can be harmed. This probability is called P2. The product of P1 and P2 is risk. Another way to interpret this is:

Risk is the probability of sustaining Harm in a Hazardous Situation

Notice that in Fig. 3 there is a dotted line around the Harm. The reason for this is that given the same Hazardous Situation, different people (subjects) experience different degrees of Harm. For example, when exposed to the influenza virus, some people with a strong immune system may experience nothing, while others may show the typical symptoms of fever and aches, and some people might even die from influenza (the flu). Without prescribing how to address these different degrees of Harm, the Standard [1] leaves the door open for the manufacturer to choose how to address this phenomenon.

Traditionally, many manufacturers take the conservative route and assume the worst-case Harm. This creates two problems. First, for many Harms there is a chance, though small, that the patient may die. Manufacturers who use the “worst case” strategy find themselves facing an exaggerated picture of the hazards of their device — a picture that seemingly shows patients could die due to most of the Hazards related to the device, even though historical data shows otherwise. Those manufacturers find themselves forced to over-design their devices, wasting a lot of engineering resources. The second problem is that resources are then spent on the highest Severity Harms based on worst-case analysis, while moderate Severity Harms that are actually more probable, get less attention. This means a lower-risk Harm would get priority over a higher-risk Harm. Remember risk = P1 × P2. Basing the prioritization decision only on the Severity of harms, loses sight of the probability of occurrence of the harms.

The BXM method uses a 5-value scale of Harm Severity based on the terms and definitions provided in Table 4 of ISO/TR 24971 [15]. These terms and definitions can be found in Table 27 in Section 17.2 below. Note that these terms have changed since the first edition of this book, and the second edition of ISO 14971 [17]. Namely,

- *Catastrophic* was changed to *Fatal* because ISO 14971 intends the highest Severity category to mean ‘death.’ The word *Catastrophic* could be misinterpreted as something very dire, but not necessarily death. The word ‘Fatal’ is unmistakable.
- *Serious* was changed to *Major* because the word ‘Serious’ is used with different meanings in other Standards such as IEC 62304 [10], and ISO 14155 [18]. Use of the word ‘Major’ will serve to reduce confusion.

With the 5-value Harm-Severity model, an enhancement to Fig. 3 can be made as depicted in Fig. 4.

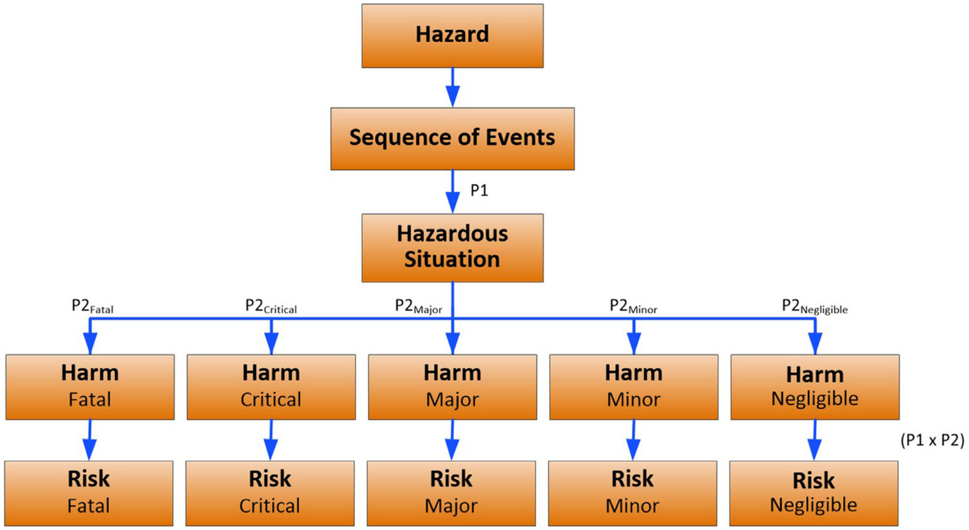


Figure 4 5-Value Risk Estimation.

Note that P1 has dimension, but P2 is dimensionless. Therefore, Risk, which is P1 × P2, has the same dimensions as P1.

Examples of P1:

- Probability of exposure of the patient to a damaged cannula is 1 in 1000 uses.
- Probability of a patient not receiving pacing from their pacemaker is $<10^{-5}$ per patient-year.

Examples of P2:

- Probability of death from intracranial hemorrhage is 2.5%.
- Probability of permanent impairment or irreversible injury from corneal scratching is 4%.

CHAPTER 6

Risk Management Standards

Abstract

There are a number of standards that address safety for medical devices, e.g., ISO 14971, IEC 60601-1, IEC 62304, IEC 62366, ISO 10993-1, and so on. ISO 14971 is the central standard for risk management of medical devices and is recognized both in the EU and the United States. Compliance with ISO 14971 is the most common way of establishing the case for the safety of a medical device.

Keywords: ISO 14971; IEC 60601-1; ISO 14971:2019; normative reference; harmonized standards

There are a number of standards that address safety for medical devices, e.g., ISO 14971 [1], IEC 60601-1 [7], IEC 62304 [10], IEC 62366 [19], ISO 10993-1 [20], and so on. Fig. 5 illustrates six such standards. ISO 14971 is the central standard for risk management of medical devices and is recognized both in the EU and the United States. The other medical device safety standards in Fig. 5 make normative references to ISO 14971 [1], which means the requirements of ISO 14971 [1] become their requirements. ISO 14971 [1] establishes a framework and defines a set of requirements for performing risk management, but it does not stipulate any specific process.

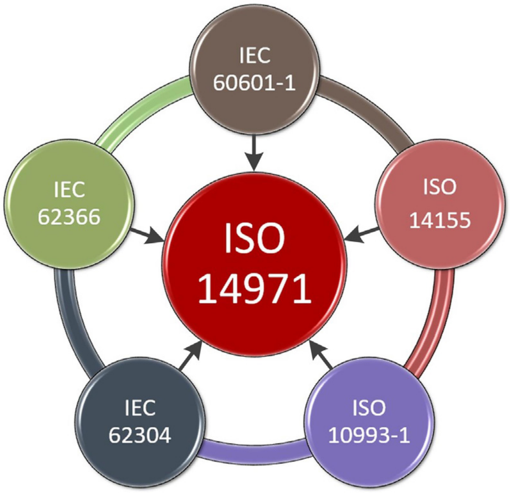


Figure 5 ISO 14971, a Central Standard.

Safety Risk Management for Medical Devices
DOI: https://doi.org/10.1016/B978-0-323-85755-0.00006-0

Most of the safety standards are becoming progressively more outcome based and less prescriptive. They specify what outputs are expected and give you the freedom to choose your own methods. This is both a blessing and a curse. On the one hand, you get freedom to create your own process. On the other hand, the standards don't tell you how to do things, so the method that you choose becomes subject to questioning and you must be prepared to defend it.

For all regulated medical devices, the manufacturers must show that formal risk management processes have been applied and that their respective safety risks have been reduced to acceptable levels.

Tip The FDA maintains a database of recognized consensus standards. You can access this database at https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfStandards/search.cfm

6.1 ISO 14971 HISTORY AND ORIGINS

ISO 14971 was originally developed in 1998 with participation from 112 countries. It is widely recognized as the official international standard for medical device risk management.

To produce ISO 14971, ISO/TC 210 WG4 was formed. Simultaneously the IEC 60601-1 third edition was planning to include risk management for medical devices. In order to combine efforts, JWG1 IEC/SC 62A was formed, so 14971 is the product of work by both IEC and ISO. The ISO designation was chosen because 14971 is not just about medical electrical equipment, but about all medical devices.

ISO 14971 was first released in the year 2000. The second edition was promulgated in March 2007, which canceled and replaced the 2000 version. In 2012, the European community identified discrepancies between ISO 14971:2007 [17] and EU directives: 93/42/EEC on Medical Devices [3], 90/385/EEC on AIMDs, and 98/79/EC on in Vitro Diagnostics, and added three annexes: ZA, ZB, and ZC, to the second edition of ISO 14971 [17] to create the European harmonized standard EN ISO 14971:2012 [21]. In December of 2019 the third edition of ISO 14971 was released. The third edition removes and cancels the previous editions of ISO 14971. Adoption of ISO 14971:2019 [1] by CEN/CENELEC in Europe engendered EN ISO 14971:2019. ISO 14971:2019 and EN ISO 14971:2019 are identical.

To assist the users of ISO 14971 [1], ISO released a companion document: ISO/TR 24971:2020 [15], as guidance on the implementation and maintenance of a risk management system in conformance with ISO 14971 [1]. ISO/TR 24971:2020 [15] contains no normative requirement. The section numbers of ISO/TR 24971:2020 [15] are aligned with the section numbers of ISO 14971 [1] for the convenience of the reader. Annexes A, B, and C of ISO/TR 24971:2020 [15] provide additional insights and guidance on the implementation of sections 1—10 of ISO 14971:2019 [1].

While ISO 14971 is primarily intended for medical devices, it can also be used by other entities who are involved in the creation of medical devices, such as suppliers. This standard could also be applied to other products which are not necessarily considered to be medical devices in all jurisdictions. For example, contact lenses, tattooing devices, and other products that are listed in Annex XVI of the EU MDR [2].

Prior to ISO 14971 there was no other standard to address the risk management of medical devices. ISO 14971 was drafted as a framework because it would be difficult to create a specific process that is optimal for all medical devices. Manufacturers are to create ISO 14971-conformant internal procedures that are optimally suited to their products.

ISO 14971 [1] requires manufacturers to establish, implement, document, and maintain an ongoing risk management process and apply it to the entire life cycle of medical devices from concept to decommissioning and disposal.

ISO 14971 is written as a generic safety standard to encompass all medical devices. For this reason, safety risk management benefits from the use of additional specific safety standards, such as IEC 60601-1, IEC 62304, ISO 10993-1, etc. In particular IEC 62366-1 complements ISO 14971 in the area of usability and addresses Hazardous Situations that can arise from use-errors.

ISO 14971 doesn't require the manufacturer to implement a QMS, but EU MDR [2] and IVDR [22] do require manufacturers to implement a QMS that addresses RM. Therefore it is advisable to implement a QMS and ensure the inclusion of the RM process within the QMS.

ISO 14971 [1] is intended for the management of risks of Harm not only to humans, but also to data, property, and the environment. There are times when Harm to data, property, or the environment leads to Harm to humans as well, e.g., damage to the software of a life-saving device, or release of toxic materials to the environment could lead into Harm to humans. There are also times when Harm to data, property, or the environment does not result into Harm to humans. ISO 14971 can be used to manage the risks of Harm in both cases. Clearly, these are very different types of Harm and are best managed separately.

6.2 HARMONIZED STANDARDS

In a strict legal sense, regulatory entities do not 'require' compliance with ISO 14971 [1]. Under EU legislation, the use of standards (or harmonized standards) is purely voluntary and you are free to comply with the General Safety and Performance Requirements of Annex I of EU MDR [2] via other means. However, with regard to risk management, ISO 14971 [1] is the recognized reference standard, and compliance to it makes it easier to persuade a Notified Body that your device is acceptably safe.

Conformance to ISO 14971 [1] provides other benefits to QMS. For example, clause 7 in ISO 13485 [23] about product realization and clause 8.2.1 on feedback during monitoring and measurement are related to risk management and can be fulfilled by conformance with ISO 14971 [1].

CHAPTER 7

Requirements of the Risk Management Process

Abstract

ISO 14971 offers a framework for managing the risks of medical devices. Rather than being prescriptive, this framework has specific requirements and expectations, i.e., hazard identification; risk estimation, evaluation, and control; risk management review; and production and post-production activities.

Keywords: Risk management process; risk management framework; fault condition

ISO 14971 [1] offers a framework for managing the risks of medical devices. Rather than being prescriptive, this framework has specific requirements and expectations, namely:

- Have a documented process, and apply it to the entire product life cycle.
- Have a plan for risk management.
- Identify the Hazards and related Hazardous Situations for the medical device.
- Estimate and evaluate the individual risks.
- Control the risks.
- Verify the effectiveness of the Risk Controls.
- Ensure completeness of Risk Controls for all identified risks.
- Evaluate the Overall Residual Risk.
- Show that the Benefits outweigh the risks.
- Perform risk management review.
- Produce a Risk Management Report.
- Monitor Production and Post-Production information and take appropriate actions based on the findings.
- Create and maintain a Risk Management File.
- Show traceability among Hazards, risks, Risk Analysis, evaluation and control, and verification of Risk Controls.
- Use competent personnel to perform Risk Management.

The manufacturer is free to create the internal processes to meet the above requirements.

7.1 RISK MANAGEMENT PROCESS

The risk management process should have at least the following elements:

Safety Risk Management for Medical Devices
DOI: https://doi.org/10.1016/B978-0-323-85755-0.00007-2

7.1.1 Risk Analysis

The requirements for Risk Analysis are:

- Provide a description and identification of the medical device under analysis.
- Define the scope of analysis – what's included and what's excluded.
- Identify the Intended Use, and Reasonably Foreseeable Misuses of the medical device.
- Identify the safety characteristics of the medical device.
- Identify the Hazards that the device could present.
- For each identified Hazard, describe the reasonably foreseeable sequences or combinations of events that could result in a Hazardous Situation.
- Estimate the risk for each Hazardous Situation.

You are required to identify the persons who perform the Risk Analysis. This is necessary for confirmation of qualification of such individuals. Also, the date of the analysis must be recorded.

7.1.1.1 Hazard Identification

The Standard [1] requires manufacturers to identify and document known and foreseeable Hazards associated with medical devices based on the Intended Use, Reasonably Foreseeable Misuse, and the characteristics related to safety, under both normal and fault conditions. This defines four types of Hazards that can manifest under various use conditions. Table 2 captures this Hazard taxonomy.

Table 2 Hazard Taxonomy

		Hazard Type	
		Known	**Foreseeable**
Fault Condition	Normal	X	X
	Fault	X	X

A number of techniques are used to identify the System Hazards. For example, Fault Tree Analysis (see Section 14.1 for details), and Failure Modes and Effects Analysis (see Section 14.4 for details).

Other techniques of Hazard identification are: search of published literature for reported Hazards of similar devices; search of databases such as MAUDE [30], and Eudamed [31]; and examination of ISO 14971 [1], Table C.1. In Table C.1, there is a listing of many common Hazards that could help with the identification of Hazards that are related to your medical device.

7.1.1.2 Risk Estimation

Risk Estimation methods are explained in detail in Chapter 17.

7.1.2 Risk Evaluation

Risk Evaluation requires knowledge of risk acceptance criteria. See Chapter 21 for a detailed discussion of Risk Evaluation.

7.1.3 Risk Control

See Chapter 18 for a detailed discussion of Risk Controls.

7.1.3.1 Risk Control Verification

See Chapter 19 for a detailed discussion of verification of Risk Controls.

7.1.4 Evaluation of Overall Residual Risk

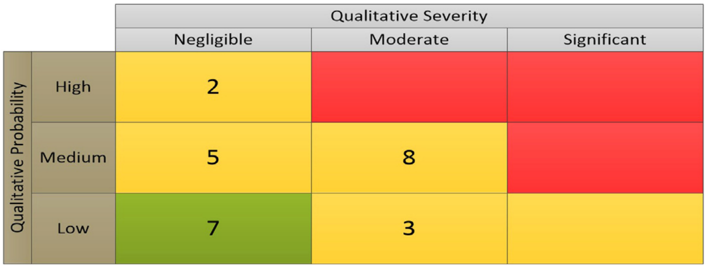
The Overall Residual Risk is the aggregation of all individual risks, after each individual risk has been reduced and accepted. The Standard [1] requires that the method to evaluate the Overall Residual Risk be documented in the Risk Management Plan. Determination of the Overall Residual Risk is not a trivial matter and cannot be determined by simply adding all the individual risks. Different methods are possible. Below, three methods are presented.

Method 1 – Quantitative Approach

If you follow the BXM method which is presented in this book, you will be able to use Boolean algebra to compute the aggregate of all the individual risks and arrive at a risk number in each of the five Severity classes. Then you simply compare the Overall Residual Risks in each Severity class against the acceptance criteria. If the Overall Residual Risk is higher than the risk acceptance criteria, it is unacceptable. Otherwise it is acceptable.

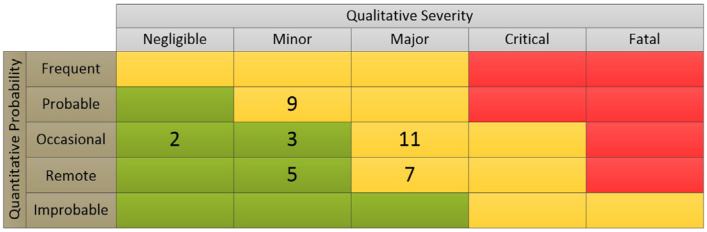
Method 2 – Qualitative, or Semi-Quantitative Approach

In this approach you create a visual representation of individual Residual Risks, by tallying the number of individual risks in each representative cell. It would look something like Fig. 6 or Fig. 7. Then you evaluate this risk profile for acceptability. If there is a predicate device, which could be your own previous generation device, then you compare the risk profiles of the old vs. the new device. If there is no predicate risk profile to compare, then you will seek a subjective judgement from experts with the knowledge, authority, and relevant experience with your medical device.



		Qualitative Severity		
		Negligible	Moderate	Significant
Qualitative Probability	High	🟨 2	🟥	🟥
	Medium	🟨 5	🟨 8	🟥
	Low	🟩 7	🟨 3	🟨

Figure 6 Qualitative Risk Profile Example.



		Qualitative Severity				
		Negligible	Minor	Major	Critical	Fatal
Quantitative Probability	Frequent	🟨	🟨	🟨	🟥	🟥
	Probable	🟩	🟨 9	🟨	🟥	🟥
	Occasional	🟩 2	🟩 3	🟨 11	🟨	🟥
	Remote	🟩	🟩 5	🟨 7	🟨	🟥
	Improbable	🟩	🟩	🟩	🟨	🟨

Figure 7 Semi-Quantitative Risk Profile Example.

Method 3 – Risk-Differential Approach

In this approach you compare the subject device against a very similar approved predicate device which is in use and available on the market. The predicate device might be your own previous generation device. The basis of this logical approach is the inference that the predicate device has an acceptable Overall Residual Risk. The presumption in this approach is that there are few differences between the subject device and the predicate device, and the Benefits are comparable. Next, we identify the individual risks that are different between the subject device and the predicate device.

If we can show that the risks of the differentiated individual risks in the subject device are lower than the predicate device, logically we can deduce that the Overall Residual Risk of the subject device is acceptable.

7.1.5 Risk Management Review

At the conclusion of the risk management process for medical devices, the Standard [1] requires the review of the final results. See Chapter 24 for a detailed discussion of the Risk Management Review.

7.1.6 Production and Post-Production Activities

Once the risk management process is completed and the medical device is released to the market, it is required that manufacturers continuously monitor for how the product is performing. This can take the form of surveillance, which is active seeking of information, or complaint handling, which is the passive method of receiving information. All collected information is to be used to update the risk management work products as necessary. See Chapter 25 for a detailed discussion of Production and Post-Production activities.

CHAPTER 8

Quality Management System

Abstract

Your Quality Management System (QMS) is the internal reflection of the external standards. Your SOPs bring the standards to life within your company. A clear, organized, and well-written SOP sends a message to regulatory bodies that your QMS is consistent and compliant to applicable standards. More importantly, well-written SOPs ensure that your personnel can faithfully and accurately follow your internal processes resulting in proper outcomes and quality work. On the other hand, a poorly written confusing SOP could result in noncompliance, which could lead to observations and warnings from regulatory bodies at best and in some cases, severe penalties.

Keywords: Quality Management System; risk management; SOP; template; work instruction

Your Quality Management System (QMS) is the internal reflection of the external standards. Your SOPs bring the standards to life within your company. A clear, organized and well-written SOP sends a message to regulatory bodies that your QMS is consistent and conformant to the applicable Standards. More importantly, well-written SOPs ensure that your personnel can faithfully and accurately follow your internal processes resulting in proper outcomes and high-quality work. On the other hand, a poorly written and confusing SOP could result in non-compliance, which could lead to observations and warnings from regulatory bodies at best and in some cases, severe penalties including consent decrees and the shutdown of the company.

In addition to SOPs, many companies employ templates and work instructions to assist in the quality execution of the risk management work. While SOPs are more high-level and designed to ensure compliance to applicable standards, work instructions provide detailed guidance on how to do the work.

As with all other controlled documents, risk management artifacts must be controlled per the methods that are stipulated in your QMS. Absent this strict control, it would be easy for analyses and their targets to go out of sync. That, in turn could lead into unwanted outcomes like missed Hazards, injured patients, audit findings, etc.

Interestingly, ISO 14971 [1] does not require manufacturers to have a quality management system in place. However, almost universally manufacturers of medical devices conform to ISO 13485 [23], which specifies the requirements for a QMS. Also, EU MDR [2] section I (32) says that all manufacturers should have a QMS. Having a

Safety Risk Management for Medical Devices
DOI: https://doi.org/10.1016/B978-0-323-85755-0.00008-4

QMS is best practice with many benefits. One of the great benefits of a good risk management process is the ability to provide safety impact analysis of proposed changes. In any good QMS, an impact analysis is done for any proposed change to a controlled design. One aspect of this impact analysis should be the determination of the effects of the proposed change on safety. Without the benefit of a formal risk management process, estimation of the safety impact of a proposed change would be just a guess.

CHAPTER 9

Usability Engineering and Risk Analysis

Abstract

Medical devices are providing ever more benefits and at the same time are becoming more complex with user interfaces that are not so intuitive, difficult to learn, and difficult to use. Use-Errors caused by inadequate medical device usability have become an increasing source of adverse safety events. As healthcare evolves, and more home-use is promoted as a cost-saving measure, less skilled users including patients themselves are now using medical devices. This chapter examines the contribution of usability engineering to the safety of medical devices.

Keywords: Use Failure; Use Error; usability engineering; IEC 62366; human factors; user-device interaction; task analysis

Medical devices are providing ever more Benefits and at the same time are becoming more complex. The users must interact with these devices to gain the Benefits that they offer. The user interface is critical to the success of the user. Engineering the user interface such that it is intuitive, easy to learn and use is not trivial. Use Errors caused by inadequate medical device usability have become an increasing source of adverse safety events. As healthcare evolves, and more home-use is promoted as a cost-saving measure, less-skilled users including patients themselves are now using medical devices. This makes usability engineering an ever more important aspect of safety risk management. Usability engineering process is intended to analyze and evaluate risks related to Use Errors and help drive better designs that enable user success.

A distinction

Use failures, which include Use Errors, describe the failure of a User to achieve the intended and expected outcome from the interaction with the medical device. The design of a device may make it difficult, or impossible for the user to use the device, even though no error is made. Physical constraints in strength, reach, or sensory acuity may prevent the user to perform the required task. Further, the user interface may be confusing and cause the user to make mistakes in performing tasks, these are use-errors.

The Standard IEC 62366 [19] does not use the term 'use failure,' instead it defines the term 'use error' as "user action or lack of user action while using the medical device that leads to a different result than that intended by the manufacturer or expected by the user." For consistency with the Standard [19], the term 'Use Error' is used in this book to mean both use-failure and use-error as distinguished above.

Safety Risk Management for Medical Devices
DOI: https://doi.org/10.1016/B978-0-323-85755-0.00009-6

It is worth noting that in the past, the terms 'user error,' or 'human error' were commonly used. This would create the implication that users were to be blamed and the manufacturers were blameless. While it is true that users do make errors, in many cases improvements to the design, or training can help reduce the potential for the users to make errors. The problem with using 'user error' is that it directs the attention to the outcome, not the cause. The FDA and usability engineering standards do not advocate the use of the term 'user error' and instead use the term 'use error.'

The leading standard for usability engineering of medical devices is IEC 62366 [19]. The latest edition of this Standard, Edition 1.1 2020-06, was released in 2020 and contains the first edition (2015-02) and its corrigendum (2016-07), and its amendment 1 (2020-06). IEC 62366 is produced jointly by IEC and ISO, and is published as both an IEC and an ISO Standard.

This international standard describes a usability engineering process to provide acceptable safety risks as related to the usability of a medical device. It should be noted that the scope of usability engineering is larger than safety. Usability engineering is also concerned with how well and easily the user can interact with the medical device in order to achieve their desired outcomes. Therefore customer experience and satisfaction are also influenced by usability engineering.

The companion document, IEC TR 62366-2 [24], provides guidance on the application of usability engineering to medical devices. This technical report contains background information that can be helpful in implementing usability engineering per the Standard [19], and for supporting extended goals beyond safety, e.g., task efficiency and user experience.

IEC 62366 [19] provides a process to assess and mitigate the risks associated with the correct-use and Use-Errors. Malice and Abnormal Use are excluded from the risk management process. See Sections 9.1 and 9.2 for further elaboration and elucidation of these terms. There is one exception to this exclusion: Security breaches deliberately bypass the Risk Controls that are put in place by the manufacturer. As such, they fit the definition of Abnormal Use. But they should be included in the scope of risk management.

It should be noted that the FDA considers Human Factors and Usability Engineering to be synonymous. See FDA Guidance on HFE [25], par 3.6. Also, the FDA has replaced the term "user error" with "use error." This means that Use Error is considered by the FDA to be a device nonconformity because human factors should be considered in the design process. Continuing this thought, it might make sense in some cases to consider the user as part of the system, and derive user requirements.

With more and more automation, artificial intelligence, and machine learning, gradually the machines are taking over more of the tasks and decision-making from humans. While this has its benefits, an unexpected side effect is that humans become less alert due to growing trust and dependency on the machines. As a result, humans become more prone to making mistakes. We can learn from aerospace experience in this regard. Automation has been used in aviation for a long time, to reduce pilot workload and increase safety. But when pilots become very dependent on automation their skills start to erode, and when the moment arrives that automation is not able to handle the situation and the responsibility befalls the human pilot, panic sets in. There is an old saying in aviation that being an airline pilot is 99% boredom and 1% sheer terror.

Tip Start usability engineering right from the start of product development. Though the FDA requires summative studies, they also want a summary of how usability engineering was performed throughout the design process.

9.1 KEY TERMS

Below, a select group of terms are defined. A clear understanding of these terms is important in the proper dispositioning of Use-Errors, and is also beneficial for communication with team members.

Term	Definition
Abnormal Use	Conscious, deliberate act or deliberate omission of an act that is counter to or violates Normal Use and is also beyond any further reasonable means of user interface-related risk control by the manufacturer [19] 3.1.
Action Error	One of the causes of Use Error. Related to error in performance of an action, and not primarily due to perception or cognition deficiencies.
Cognition Error	One of the causes of Use Error. Related to deficiency in cognition, and not primarily due to perception deficiencies or the inability to perform the action.
Correct Use	Normal Use without Use Error [19] 3.3.
Formative Evaluation	User interface evaluation conducted with the intent to explore user interface design strengths, weaknesses, and unanticipated Use Errors [19] 3.7. Also known as Formative Study.
Hazard-Related Use Scenario	Use Scenario that could lead to a Hazardous Situation or Harm [19] 3.8.

(*Continued*)

(Continued)

Term	Definition
Lapse	A memory failure. The User had the knowledge but temporarily forgets the knowledge and makes a decision based on incorrect knowledge. User executes the decision without Slips. This term was used in IEC 62366 2007 version, but not used in the 2020 version.
Malice	Intentional act to do harm to people, property, or the environment.
Mistake	Deficiencies or failures in the judgmental and/or inferential processes. User executes without Slips. Adapted from IEC 62366:2007 Annex B. This term was used in IEC 62366 2007 version, but not used in the 2020 version.
Misuse	Incorrect or improper use of the medical device [17] 4.2, Note 1. Note – this is not an official definition.
Normal Use	Operation, including routine inspection... according to the instructions for use or in accordance with generally accepted practice for those medical devices without instructions for use [19] 3.9.
Perception Error	One of the causes of Use Error. Related to deficiency in perception, and not primarily due to cognition deficiencies or the inability to perform the action.
Primary Operating Function	Function that involves user interaction that is related to the safety of the medical device [19] 3.11.
Slip	The User has the knowledge and the intention but executes incorrectly. Attentional error. This term was used in IEC 62366 2007 version, but not used in the 2020 version.
Summative Evaluation	User interface evaluation conducted at the end of the user interface development with the intent to obtain objective evidence that the user interface can be used safely [19] 3.13. Note – Summative evaluations are frequently used to provide verification of effectiveness, of Risk Controls.
Task	One or more user interactions with a medical device to achieve a desired result [19] 3.14. Note – A task can be further broken down into "steps."
Usability	Characteristic of the User Interface that facilitates use and thereby establishes effectiveness, efficiency, and user satisfaction in the intended use environment [19] 3.16.
Use Error	User action or lack of user action while using the medical device that leads to a different result than that intended by the manufacturer or expected by the user [19] 3.21. Note – Use Error includes the inability of the user to complete a task.

(*Continued*)

(Continued)

Term	Definition
Use Scenario	Specific sequence of tasks performed by a specific user in a specific use environment and any resulting response of the medical device [19] 3.22.
User Interface (UI)	Means by which the user and medical device interact [19] 3.26. Note – user interface includes all the elements of the medical device with which the user interacts including the physical aspects of the medical device as well as visual, auditory, tactile displays and is not limited to a software interface; includes the accompanying documentation.

9.2 DISTINCTIONS

As defined in Section 9.1, Abnormal Use is "Conscious, deliberate act or deliberate omission of an act that is counter to or violates Normal Use and is also beyond any further reasonable means of user interface-related Risk Control by the manufacturer" [19]. Examples include reckless use, sabotage, or intentional disregard for safety instructions.

Malice is an intentional act with the aim of causing Harm. The distinction between Malice and Abnormal Use is that Malice has the intention to do Harm, while Abnormal Use is recklessness that might cause Harm.

Setting aside Abnormal Use and Malice, we are left with Normal Use. Normal Use includes the Intended Use of the device, i.e., the medical purpose of the device, as well as other ancillary uses such as maintenance, transport, etc. See Fig. 8. Also see IEC 62366 [19] Section 3.9 Note 1 to entry, for further elaboration on this concept.

Any Normal Use is subject to Use Errors, which could lead into a Hazardous Situation.

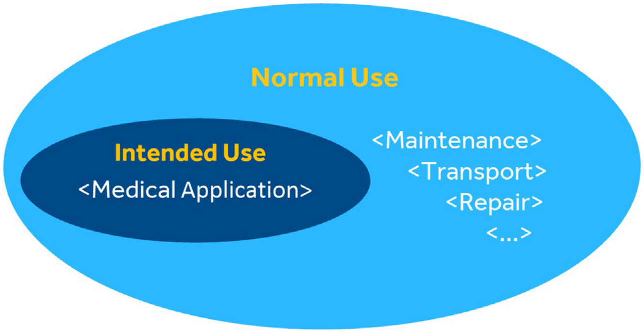


Figure 8 Types of Normal Use.

Use Error vs. Misuse — ISO 14971 [1] Section 3.15, Note 2, states that "Reasonably foreseeable misuse can be intentional or unintentional." This can create confusion between an intentional and successful off-label use of a device (a Misuse), and an unintentional Use Error. Although Risk Management addresses the safety risks of both Misuses and Use Errors, to reduce confusion it is advisable to distinguish the terms: Misuse and Use Error.

Usability Engineering is concerned with improving the usability of a device to reduce Use Errors. In contrast, to prevent a deliberate misuse would require measures to make it more difficult, if not impossible, to perform certain actions.

9.3 USER-DEVICE INTERACTION MODEL

Modeling of human interaction with technological systems helps with prediction of Use Errors and has its roots in aerospace and defense for the design of aircraft cockpits and crew stations. They model the human in three parts:

1. input/sensing
2. processing
3. output

Fig. 9 shows a model of the User-Medical Device interaction. In this figure, there are two possible ways in which a Use Error can lead into a Hazardous Situation.

a. The User enters an erroneous input into the Medical Device, which in turn produces an output that is hazardous, e.g., User enters the wrong dose on the user interface of an infusion pump.

b. Through either a perception error, or a cognition error, the User takes an action that creates a Hazard. This action could be on the Medical device, or outside of the Medical Device, e.g., a diabetic patient misreads, or misinterprets the glucose reading on a glucose monitor and administers too high an insulin dose to him/herself.

Using this model facilitates prediction of potential Use Errors, and also helps identify the required human capabilities for interacting with the medical device. This in turn can guide the design of the User Interface for safer and more effective medical devices.

Perception examples: See, Hear, Feel. Perception may be distorted, disrupted, or impossible depending on the environmental conditions. For example, a surgeon may not be able to feel surface texture with a gloved hand.

Cognition examples: Interpret, Know, Compute, Decide. Cognition also, may be difficult or compromised under conditions of stress, fatigue, heavy or multitasking workload.

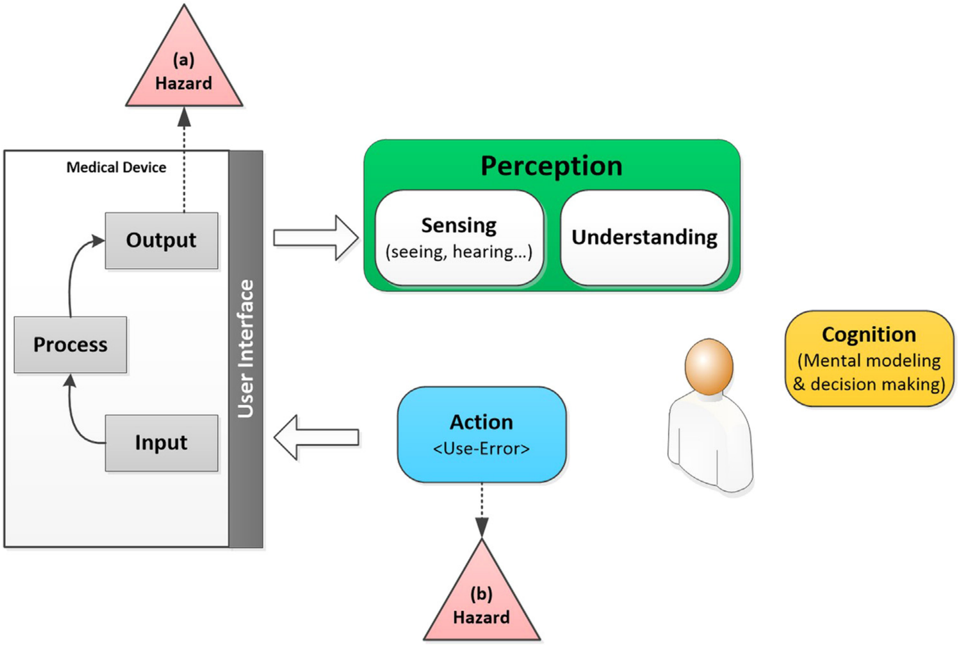


Figure 9 Model of User-Medical Device Interaction.

Action examples: Press, Touch, Twist, Pull, Push, Follow. Actions may be challenged under conditions of fatigue, pain, injury, or barriers such as gloved operations.

Design factors that could cause Use Errors include:

- Insufficient visibility, audibility or tactility.
- Complex or confusing control system which could lead to dissonance between user's mental model and reality.
- Ambiguous or unclear device state, settings.
- Poor mapping of controls to actions, or of displayed information to the actual state of the device.

In most cases, Use Errors are the result of an incongruity between the mental model that a patient/User has of the System and the actual behavior of the System. For example, in most houses the light switches that are mounted on walls are oriented in such a way that an up action causes the lights to come on, and a down action causes the lights to go off. Now imagine if you enter a room where the electrician has installed the light switch upside-down. It is easy to imagine that with the mental model that was described above, you would flip the switch up to turn on the light. And then when that fails, you flip the switch down to get the desired effect.

Not all Use Errors result in a Hazard. The BXM method employs the principles of usability engineering at the service of identification of Hazards that are the result of Use Errors. Specifically, a failure-modes-and-effects-analysis of the uses and misuses (UMFMEA) of the medical device is performed for this purpose. The inputs to the UMFMEA are the medical device use-scenarios and task analyses. See Section 14.8 for further details on UMFMEA.

9.4 USE ERRORS

In this section, we delve more deeply into Use Errors. A Use Error is the failure of a user to achieve the intended and expected outcome from the interaction with the medical device. How can this happen?

a. The user is unable to perform the task.

This could be due to confusing user interface, or physically not doable action by the user.

b. The user completes the task, but with significant difficulty.

For example, due to a confusing user interface, the user struggles, makes error(s), but notices the error(s) and corrects it, and in the end completes the task. Although by the strict definition of Use Error, this would not be a Use Error, because the user eventually completes the task, it is advisable to count this type of interaction as Use Error so that it receives the appropriate attention.

Close-calls, or near-misses where a user almost fails a task, should also be treated as Use Errors so that they could inform design decisions for improvements.

c. The user executes the task erroneously. Reasons:

- Perception error

  Example: User cannot read a display due to font size, contrast, brightness, layout, etc.
- Cognition error
  - o Memory failure
    - – Inability to recall knowledge which was gained before.
    - – Lapse. User has the knowledge but temporarily forgets, or omits an action.
  - o Rule-based failure
    - – Incorrect application of a rule to the task.
    - – Application of an inappropriate rule to the task.
  - o Knowledge-based failure
    - – User does not have the knowledge, e.g., due to no training, or not reading the instructions for use.
    - – User applies the wrong mental model, e.g., improvisation under unusual circumstances.

- Attentional error
  - Slip. User has the knowledge and the intention but executes incorrectly, e.g., transposing two keys on a keyboard.
- Action error, e.g., pressing the wrong button; reason: buttons are too small and too close to each other. Or, double hitting of a button on a user interface, e.g., intending to program a dose on an infusion pump by pressing 4, but accidentally double hitting the key and programming 44 for the wrong dose.

9.5 ENVIRONMENTAL FACTORS

Environmental factors are a contributing Cause to Use Errors. Some environmental factors that could play a role in causing Use Errors are:

- Temperature
- Humidity
- Vibration
- Atmospheric conditions
- Distractions
- Lighting
- Physical surroundings
- Acoustic noise
- Workload-related stress
- Other systems and devices in the environment of use

While you may not have any control over the environmental factors that surround the medical device, knowledge and awareness of such factors is critical for the proper design of the user interface of the medical device.

Tip Consider the typical workflows where your device will be used. If your device replaces an existing device, legacy behaviors may carry over to the use of your System.

9.6 DESIGN MEANS TO CONTROL USABILITY RISKS

In most cases, changes to the design of the medical device can serve to reduce the risks due to Use Errors. Below are some examples of such design controls:

- **Keystroke debouncing** – if the same key is pressed within 250 ms, ignore the second keystroke.

- **Reasonableness checks** – evaluate the user input for reasonableness. If the input is out of range or unreasonable, inform the user.
- **Proper sizing** – use anthropometric data to size the user interface such that physical errors are less likely, e.g., buttons sized to human fingers.
- **Alarm types** – use IEC 60601-1-8 [26] for guidance on proper design of alarms.
- **Font size** – use AAMI HE75 [27] for guidance on font sizes for visual displays.

If such design means are employed to reduce risk, they should be verified for effectiveness in risk reduction.

9.7 TASK ANALYSIS

The Standard [19] requires that the manufacturers identify user interface characteristics that could be related to the safety of medical devices. A common tool to achieve this, is task analysis. Task analysis is a formal and systematic activity that starts by creating a detailed description of sequential and simultaneous actions of the user of the medical device. Task analysis usually starts with high-level use-scenarios, and then adds tasks and ultimately details down to individual steps are spelled out. The output of task analysis is input to the UMFMEA (see Section 14.8). As such, conditions of use and user profiles are important to know and should be included in the task analysis. Task analysis results are typically stored in a tabular or flowchart format.

Task analysis should begin at concept development stage at a high-level and should progress with more details as user interface design matures. Because designs iterate multiple times during the design process, task analysis should be kept in sync with the UI design to ensure the validity of risk management with respect to UI design.

For the purposes of risk management, what is of interest are the user-performed steps, and how errors in performing them could result in Hazards.

9.8 USABILITY AND RISK

Some Use Errors can result in Hazards. The UMFMEA analyzes all Use Errors and captures the Hazards that are due to Use Errors in the End Effects column. Just as in other FMEAs, the End Effects which are Hazards are then captured in the Risk Assessment and Control Table (RACT) for Risk Estimation.

Risk is the product of P1, the probability of occurrence of a Hazardous Situation, and P2, the probability of experiencing Harm from the Hazardous Situation. P1 itself is the product of P(Hazard) and P(Exposure to the Hazard). Ordinarily, P(Hazard) can be derived from the Occurrence rating in FMEAs. However, with respect to risk, IEC 62366 [19] Annex A, Subclause 5.5 makes the following statements:

> *Selection of the HAZARD-RELATED USE SCENARIOS can be based on the SEVERITY of the potential consequences of the associated HAZARDS. It can be needed in this way to focus on HAZARDS rather than RISKS because the probability of occurrence of encountering a HAZARD, which is one component of RISK, can be very difficult to estimate, especially for a novel MEDICAL DEVICE for which no POST-PRODUCTION data are available.*
>
> *Another basis for selection of the HAZARD-RELATED USE SCENARIOS is the RISK of the occurrence of HARM to the PATIENT or USER. These values can also be difficult to determine, as they are based on assumptions closely related to probability of occurrence and without data, can be difficult to justify. Finally, and only in the presence of data that provides a justification, should RISK values based on the combination of SEVERITY and probability of occurrence of the HAZARD be used as the basis for prioritization of HAZARD-RELATED USE SCENARIOS. Values for these probabilities or probability of occurrence can be derived from POST-PRODUCTION data on current or previous versions of the same MEDICAL DEVICE or on the level of certainty that the RISK CONTROL measures are effective, which should also be justified with data.*

ISO/TR 24971 [15] provides some guidance in Section 5.5.3 that when accurate and reliable quantitative data, or a reasonable qualitative estimate based on a consensus by qualified experts is not available it is necessary to establish an upper bound on the risk. Usually this translates into assuming P1=1 and basing the Risk Estimation on the P2 alone. Ref. [15] advises to focus the Risk Controls on preventing the Hazardous Situation, i.e., getting P1 to zero, or reducing the Severity of the Harm, i.e., reducing P2.

The manufacturer has three options:

1. Ideally, eliminate the Hazardous situation, i.e., drive P1 to zero by eliminating the Hazard, or preventing exposure to the Hazard.
2. Gather data, upon which P1 could be estimated, and thus risk could be computed.
3. Use design process rigor to reduce the risk of Harm.

In the following subsections, each option is explored.

9.8.1 Elimination of Hazardous Situation

Risks that are the result of Use Errors are often controlled in the User Interface design. However, in some cases it is necessary to deploy Risk Control measures outside of the User Interface. It may be possible in some cases, to eliminate the use-related Hazardous Situation either by eliminating the Hazard, or exposure to the Hazard. For example, imagine a medical device that requires the manual entry of patient lab-results to determine radiation dosage. It is possible that an error in data entry could happen. If the design is changed such that the data is automatically transmitted from the lab to the device, then the potential for this use-related Hazard is eliminated. An example of elimination of the Hazardous Situation by preventing exposure is a safety lancet, where the needle is always protected, when not in use.

Tip A system that is designed to be acceptably safe from a usability standpoint can over time become unsafe due to changes in user behavior. For example, consider a diagnostic system where the clinician is expected to examine the device output for reasonableness. If the device performs reliably and accurately, it will gain the trust of the clinician to a point where the clinicians become complacent and stop checking the output of the device.

9.8.2 Data Gathering

If the medical device is based on an existing released product, for which Post-Production data is available, derive probability of occurrence of Hazardous Situations due to Use Errors from the available data. Use this probability in conjunction with P2 data to estimate the risks due to Use Errors.

If the medical product is new, or the part of User Interface that is under analysis is new, or if Post-Production data of sufficient quality is unavailable, then plan and execute formative and summative studies to generate the necessary data to support the P1 estimates. Compute the risks of Use Errors based on the P1 data.

9.8.3 Risk Reduction and Compliance with IEC 62366 Process

An inverse relationship can be presumed between the rigors of design process and the likelihood of occurrence of Use Errors. The more rigorous, and well-thought-out the process, the less likely it is for the product design to evoke a Use Error. In this third option, the manufacture can follow the Standard IEC 62366 [19] as a means to reduce Use Errors to the degree possible.

Absent a value for P1, risk of Use-Errors cannot be estimated. If Use-Error risks are not estimated, they cannot be included in the Overall Residual Risk computations.

CHAPTER 10

Biocompatibility and Risk Management

Abstract

The International Standard ISO 10993-1 is intended for the protection of humans from potential biological risks from the use of medical devices. It describes the process for biological evaluation of medical devices within the framework of a risk management process. ISO 10993-1 describes biological evaluation of medical devices as a design verification activity in the broader context of risk management, which is governed by ISO 14971.

Keywords: Biocompatibility; biological testing; ISO 10993; biological hazards; toxicity; exposure

The International Standard ISO 10993-1 [20] is intended for the protection of humans from potential biological risks from the use of medical devices. It describes the process for biological evaluation of medical devices within the framework of a risk management process.

Annex B of the Standard [20], describes biological evaluation of medical devices as a design verification activity in the broader context of risk management, which is governed by ISO 14971 [1]. Annex B includes guidance on the application of ISO 14971 [1] to the conduct of biological evaluation.

Sections B.2 and B.3 of Annex B of ISO 10993-1 [20] "describe a continuous process by which a manufacturer can identify the biological hazards associated with medical devices, estimate and evaluate the risks, control these risks, and monitor the effectiveness of the control."

In general, manufacturers aim to use existing materials that are proven to be acceptably safe for medical use from a biological perspective. However, at times it could be found that existing proven materials are not suitable for the specific medical device at hand.

When selecting a material for a medical device which would come in contact with the patient, particularly for implantable devices, it is important that all Hazards due to the use of the selected materials be identified, and the risks for each Hazard be estimated and evaluated.

Application of ISO 14971 [1] risk management methodology can identify, estimate, and evaluate the risks due to biological hazards and judge their acceptability.

As biological evaluation is a component of medical device risk management activities, it must be planned in advance. This includes literature searches, biological

Safety Risk Management for Medical Devices
DOI: https://doi.org/10.1016/B978-0-323-85755-0.00010-2

evaluations, reviews and approvals of biological evaluations, and documentation of Residual Risks.

In biological evaluations, the safety risk to patient/user is a function of the toxicity of the materials, their route and duration of exposure, and the physical properties of the materials. For example, a rough surface creates a larger exposure area than a smooth surface.

ISO 14971 [1] and ISO 10993 [20] require characterization of medical devices for potential Hazards. This includes the materials themselves, all additives and processing aids, interaction with sterilization processes, and chemical transformation of the materials (e.g., degradation) during use. Also consider the interaction with, or contamination from, the packaging materials. Both direct and indirect tissue contact of medical device materials should be considered.

Factors that can influence the biological safety of medical device materials include:

- Mechanical wear, strain, vibration, and deformation due to use.
- Biomechanical interactions such as abrasion, friction, sticking.
- Biochemical interactions such as with acids, enzymes.
- Heat/cold.
- Radiation.
- Chemicals, such as ethylene oxide used in the course of sterilization.
- Cleaning solutions.

Risk estimation requires two components: (1) the likelihood of exposure to a Hazard, and (2) the probability of sustaining Harm from the Hazardous Situation.

Determination of the likelihood of exposure to a biological Hazard depends on factors including:

a. The bioavailability of toxic materials – how likely is it for the toxin to become present?
b. The potential for exposure.

Determination of the probability of sustaining Harm in the event of exposure depends on factors including:

a. The nature of the toxin.
b. The quantity of the toxin (dose response).
c. The tissue that is exposed (e.g., intact skin, vs. mucous membranes).
d. The duration of exposure.
e. Geometric properties (e.g., particle size, porosity, surface texture).

Much information can be derived from published literature, existing in-house data, or suppliers of materials. Where such information is unavailable, chemical or physical characterization, or biological testing may be required to gather the required data.

Data requirements are less stringent for lower risk applications, e.g., temporary intact skin contact, than for higher-risk applications, e.g., brain implants.

Once the risk has been estimated, it is evaluated against the risk acceptance criteria, which are defined in the Risk Management Plan. For biological risks certain measures can be taken to bring the risks down. For example, replacement of a material that has toxicological risks, with a material that doesn't have toxicological risks creates a design that is inherently safe. Other potential Risk Control measures:

- Reducing exposure time.
- Reducing exposure surface area.
- Use of coatings/materials that reduce adverse biological response.
- Changes to manufacturing processes to reduce/eliminate toxic additives, or manufacturing aids.
- Better cleaning/rinsing processes to remove toxic residues.

Keep in mind that some Risk Control measures may introduce new Hazards, or increased risks elsewhere in the design. In such cases, some retesting may become necessary.

Biological evaluation of medical device materials relies on risk assessment to provide justification for not conducting certain testing. This is valuable from a project cost and schedule perspective, and more importantly from the ethical perspective, in that some animal testing may be avoided.

An important factor to consider is that even if a given material is shown to be sufficiently safe by itself, it cannot be deduced that the same material when used in combination with other materials will still be safe. Therefore the total device in its final form, produced using the final processes, is typically subject to biological testing.

As described in Chapter 25, data from Production and Post-Production must be monitored for any occurrences of adverse effects, including due to biocompatibility. Such learnings must be used to update the Risk Management File as necessary.

CHAPTER 11

Influence of Security on Safety

Abstract

Medical devices are becoming progressively more connected to other healthcare systems, and the cybersecurity attack surfaces are becoming larger. Security exploits can be used to harm patients in many ways. The safety impact of cybersecurity exploits must be considered in the overall residual safety risk of medical devices.

Keywords: Cybersecurity; exploits; safety; security threat

Medical devices are becoming progressively more connected to other healthcare systems, and cybersecurity attack surfaces are becoming larger. Security exploits can be used to Harm patients in many ways. Because this book is focused on the safety risks of medical devices, we will stay focused on the impact of security on the safety risks of medical devices. Cybersecurity is a larger topic than what is covered here.

Security risk analysis is a parallel and related process to safety risk management. With respect to safety, security is another potential cause of Hazards. The types of security-related Hazards include:

- Unavailability – a security attack may cause the medical device to become unavailable. In some cases, e.g., life supporting medical devices, this would create a Hazard.
- Change of programming, or code – a security attack could alter the code, or programming parameters of a medical device, thus altering its behavior, or performance.

As seen in Fig. 10, there is an inverse direction of impact, when safety and security aspects are compared. In the domain of safety, humans are potentially harmed by Hazards from the medical devices. For security, the medical device is the potential target of Harm by intended, or accidental attacks carried out by humans. The security of a medical device might impact its safety, and loop back to Harm the humans.

Security threats can be divided into three groups:

Group 1: Intentional – Malicious (aims to Harm)
Group 2: Intentional – Misuse (aims to do good, e.g., get around a cumbersome UI)
Group 3: Unintentional – Use Error

DOI: https://doi.org/10.1016/B978-0-323-85755-0.00011-4

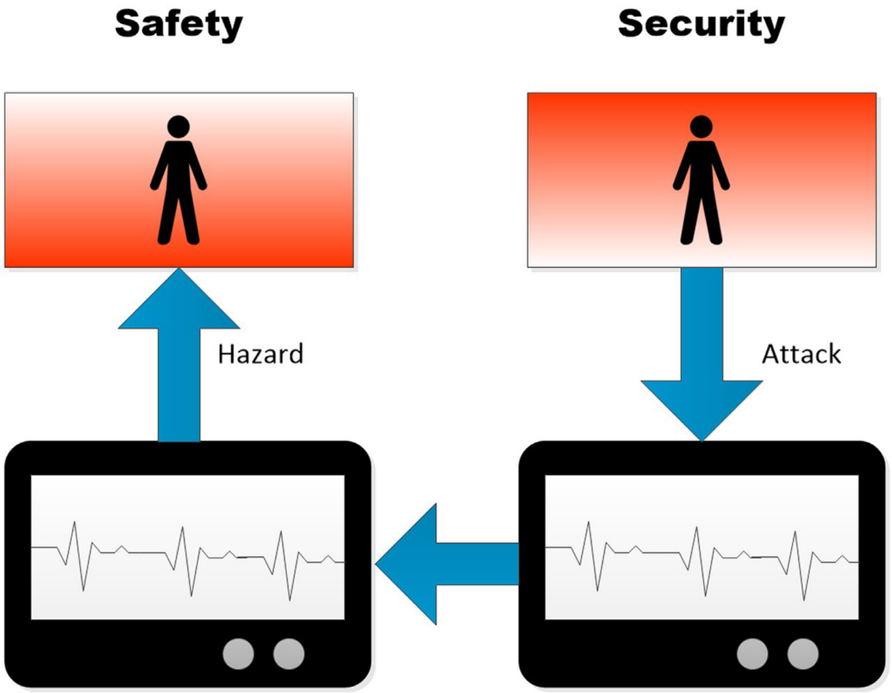


Figure 10 Safety and Security Relationship.

Traditionally, malicious actions are excluded from safety Risk Analysis, i.e., the Hazard of someone using a medical device as a weapon is not included in safety Risk Analysis. However, because malice is a normal and expected part of security risk threats, we include group 1 above in the safety risk impact assessment.

Group 2 is a valid input from Security Risk Analysis that should be captured in the Causes/Mechanisms of Failure in the UMFMEA. In this case, the security threat can potentially damage a function of the System, which may then have a safety impact.

Group 3 is already covered under UMFMEA.

Risk management involves the identification of Hazards, and the estimation of risks due to those Hazards. Risk Estimation requires knowledge of the probability of occurrence of Hazardous Situations. In the case of security-related Hazards, estimation of the probability of an exploit is very difficult. Conventional wisdom suggests using motivation as an indicator of the likelihood of an attack. But experience has shown that motivation plays a smaller role than people think. For many attackers, the challenge of a break-in and the thrill of the exploit is enough reward.

It's important to consider that while security threats can have an adverse safety impact, the security Risk Controls themselves could create safety Hazards. Estimating the probability of occurrence of a Hazard from a security Risk Control is as difficult as estimating the probability of occurrence of a software failure.

The FDA has released a guidance titled: Postmarket Management of Cybersecurity in Medical Devices [28]. In this guidance, the FDA states that "estimating the probability of a cybersecurity exploit is very difficult due to factors such as complexity of exploitation, availability of exploits, and exploit toolkits." The guidance [28] suggests that in the absence of probability data, to use a "reasonable worst-case estimate" and set the value of probability of occurrence of the Hazardous Situation to 1. Alternatively, the FDA suggests that manufacturers instead use a "cybersecurity vulnerability assessment tool, or similar scoring system for rating vulnerabilities and determining the need for, and urgency of the response."

To handle safety-risks from security exploits, estimate the vulnerabilities of the medical device to security threats, using means such as a cybersecurity vulnerability assessment tool. With that knowledge, assuming the exploit has happened, estimate the worst-case Hazard from the exploit. Further, assume the probability of exposure to the Hazard is 100%, and identify the potential Harms. To determine the acceptability of security-related safety risks, in the absence of quantifiable data, Ref. [28] suggests using a qualitative matrix that combines exploitability vs. Harm Severity. Fig. 11 is from Ref. [28], which can be used as a model. It indicates a fuzzy boundary between controlled and uncontrolled risks. The specific construct of the matrix for different applications is left up to the manufacturer.

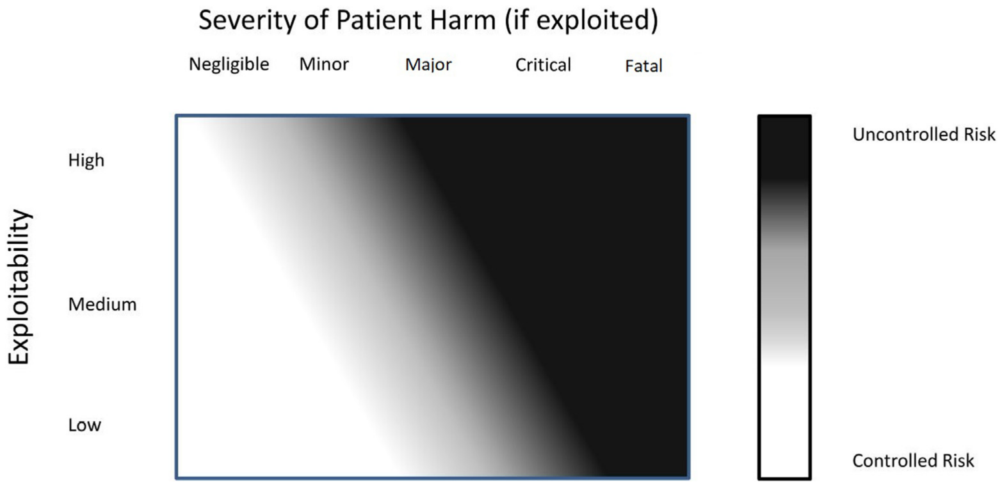


Figure 11 Exploitability vs. Harm Severity.

If you use a single value for Harm severities, plot the security threat's exploitability vs. Harm Severity in the matrix. In the BXM method, five probability values are given for each Harm in the HAL, one for each Severity class. Choose the Severity with the highest likelihood, and similarly plot the security threat's exploitability vs. Harm severities.

Triage the security threats based on the matrix, from the most critical to the least critical, and address them in the order of urgency using the best available methods and tools. This way the security-related safety risks are reduced as far as possible.

Next, analyze the safety risk potential from the security Risk Controls themselves. Reduce the safety risks due to the security Risk Controls as far as possible.

While it is difficult to predict the probability of a cybersecurity exploit, it may be possible to estimate the probability of Hazards due to the security Risk Controls, because they are implemented under the manufacturer's control. For example, if an encryption algorithm is used to protect certain data, it may be possible to estimate the probability of an error in the encryption/decryption process.

By this point, safety risks due to cybersecurity threats are reduced as far as possible. If the overall risk of the product is found to be acceptable, and the product is released, Post-Market risk management processes should be used to maintain and update the Risk Management File with respect to security threats in the same manner as other safety risks.

CHAPTER 12

The BXM Method

Abstract

The methodology presented in this book is called BXM. The BXM method is a quantitative, simple, efficient, and explainable method of risk management that is compliant with ISO 14971. The basic premise of the BXM method is to objectively assess residual risks. The efficiency of the BXM method is achieved via the reuse of existing work, and via the ability to use parallel work streams to optimize labor and skills usage. The characteristics of the BXM method, and its quantitative nature lends itself to computer automation, which saves on the labor of performing risk management.

Keywords: BXM method; decomposition; integration; quantitative risk estimation; computer automation; automation; explainability; efficiency

The methodology presented in this book is called BXM. The BXM method is compliant with ISO 14971 [1], and is designed to provide benefits to the manufacturer, the patient, and the regulator. The characteristics of the BXM method are listed below.

1. **Simplicity** – Application of the BXM method is easy to understand and execute. The BXM process-map offers a clear flowchart of decisions and actions. The analyst can always tell where in the process he/she is, what work has been completed, and what work remains.
2. **Efficiency** – The basic premise of the BXM method is to decompose the System; do Risk Analysis on the constituent parts of the System; and then integrate the underlying analyses into the System-level analysis. This technique allows parallel work streams where different teams can be simultaneously analyzing the different System components. It also allows more efficient use of workers' times. For example, during analysis of a mechanical component of the System, electrical engineers would not be required to attend, as they would not add significant value to that analysis.

   The decomposition and integration strategy also allows modularity and reuse. If a particular component is used in multiple Systems, or even different generations of the same System, the analysis of that component can be reused.
3. **Accuracy** – Decomposition of complex System designs into several simpler parts supports ease of understanding and reduces the probability of errors of omission or commission.

DOI: https://doi.org/10.1016/B978-0-323-85755-0.00012-6

4. **Scalability** – ISO 14971 [1] requires management of the risks of medical devices and doesn't stipulate the use of any specific tool or method. As such, it is possible to scale the BXM method to match the complexity of the medical device at hand. For example, the Risk Analysis, estimation, evaluation, and controls for a bandage could be all contained in a RACT, whereas for a complex surgical robot, all the tools, techniques, and work-products that are identified in the BXM method would be deployed.
5. **Explainability** – The BXM method is simple, cohesive and logical, and easy to explain. A regulatory reviewer would more easily understand the process and have fewer questions. The product development team also benefits from this attribute of the BXM method in smoother on-boarding of new team members, and less confusion during technical reviews.

In the following sections the BXM method is elaborated.

12.1 SYSTEM DECOMPOSITION

Let's say that at the top-level the System is called Level-1 (L1). In the example in Fig. 12 the L1 System is decomposed into two Level-2 (L2) components. Each L2 component is further decomposed into multiple L3 components and so on. This decomposition follows the System architecture.

The criteria for decomposition and how far to go are the novelty of the System, and the degree of reusability that you want. For novel Systems, decompose the system more. If a component is reused in other Systems, then decompose to a level where

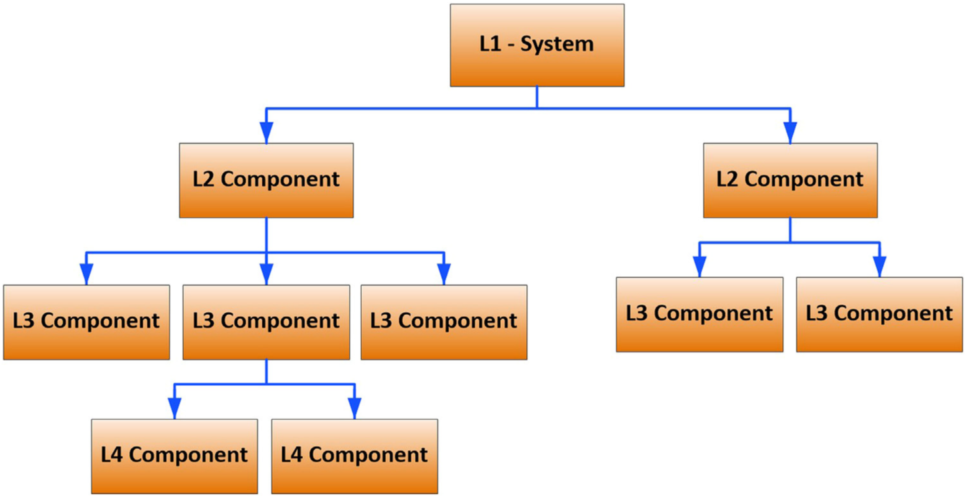


Figure 12 System Decomposition.

the reusable component gets analyzed. That way, its analysis would become available for reuse elsewhere. To elucidate, two examples are offered.

Example 1 – We are analyzing an automobile for safety. The fuel system in this automobile has been in use in multiple models and there is a lot of performance data available on it. As we decompose the automobile, when it comes to the fuel system, we do not further decompose it, because of the knowledge and history that is available on it.

Example 2 – Let's say an automobile manufacturer uses the same brake caliper in a brake system which is in use in three different automobile models. The brake system is well understood and has a history of use in the field. So, ordinarily we would not need to decompose the brake system further. But, we are going to design a new brake system which will use the same caliper. We don't already have an analysis for the caliper. We want to reuse the analysis of the brake caliper in the future brake system. So, in this case we would decompose the brake system down to the level of the caliper.

12.2 INTEGRATION

Integration is the corollary and complementary concept to decomposition, which was described in Section 12.1. The principal concept in integration strategy is the hierarchical multi-level Failure Modes and Effects Analysis (FMEA). See Sections 14.4.2 and 16.1 for details of this mechanism.

The BXM methodology uses the architectural design of the System as a roadmap and looks for the Failure Modes of each architectural element. A critical principle in this method is the strict adherence to the scope, and boundary of analysis within the FMEAs. This principle allows the performance of an FMEA of a given component agnostic of the System in which it is used. That is, the FMEA needs to only concern itself with identifying the End Effects at the boundary of analysis. A great benefit of this principle is that the analyses of the architectural components can be integrated in the same way that the physical components are integrated per the System architecture.

12.3 QUANTITATIVE RISK ESTIMATION

Another attribute of the BXM method is the quantitative estimation of risk. See Section 17.3 for details. Quantitative estimation of risk enables a simple way of evaluating the acceptability of Residual Risks. It boils down to a simple comparison of two numbers: the Residual Risk, and the acceptable risk level. The BXM method uses

Boolean algebra to compute the Residual Risk of a System: both individually and overall.

Thanks to its mathematical approach, the BXM method lends itself to implementation in software tools. The benefits of use of a software tool in risk management are:

1. Objective and automatic determination of risk acceptability
2. Avoidance of error-prone manual computation/assessment of risk
3. Ability to always have an up-to-date risk assessment
4. Ability to evaluate the safety impact of proposed design changes
5. Ability to reuse estimations of Harm probabilities across multiple projects
6. Ability to compute the Overall Residual Risks of the System (medical device)

CHAPTER 13

Risk Management Process

Abstract

ISO 14971 requires the manufacturer to have a documented process for risk management, and provide the specifications for such a process. However, the Standard does not provide a process — that is left up to the manufacturer. In this chapter a compliant risk management process is presented and expounded. Management responsibilities are laid out, including the responsibility for creating a policy for establishing the risk acceptance criteria. Two key tools of the BXM process: Clinical Hazards List and Harms Assessment List are discussed.

Keywords: Risk Management Process; management responsibilities; risk management file; risk management plan; criteria for risk acceptability; clinical hazards list; harms assessment list

ISO 14971 [1] requires the manufacturers to have a documented process for risk management and provide the specifications for such a process. The Standard [1] provides a framework for such a process, but does not provide a specific process — that is left up to the manufacturer.

The BXM method uses a process that is depicted in Fig. 13. In broad terms, it includes Hazard identification, Risk Estimation, Risk Control, Risk Evaluation, and monitoring Production and Post-Production information.

This process is applicable for:

- each new device, or derivative device
- new Indications for an existing device
- each change (in a part) of a released device
- each change (in a part) of a realization process of a released device, including changes to suppliers/manufacturing sites
- discovery of mislabeled or non-conforming product
- CAPA events with potential risk to patient safety

The process starts with formation of the Risk Management File (see Section 13.2), and writing a Risk Management Plan (see Section 13.3). It would be beneficial to determine the safe-state(s) of your medical device, if any. This would help both in the design and in the risk management decisions. Next, a Preliminary Hazard Analysis is done (see Section 14.3). Thereafter, the project transitions to the design and development phase.

DOI: https://doi.org/10.1016/B978-0-323-85755-0.00013-8

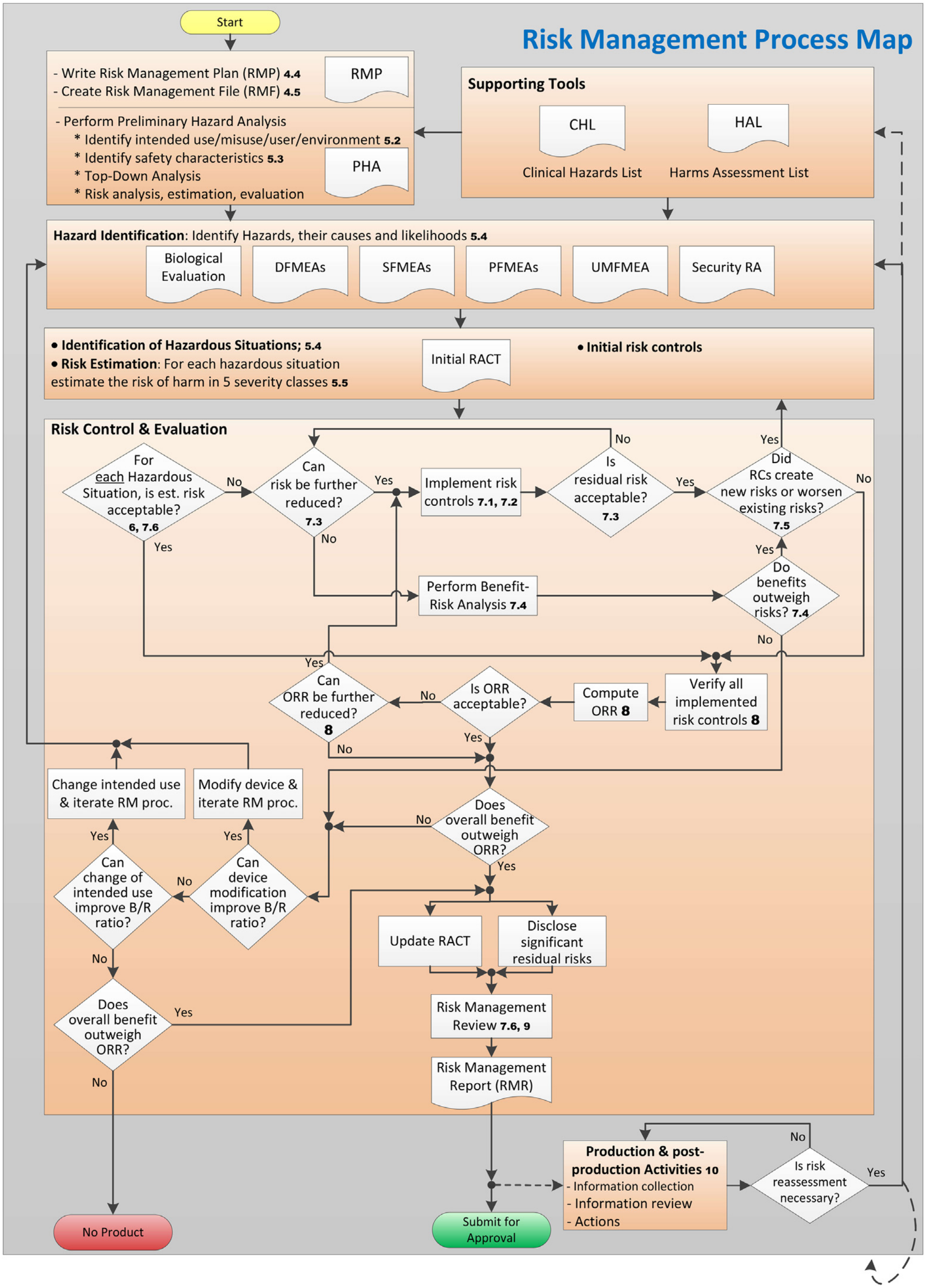

Risk Management Process Map
Start
- Write Risk Management Plan (RMP) 4.4
- Create Risk Management File (RMF) 4.5
RMP
- Perform Preliminary Hazard Analysis
* Identify intended use/misuse/user/environment 5.2
* Identify safety characteristics 5.3
* Top-Down Analysis
* Risk analysis, estimation, evaluation
PHA
Supporting Tools
CHL
HAL
Clinical Hazards List
Harms Assessment List
Hazard Identification: Identify Hazards, their causes and likelihoods 5.4
Biological Evaluation
DFMEAs
SFMEAs
PFMEAs
UMFMEA
Security RA
• Identification of Hazardous Situations; 5.4
• Risk Estimation: For each hazardous situation estimate the risk of harm in 5 severity classes 5.5
Initial RACT
• Initial risk controls
Risk Control & Evaluation
For each Hazardous Situation, is est. risk acceptable? 6, 7.6
No
Yes
Can risk be further reduced? 7.3
Yes
No
Implement risk controls 7.1, 7.2
Is residual risk acceptable? 7.3
No
Yes
Did RCs create new risks or worsen existing risks? 7.5
Yes
No
Yes
Do benefits outweigh risks? 7.4
No
Perform Benefit-Risk Analysis 7.4
Yes
Can ORR be further reduced? 8
No
No
Is ORR acceptable?
Yes
Compute ORR 8
Verify all implemented risk controls 8
Change intended use & iterate RM proc.
Modify device & iterate RM proc.
Yes
Yes
Can change of intended use improve B/R ratio?
No
Can device modification improve B/R ratio?
No
Does overall benefit outweigh ORR?
No
Yes
Update RACT
Disclose significant residual risks
No
Does overall benefit outweigh ORR?
Yes
No
Risk Management Review 7.6, 9
Risk Management Report (RMR)
No Product
Submit for Approval
Production & post-production Activities 10
- Information collection
- Information review
- Actions
No
Is risk reassessment necessary?
Yes

Figure 13 The BXM Risk Management Process.

As designs become available Failure Modes and Effects Analyses are performed and iterated throughout the design and development phase (see Section 14.4). Additional activities, if relevant, are Security Risk Assessment and Biological Evaluation of the device for identification of hazards of the system. These activities, together with FTA, constitute the Hazard identification phase.

Next, the Risk Estimation phase is entered (see Chapter 17). This is where all the Hazards and their causes, the corresponding Hazardous Situations and Harms are brought together in one table called the RACT. The RACT is the heart of the BXM risk management process. In any ISO 14971 compliant risk-management process something like the RACT is found. It may be called by other names, e.g., Risk Table, Risk Matrix, Risk Analysis Chart, etc. At this point individual risks can be estimated and if not acceptable, additional Risk Controls applied to bring them down to acceptable levels. If further reduction of individual risks is not possible, then Benefit-Risk analyses are done on the individual risks. After all individual risks have been managed, the Overall Residual Risk is assessed and compared against the potential Benefits of the device.

If the Benefits do not outweigh the Overall Residual Risks and no further risk reduction is possible, then the manufacturer can either modify the device, or the Intended Use of the device in an attempt to balance the risks and Benefits. If that is not successful, the device may not be released for commercial purposes.

If the Benefits do outweigh the Overall Residual Risk, then the RACT is updated with any additional Risk Controls that were put in place since the initial RACT was produced, and the significant Residual Risks are disclosed.

Subsequently, a risk management review is performed to ensure the Risk Management Plan was faithfully executed and that the Benefits of the device outweigh its risks. A Risk Management Report is generated and submitted for Regulatory approval.

If the Risk Management File for a similar medical device is available, relevant, and adequate, it can and should be applied to the analysis of the subject medical device.

After the product is released Production and Post-Production monitoring continues for as long as the product is in the field. Input such as complaints, surveys, Post-Market Clinical Follow-ups, and even changes to the Standard ISO 14971 [1] itself are considered. If any change or finding warrants revising of the risk management work-products, the required changes are made and the results are reflected in the RMF and RMR. See Chapter 25 for more details on this topic.

ISO 14971 [1] does not specify the periodicity of Production and Post-Production data review. The manufacturer gets to specify that in the PMS Plan. But the choice by the manufacturer must be defensible. A reasonable approach would be to choose the period based on the device risk and novelty. For example, if a device is high-risk and novel, it makes sense to review its RMF more frequently immediately after launch, e.g., twice per year. Then as more knowledge is gained about the device, reduce the frequency to once a year or once every 2 years. For devices that are just iterations on an existing device, about which much knowledge exists, you can start with a lower frequency. In any case, if an adverse event happens in the field, or changes are made to the design or Indications of the device, the RMF must be examined for potential impact.

13.1 MANAGEMENT RESPONSIBILITIES

ISO 14971 [1] Section 4.2 defines specific responsibilities for Top Management. Top Management is required to provide evidence of its commitment to the risk management process by:

- establishing a suitable risk management process
- ensuring the provision of adequate resources (personnel, tools, facilities, time, money, consultants, etc.)
- ensuring the assignment of competent personnel for risk management

Other responsibilities of Top Management are:

- define and document the policy for determining criteria for risk acceptability (see Section 13.3.1 for further details)
- review the suitability of the risk management process at planned intervals to ensure continuing effectiveness of the risk management process. For example, a review of the performance of released products for safety-related issues within the first few months after release could be an indicator of the effectiveness of the risk management process. Any decisions and actions taken during the reviews should be documented. If you have a Quality Management System in place, e.g., one that is compliant with EN ISO 13485 [23], the risk management process review can be part of the regular management reviews of the QMS.

‘Top Management’ is defined in the Standard [1] as person or group of people who directs and controls a manufacturer at the highest level. This could mean different things in different companies. For example, in a small company Top Management could be the general manager. But that would not be the case in a large multinational company. The best way to discern what ‘Top Management’ means for your company is to consider the governing QMS. The person(s) at the level where Risk and Quality policy decisions are made, as well as those who can assign resources, priorities, and responsibilities can be considered 'Top Management.' Therefore, for a company with multiple business units that have different QMSs, 'Top Management' could be the business unit board members, e.g., manager of R&D, Manager of Quality, and the general manager.

13.1.1 Policy for Establishing Risk Acceptance Criteria

ISO 14971 [1] requires Top Management to create the policy for establishing risk acceptance criteria. The policy doesn't establish the risk acceptance criteria; it provides a framework to guide the teams to establish the risk acceptance criteria for their projects. The policy should cover both individual, and Overall Residual Risk acceptance criteria, and also situations where the risk of Harm cannot be estimated.

The policy is at a higher level than the procedure. It doesn't need to be part of the RMF. But it has to be part of the QMS. The policy would guide the establishment of the risk acceptance criteria, which may be the same, or different among various products.

The construct of the policy can have the following elements:

- Purpose and scope
- Factors to consider, e.g.,
  - Relevant harmonized standards
  - Relevant international/national standards
  - Specific regional regulatory requirements
  - State of the Art
  - Stakeholder concerns
- Approaches to Risk Control
  - As Low As Reasonably Practicable (ALARP)
  - As Low As Reasonably Achievable (ALARA)
  - As Far As Possible (AFAP) without adversely affecting the Benefit-Risk ratio
- The requirements for review and approval of the policy, and the risk acceptance criteria

See ISO/TR 24971 [15] Section C.2 for more details.

A method for the determination of when AFAP has been achieved is not offered in EU MDR [2] or IVDR [22].

Note that stakeholder concerns can have both a positive or a negative effect on risk acceptance criteria. For example, political, social, or psychological factors may demand more safety. Conversely, stakeholder concerns may lead to the acceptance of higher risks. For example, many people are concerned about manufacturing sustainability and carbon footprint of medical devices. This led the manufacturer of a disposable medical device to create a new, reusable version of the same product. Although the new design has a smaller carbon footprint and is more sustainable, the reuse presents increased safety risks as compared to the single-use version of the same device.

Annex C.2 of ISO/TR 24971 [15] provides a suggested structure and example language for a policy for establishing risk acceptance criteria.

13.2 RISK MANAGEMENT FILE

One of the earliest actions in the risk management process is the creation of a Risk Management File (RMF). The RMF is a repository of the risk management artifacts. The purpose of the RMF is to enable easy and prompt access to the risk management artifacts. The RMF can take any form that supports its purpose. For example, the RMF could be in paper form, in folders and cabinets, or it can be in electronic form as a collection of files in a computer. It can even be an index to files that are in different locations.

The RMF should have a keeper – a person who is responsible for its upkeep and maintenance. This is particularly important after product development is concluded and the product is released. This is because risk management is a living process which continues for as long as the product is in the market. Therefore, the risk management artifacts are periodically updated and need to be properly filed in the RMF.

The Standard [1] does not prescribe a list of items that must be in the RMF. But the following is a conceivable list of items that could be found in an RMF:

- Risk Management Plan
- Top-Down analyses, e.g., Fault Tree Analysis
- PHA
- DFMEAs
- SFMEAs
- PFMEAs
- UMFMEA
- Risk Assessment and Control Table (RACT)
- Risk Management Report(s)
- Records of reviews and approvals of risk management artefacts
- CHL
- HAL
- Benefit-Risk analyses

- Verifications of Risk Controls
- Log of Production and Post-Production activities
- PSUR
- PMSR
- SSCP
- FSN

13.3 RISK MANAGEMENT PLAN

ISO 14971 [1] requires that a Risk Management Plan (RMP) be created at the beginning of the risk management process. The RMP should include the following elements:

1. Purpose and scope
   a. Scope should identify what phases of product development process are addressed in the plan. It is possible to initially write a plan for the early phases of the product development process, and later update the RMP to include the remaining phases.
2. Overview of the System
   a. Describe the System, its function, its elements, Indications, Intended Use, user, and use environment.
   b. Identify the scope of analysis – specifically what is included or excluded. It's a common mistake to exceed the scope of analysis and include peripheral devices that are not part of the System under analysis.
3. State your risk management strategy
   a. What is your main strategy to manage the risks of your System?
   Examples:
      i. For a therapy-advisory System, you may choose to keep the physician in the decision-making loop.
      ii. For a deep brain stimulator, you may require the use of accurate navigation in the brain to avoid causing brain hemorrhage during the implant surgery.
4. List your planned risk management activities. What techniques will you use?
   a. Examples: Preliminary Hazard Analysis, Fault Tree Analysis, Failure Modes and Effects Analysis, Benefit-Risk Analysis, etc.
5. Identify any special tools, such as specialized FTA software, customized software, etc.
6. Identify people/roles who have responsibility for risk management activities, and their authorities. Include who will be responsible for the maintenance of the RMF.

7. Spell out the requirements for review of risk management activities.
    a. At what points in the project will you review the risk management process outputs?
    b. What will be the objective of each review?
    c. Who will be responsible for the reviews?
8. Define the risk acceptance criteria, including when the probability of occurrence of Harm cannot be estimated.
9. Define how the Overall Residual Risk will be evaluated.
10. Describe how Benefit-Risk analyses will be done.
11. Describe the verification activities and deliverables. This includes both verification of implementation of the Risk Controls, and verification of effectiveness of the Risk Controls.
12. Describe how risk management will affect other aspects of product development process such as sample size determination, production acceptance criteria, etc.
13. Describe how Production and Post-Production information will be captured, reviewed, processed, and fed back into the risk management process. This may include a reference to the Post-Market Surveillance Plan.

The above list describes best-practice for an RMP. However, the minimum requirements for the RMP per ISO 14971 [1] are items 1, 2, 6, 7, 8, 9, 11, and 13.

13.3.1 Criteria for Risk Acceptability

As described in Section 13.1.1, ISO 14971 [1] requires that a policy for establishing risk acceptance criteria be defined and documented. The policy could be applied to the entire range of a manufacturer's medical devices, or be specialized for different groupings of the manufacturer's medical devices. Similarly, the policy may be the same for individual and Overall Residual Risks, or be distinct. The manufacturer can take into account the applicable regulatory requirements in the regions where a medical device is to be marketed.

To maintain objectivity, the criteria for risk acceptance should be established before starting the risk assessment and be documented in the RMP.

For some hazards, harmonized or recognized international standards can provide specific safety requirements, and criteria to demonstrate compliance to the standard. The risks of these hazards are deemed acceptable for medical devices which satisfy the requirements and compliance criteria of the standards. The requirements of the standards (such as engineering or analytical processes, specific output limits, warning statements, or design specifications) can be considered Risk Control measures established by the standards writers that are intended to address the risks of specific Hazardous Situations.

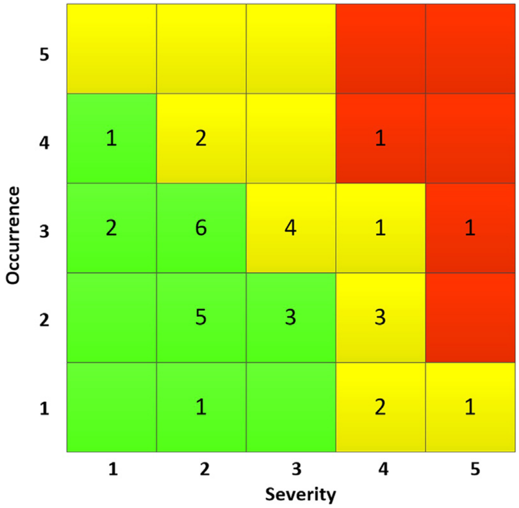
In many cases, the standards writers have performed and completed elements of risk management and provide manufacturers with solutions in the form of design requirements and test methods for establishing conformity. When performing risk management activities, manufacturers can take advantage of the work of the standards writers and need not repeat the analyses leading to the requirements of the standard. International standards, therefore, provide valuable information on risk acceptability that has been validated during a worldwide evaluation process, including multiple rounds of review, commenting, and voting.

In the absence of an applicable harmonized or recognized international standard, depending on where the medical device is going to be marketed, it is also possible to apply a similar strategy which is specific to a geography. That is, it is possible that a particular country has an applicable national product safety standard. Therefore, compliance to that standard would establish acceptability of risk in that country.

Evaluation of Overall Residual Risk comes after the evaluation of the individual risks. Depending on the policy of the manufacturer, the criteria for risk acceptability of Overall Residual Risk may, or may not, be the same as individual risks.

In the BXM quantitative method, the Overall Residual Risk is a computed probability number which is compared against the maximum acceptable probability of Harm to determine acceptability. If quantitative methods are not used, an alternative method is to create a safety risk-profile for the device and compare it against a reference profile.

An example risk profile could look like Fig. 14. The method to create this type of risk profile is as follows.



	1	2	3	4	5
5					
4	1	2		1	
3	2	6	4	1	1
2		5	3	3	
1		1		2	1

Figure 14 Example Risk Profile.

Use a Severity scale, such as Table 27, and a probability scale, such as Table 28. Determine the risk of Harm(s) for every Hazard. If your process uses a single Harm-Severity method, then R describes the probability of occurrence of the Harm in one class of Harm, e.g., Critical (rank 4). For all the Hazards of the System, count the number of risks that fall in each cell of the matrix in Fig. 14. Populate the matrix as in Fig. 14. This would be the risk profile for the device in question. Compare it against the reference profile to determine acceptability. The reference risk profile would be the profile of a comparable approved device on the market. If your device is a first-of-a-kind, you would engage a panel of experts to determine if the risk profile is acceptable when compared to the Benefits of the device. When your device gets regulatory approval, its risk profile would become the reference risk-profile for future products.

Comparison of the risk profile of a new product with a reference risk profile is not so obvious. One way of comparison is to engage a panel of experts to give opinion as to whether the new profile is equal to, or better than the reference profile. A better way is to create an algorithm to objectively compare the new risk profile against the reference risk profile. For example, one possible algorithm is to assign a score to each risk profile which is the sum of the products of the entry in each cell of the matrix by its Severity and occurrence rankings. In other words:

$$\text{Score} = \sum (\mathrm{N} \times \mathrm{S} \times \mathrm{O}) \ \text{ for all cells}$$

where:

N = the entry in the cell

S = the Severity ranking for that cell

O = the occurrence ranking for that cell

A lower score would be better than a higher score. This is an extremely simple algorithm. Consider using a more sophisticated algorithm.

Another approach could be a policy statement such as: no red-zone risks, and no more than 1/3 of the risk could be in the yellow zone.

13.3.2 Other Considerations for Risk Reduction End-Point

Bordwin in Ref. [29] states “The law books are filled with cases alleging defective design of equipment that plaintiffs claim caused injury or death.” “A product is defective when . . .it is defective in design . . . A product is defective in design when the foreseeable risks of Harm posed by the product could have been reduced or avoided by the adoption of a reasonable alternative design by the seller. . .”

It is very likely for most medical device companies to face legal challenges at some point and have to defend themselves in liability lawsuits. As quoted above, in such lawsuits the assertion would be that the manufacturer did not take reasonable measures to reduce the risk of Harm from the device. Having a rational, defensible, and documented methodology to determine risk-reduction end-point, would be very valuable in the legal defense in such lawsuits. In particular, safety of the product must not be traded off against business perspectives.

13.4 HAZARD IDENTIFICATION

The manufacturer is expected to identify all risks due to the use of the medical device. This requires knowledge of all the Hazards associated with the use of the device. While it is difficult to claim completeness, the use of a standardized Clinical Hazards List (CHL) enables you to claim that you are as complete as possible. See Section 13.5 for further details on the CHL and how to create it.

The Hazard identification phase also entails identifying the Causes of the Hazards and the likelihood of occurrence of the Hazards. This is facilitated by the use of the technique of Failure Modes and Effects Analysis. See Section 14.4 for details on FMEAs.

A major source of Hazards is the interoperability of interfacing parts. Most medical devices are comprised of parts that connect and interoperate with each other. These include mechanical, electrical, and informational interfaces. Additionally, you should consider interfaces with the outside world.

An important, and sometimes missed aspect of medical device Risk Analysis is the packaging. Packaging must protect the medical device in handling, transportation, and storage. For sterile products, the packaging also has the duty of maintaining sterility of the product. Packaging also has the role of protecting people, property, and the environment from the device.

In addition to the Hazards that could directly Harm patients, also consider Hazards that could indirectly Harm patients. An example of indirect Hazard is the informational type. For instance, if a diagnostic device produces a false negative result, it could mislead the clinician into not delivering the needed therapy to the patient.

13.5 CLINICAL HAZARDS LIST

Identification of hazards is a cognitive process that requires not only a thorough understanding of the System operation, but also user interaction, peripheral equipment, and the environment. A Clinical Hazards List (CHL) is a complete list of all the known and foreseeable Hazards that could potentially arise from the use of a medical device. A claim of completeness is special and noteworthy. This claim can be made by the mechanism with which the CHL is created and kept up-to-date.

A good place to start for identifying the Hazards associated with the medical device is Table C.1 of ISO 14971 [1]. Use this table as a thought stimulator. Likely you will find that many of the Hazards are irrelevant to your device, but on the other hand it might bring to your attention some Hazards that you might have overlooked. Table B.2 of IEC 62366 [19] is another resource that could serve as a thought stimulator for identification of Hazards due to Use Errors. Next, examine other sources. Below, are some suggestions:

- Literature search of comparable products
- Your internal historical data based on CAPAs, complaint handling database, and repair records
- Adverse-events databases, e.g., MAUDE [30], Eudamed [31]
- See Appendix D, for links to additional adverse events databases
- Input from subject matter experts

After you have compiled the list of Hazards, review it for duplications, and erroneous entries. It is common that people enter items in the CHL that are not Hazards. A common mistake is to enter Causes, Hazardous Situations, or Harms in the list. Use this test to distinguish true Hazards: 'If someone was exposed to this item, could they potentially be harmed?'

Examples of CHL entries that are not Hazards:

- Missing labeling
- Software
- Bleeding

After the first pass of cleanup, route the list for review to subject matter experts. For example, clinicians, clinical investigators, or R&D engineers who have experience with similar devices. After the second round of reviews, the list should be ready for approval and use in your risk management process.

For readability, you may want to group the hazards in categories, e.g., Electrical Hazards, Chemical Hazards, and Biological Hazards.

You may find that some Hazards may need to be stratified. For example, exposure to hot surfaces at 80°C, 150°C, and 250°C could have dramatically different harms. In such cases the same Hazard (hot surfaces) could be cited n times, each with a different qualification.

The CHL is a living document which is kept up to date. If at any time a new Hazard manifests that was not previously in the CHL, revise and update the CHL. This is how the claim of completeness can be made — that at any given time, the CHL is as complete as possible.

Tip A Hazard doesn't belong in the CHL unless it is connected to a Harm in the HAL.

13.6 EXCEPTIONS TO THE CHL

At times you will encounter items that are not hazards per the definition of a Hazard but have an ultra-high potential for causing Harm. Examples:

- A therapeutic X-ray generator that is out of calibration (with no indication)
- A pinhole in a sterile package
- A surgical stapler with a defective fire mechanism

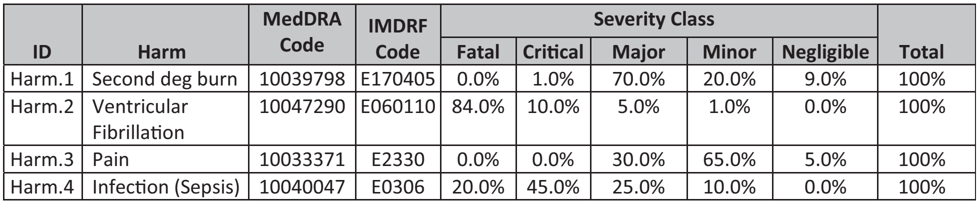
Exposure to a sterile package with a pinhole does not cause Harm. But the content of the package could cause an infection. Holding a stapler with a defective fire mechanism does not cause Harm, but a patient who receives a wrongly placed staple might receive Harm.

Because in these examples the user would not be aware of their high potential for Harm, and thus use the devices, it is almost certain that they would lead into patient Harm. In order to not lose sight of such cases, you can create a section within the CHL for high-potential causes. In practice, these items would appear as End Effects with safety impact in the top-level system FMEAs. You would cite them in the Hazard column of the RACT and treat them as hazards. But the Hazardous Situation would not be exposure to these elements — it would be exposure to the hazards that are created by them, e.g., high-dose X-ray.

13.7 HARMS ASSESSMENT LIST

Another pivotal tool in the BXM method of risk management is the Harms Assessment List (HAL). The HAL is a list of all the potential Harms that could result from the use of the System under analysis. Fig. 15 shows a partial example of a HAL.

NOTE: the data in Fig. 15 is fictitious — do not use for actual analysis.



		MedDRA Code	IMDRF Code	Severity Class					
ID	Harm			Fatal	Critical	Major	Minor	Negligible	Total
Harm.1	Second deg burn	10039798	E170405	0.0%	1.0%	70.0%	20.0%	9.0%	100%
Harm.2	Ventricular Fibrillation	10047290	E060110	84.0%	10.0%	5.0%	1.0%	0.0%	100%
Harm.3	Pain	10033371	E2330	0.0%	0.0%	30.0%	65.0%	5.0%	100%
Harm.4	Infection (Sepsis)	10040047	E0306	20.0%	45.0%	25.0%	10.0%	0.0%	100%

Figure 15 Example HAL.

The HAL provides P2 values, the probability of sustaining Harm in a Hazardous Situation. In other words, it is assumed that the Hazardous Situation has already happened.

The HAL model presented here is inspired by ISO 14971 [1]. Note the following in the construct of the HAL:

- For each Harm five P2 numbers are provided, one for each Severity class. The P2 numbers are inclusive of any subsequent harm. For example, for the citation of the harm: 'infection,' a subsequent harm may be 'organ failure,' which is a Critical injury. The $P2_{Critical}$ number for 'infection' would include the cases where organ failure happened as a result of infection.
- Sometimes no Harm occurs in a Hazardous Situation. In this example, the lowest Severity class: Negligible, includes the 'No Harm' outcomes.
- The totals of all the five P2 numbers adds up to 100%. This means all possibilities are accounted – from nothing to death.
- The Harm outcomes are the aggregate of all potential circumstances, e.g., for Harm.1 in Fig. 15, if some burn victims receive medical care and some don't, the cited P2 numbers for Harm.1 account for both cases of receiving care, and not receiving care.

The creation of a HAL requires foresight and good judgement. Harm outcomes depend on many factors. The same Harm would have different outcomes on different patient populations, under different conditions, etc. For example, consider the Harm of electrocution, meaning injuries due to electric shock. The voltage and current of the source, the impedance of the skin of the person, the location of electrical discharge on the body, are all factors on the Severity of the Harm. The creator of the HAL may choose to create multiple lines for the Harm of electrocution, e.g., electrocution due to:

- Exposure to 100–200 volts
- Exposure to 200–400 volts
- Exposure to 400+ volts
- Exposure to unprotected hand
- Exposure to gloved hand
- Exposure while user is standing in water
- . . .

Application of this strategy to all the Harms could create a very large HAL. Alternatively, all the various circumstances of electrocution could be aggregated into one line – *electrocution*. This option would offer less precision in the determination of the risk of Harm but is more practical with respect to the size of the HAL. A midway method would be to consult KOLs about the most likely levels of Harm for your device, and stratify the Harm only to those most likely levels. Striking the right balance is the art of risk management.

Remember that only a qualified person (e.g., an MD) can assign severities to Harms.

13.7.1 How to Create a HAL

There are two methods by which a HAL can be created:

Method 1 – Using published data
Method 2 – Using expert opinion

Each method is detailed below.

Method 1 – Using Published Scientific Papers

Method 1 is the preferred method because it relies on actual data. Below are the steps to follow for Method 1:

1. Define search criteria, and exclusion criteria for the literature search.
2. Search for published scientific papers, or other formal sources using the search criteria from step 1. There are many databases such as PubMed, or Cochrane® that can be used for this purpose.
3. Filter the results of the search based on the exclusion criteria.
4. Review the remaining papers to ensure appropriateness of the selected papers for your System.
5. From each paper extract the number of observations of the Harms in the HAL in each Severity class of: [Fatal, Critical, Major, Minor, Negligible].
6. Sum the total number of observations per Severity class, per Harm from all the selected papers. This yields the numerators for P2 computations.
7. For each Harm in the HAL sum all the observations in all Severity classes from all the selected papers. This makes the denominator for P2 computations.

Example:

Let's say we have selected 14 published papers that are relevant to the System under analysis. And, let's say the Harm of interest is: Hemorrhage, intracranial.

The total number of reported intracranial hemorrhages in all papers = 79
Total number of deaths from intracranial hemorrhage (Fatal) = 2
Total number of symptomatic, persistent intracranial hemorrhages (Critical) = 15
Total number of symptomatic, treated transient intracranial hemorrhages (Major) = 25
Total number of asymptomatic untreated intracranial hemorrhages (Minor) = 37

In no case the physicians considered an intracranial hemorrhage an inconvenience/discomfort (Negligible).

Therefore,	P2(Fatal)	= 2/79	= 2.5%
	P2(Critical)	= 15/79	= 19.0%
	P2(Major)	= 25/79	= 31.7%
	P2(Minor)	= 37/79	= 46.8%
	P2(Negligible)	= 0/79	= 0.0%
	Total		= 100%

Tip If you have access to registry data, it is a preferred source over published clinical studies. The reason is that in many cases in clinical studies patients are selected who are most likely to benefit from the therapy. Whereas in registries all users of a device are taken into consideration. And the patient population is much larger than those in clinical studies. Therefore, the data is more representative of the 'real world.' Also, in comparison with complaint data, registry data is superior because for registries data is actively sought, while complaint data-gathering is passive and likely subject to under-reporting.

Method 2 – Using Expert Opinion

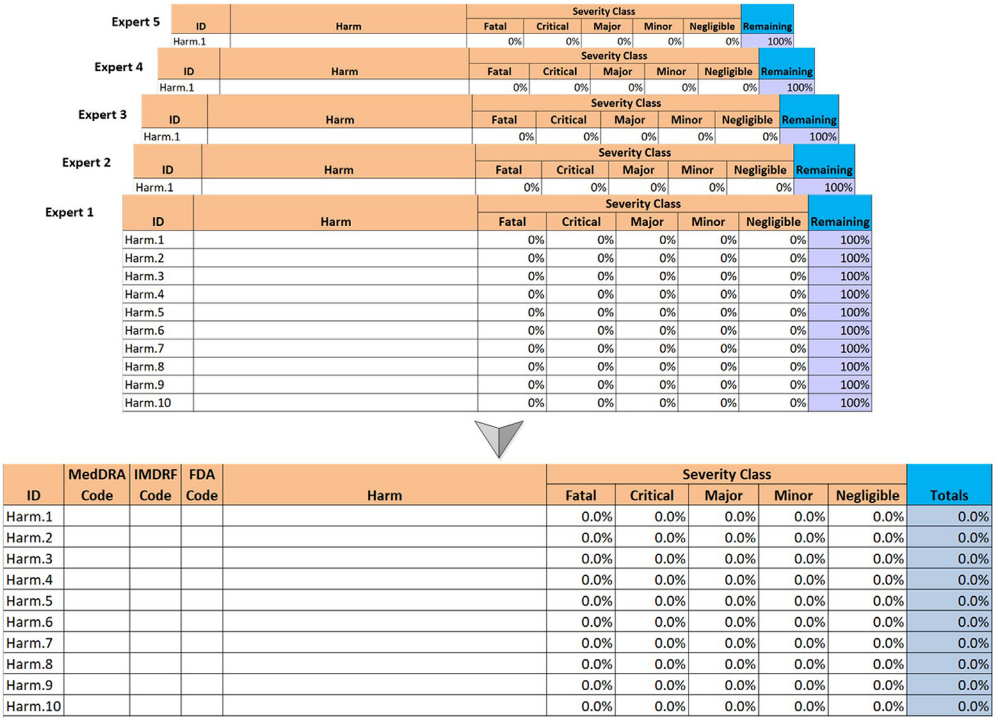
In this method, you seek the opinions of multiple experts and ask them the question: given the Harm has happened, what is the likelihood of:

- Death
- Permanent impairment or irreversible injury
- Injury or impairment that requiring medical or surgical intervention
- Temporary injury or impairment not requiring medical or surgical intervention
- Inconvenience, or temporary discomfort, or no Harm

Ask this question for every Harm that is listed in the HAL. Then aggregate the responses of all the experts into an overall table. Fig. 16 displays a graphical representation of this method.

Method 2 is inferior to Method 1, because it depends on the subjective opinions of the clinicians. The opinion of a clinician is formed by their personal experience with their patients, which is naturally limited. The larger the number of interviewed clinicians, the better the quality of the data in the HAL. The principle behind this technique is cancelation of noise in judgments where there is natural variability.

This concept is over a century old. In the fall of 1906 the British scientist, Sir Francis Galton (cousin of Charles Darwin) went to the Plymouth Country Fair. There were many animals on display. One was a prize-winning large ox. People were given a chance to buy a ticket for 6 pence and guess the weight of the ox. The best guesses would win prizes (Fig. 17).



Expert 5

ID	Harm	Severity Class					Remaining
		Fatal	Critical	Major	Minor	Negligible	
Harm.1		0%	0%	0%	0%	0%	100%

Expert 4

ID	Harm	Severity Class					Remaining
		Fatal	Critical	Major	Minor	Negligible	
Harm.1		0%	0%	0%	0%	0%	100%

Expert 3

ID	Harm	Severity Class					Remaining
		Fatal	Critical	Major	Minor	Negligible	
Harm.1		0%	0%	0%	0%	0%	100%

Expert 2

ID	Harm	Severity Class					Remaining
		Fatal	Critical	Major	Minor	Negligible	
Harm.1		0%	0%	0%	0%	0%	100%

Expert 1

ID	Harm	Severity Class					Remaining
		Fatal	Critical	Major	Minor	Negligible	
Harm.1		0%	0%	0%	0%	0%	100%
Harm.2		0%	0%	0%	0%	0%	100%
Harm.3		0%	0%	0%	0%	0%	100%
Harm.4		0%	0%	0%	0%	0%	100%
Harm.5		0%	0%	0%	0%	0%	100%
Harm.6		0%	0%	0%	0%	0%	100%
Harm.7		0%	0%	0%	0%	0%	100%
Harm.8		0%	0%	0%	0%	0%	100%
Harm.9		0%	0%	0%	0%	0%	100%
Harm.10		0%	0%	0%	0%	0%	100%

ID	MedDRA Code	IMDRF Code	FDA Code	Harm	Severity Class					Totals
					Fatal	Critical	Major	Minor	Negligible	
Harm.1					0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
Harm.2					0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
Harm.3					0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
Harm.4					0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
Harm.5					0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
Harm.6					0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
Harm.7					0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
Harm.8					0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
Harm.9					0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
Harm.10					0.0%	0.0%	0.0%	0.0%	0.0%	0.0%

Figure 16 HAL Creation via Expert Opinion.

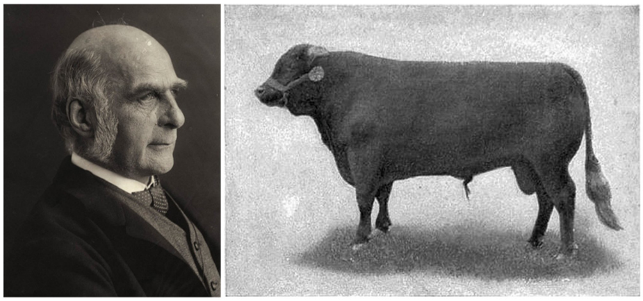


Figure 17 Sir Francis Galton (left) – Ox Weight Estimation.

Galton collected the 878 tickets that were entered in the competition to do some statistical analysis. One of the things that he did was to calculate the average of the guesses. The average of the 878 guesses was 1197 lbs. The actual weight of the ox was 1198 lbs. Colloquially, this is called the wisdom of the crowds. James Surowiecki discusses this topic in detail in his book: The Wisdom of Crowds [32].

Delphi technique – As an extra means of improving the accuracy of the HAL P2 numbers, it is recommended to show the aggregated HAL to the interviewed clinicians, in a second round of interviews. Offer them a chance to revise their first estimates. It may be that they would change their minds on their initial estimates, once they see the aggregate of the collective opinions. If they change their mind on some of their initial estimates, collect the new data and update the HAL with the latest input from the clinicians. Theoretically, you can repeat this process until consensus is achieved. However, in practice, usually only one round of repeat interviews is performed.

CHAPTER 14

Risk Analysis Techniques

Abstract

Identification of hazards for risk analysis can be done using various tools. Two of the most common tools are Fault Tree Analysis (FTA) and Failure Modes and Effects Analysis (FMEA). In this chapter three types of FMEA are discussed: DFMEA, PFMEA, and UMFMEA. Additionally, two other tools are presented: Mind Map Analysis and P-Diagram. Ultimately it is the analyst's choice on how many tools to use. While extra analyses consume more resources, they also reduce the likelihood of missing some Hazards and their causal chains.

Keywords: Fault Tree Analysis; FTA; Failure Modes and Effects Analysis; FMEA; DFMEA; PFMEA; UMFMEA; Mind Map Analysis; P-Diagram

14.1 FAULT TREE ANALYSIS

14.1.1 Introduction

The Fault Tree Analysis (FTA) technique was developed by Bell Labs in 1962 for use on the Minuteman missile system. Later it gained wide use in civil aviation, space, and military applications. MIL-HDBK-338B published in 1998 provides a reference for this technique. After the 1979 incident at Three Mile Island, Pennsylvania, USA, the United States Nuclear Regulatory Commission expanded the use of FTA and published the handbook NUREG-0492 – *Fault Tree Handbook* in 1981. This handbook was later updated by NASA in 2002 with the title *Fault Tree Handbook with Aerospace Applications* [33].

Fault Tree Analysis is a deductive top-down reasoning process that starts from the undesired system outcomes and attempts to find out all the credible sequences of events that could result in the undesired system outcomes. The Fault Tree is a graphical model that depicts the logical relationships among the parallel and sequential combination of events that could lead to the event at the top of the tree.

FTA can model both normal and fault conditions under various environmental and operational scenarios. FTA can also identify and model fault dependencies and Common Cause Failures (CCFs).

Fault Trees (FTs) are constructed using logic gates, such as AND and OR gates. As such, Fault Trees lend themselves to mathematical representation, logical simplification, and reduction. Therefore, there is not just one correct Fault Tree to describe a system, but potentially multiple logically equivalent Fault Trees.

DOI: https://doi.org/10.1016/B978-0-323-85755-0.00014-X

Due to its nature, besides being used for qualitative analysis, the FTA can also be utilized for quantitative analysis, to estimate the probability of occurrence of the top undesired events. It is important to understand that a Fault Tree is not in itself a quantitative model. It is a qualitative model that can be evaluated quantitatively.

The FTA can be applied to new products before design details are available. In this capacity, the FTA can reveal at a high-level, potential event sequences that could result in System Hazards, and thus alert the design teams to safety-critical aspects of the System. When FTA is applied to existing Systems, it can identify design weaknesses and aid in the identification of design upgrades to make the System safer.

A principal output of the FTA is a collection of minimal cut sets to the Top Event. "A cut set is a set of Basic Events, which if they all occur, will result in the Top Event of the fault tree occurring" [33]. A minimal cut set is the smallest set of Basic Events, which if they all occur will result in the occurrence of the Top Event. The term minimal is used to mean that in a given path to the Top Event, if any of the Basic Events do not happen, then the Top Event won't happen. Minimal cut sets can also be identified for intermediate events. If a minimal cut set is shown to be comprised of only one Basic Event, it reveals a vulnerability to a single-point failure.

When probabilities are applied to a Fault Tree, the dominant cut sets can be identified. Those are the pathways with the highest probabilistic contribution to the occurrence of the Top Event. Additionally, the FTA can provide the relative importance of the Basic Events, and the sensitivity of the Top Event to the different Basic Events. With this knowledge, actions and resources can be prioritized to achieve the largest reduction in the likelihood of occurrence of the Top Event.

One of the strengths of the FTA is that unlike the FMEA, for which architectural hierarchy is material and relevant to the analysis, in the FTA hierarchy doesn't matter. The FTA simply looks for the contributors to an event and crosses the hierarchical boundaries. Another strength of the FTA that it is easy to learn, and, due to its graphic nature, easy to understand. FMEA is a bottom-up single-thread analysis technique, but FTA is a top-down multi-thread analysis method.

FTA is not risk management. But at the service of risk management, the FTA is used to find the pathways to Hazardous Situations. Beyond Hazardous Situations, there may be many more Top Events that are of interest to other disciplines, e.g., reliability, service, etc. By its nature, the FTA is a brainstorming technique to identify the events that are on the path to the Hazardous Situation. This means the FTA is limited by the imagination of the analysts. If they don't imagine it, it will not show up in the FTA. That is why it is critical that the FTA analysts be knowledgeable about the system under analysis. The FTA is not exhaustive. The technique is applied to Top Events of interest, i.e., the foreseen Hazardous Situations. Therefore, if we don't foresee a Hazardous Situation, it will be left out of the analysis.

In the FTA the words 'fault,' and 'failure' are meaningful depending on the context in which they are considered. Failures can be the result of faults. But when a fault is viewed in consideration of its underlying contributors, then it can be seen as a failure. The word 'event' is a more general term that can be applied to both faults and failures.

Tip Careful choice of the Top Event is important to the success of the FTA. If it is too general, the analysis become unmanageable; if it is too specific, the analysis does not provide a sufficiently broad view of the system. NUREG-0492 [34].

14.1.2 Theory

A Fault Tree is a graphical representation of parallel and sequential events that are interconnected by logic gates, leading up to a Top Event. The Top Event usually represents an undesired outcome, such as a Hazardous Situation, and the lower events include faults, Use Errors, and normal conditions. An example of a Fault Tree can be seen in Fig. 18. The logic gates show the required relationships among the lower-level events that are needed to cause the output of the gate in question. The event at the top of a gate is called the 'higher' event and is the output of the gate. The events

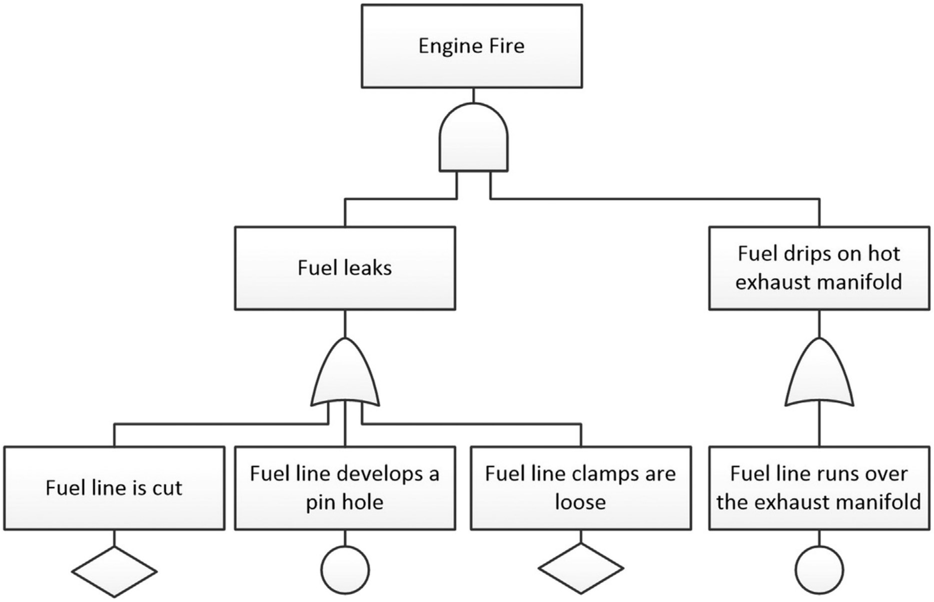

Engine Fire
Fuel leaks
Fuel drips on hot exhaust manifold
Fuel line is cut
Fuel line develops a pin hole
Fuel line clamps are loose
Fuel line runs over the exhaust manifold

Figure 18 Example FTA Diagram.

below a gate are called the 'lower' events and are the inputs to the gate. The lines connecting the gates depict pathways to the top undesirable event.

Due to its logical construct, a Fault Tree can be translated into a set of Boolean equations. As such, the rules of Boolean algebra can be applied to Fault Trees to simplify and reduce them. This simplification is beneficial for the derivation of the minimal cut sets of the tree, and can also simplify the understanding of the relationships of the inputs of the System under analysis, to its outputs.

Analysis of Fault Trees can provide us with:

- minimal cut sets of the tree
- qualitative importance of the system components
- knowledge of cut sets that are susceptible to Common Cause Failures

If probabilities of Basic Events are known, the quantitative analysis can provide:

- probability of occurrence of the Top Event
- quantitative importance of the minimal cut sets and components
- sensitivity evaluations

Sensitivity evaluation shows the sensitivity of the Top Event to the variations in probabilities of occurrence of Basic Events that lead to the Top Event.

14.1.2.1 Primary, Secondary, and Command Faults

Ref. [33] identifies three categories of faults: primary, secondary, and command. It describes them as follows:

- **Primary fault**: "any fault of a component that occurs in an environment for which the component is qualified"; e.g., "a pressure tank, designed to withstand pressures up to and including a pressure P_0, ruptures at some pressure $p \le P_0$ because of a defective weld."
  A primary fault is inherent to the component and occurs under design conditions. A primary fault in one component is presumed to be independent of a primary fault in another component, i.e., a primary fault in component X would not cause a primary fault in component Y.
- **Secondary fault**: "any fault of a component that occurs in an environment for which it has not been qualified. In other words, the component fails in a situation which exceeds the conditions for which it was designed, e.g., a pressure tank, designed to withstand pressure up to and including a pressure P_0, ruptures under a pressure $p > P_0$."
  A secondary fault is due to unforeseen external factors.
- **Command Fault**: "proper operation of a command, but at the wrong time/place."

A command path is a chain of events through the system that culminates in the desired command. In the development of command-faults, identify what sequence of faults led to the command fault. The terminus of this chain would be primary/secondary faults.

14.1.2.2 Immediate, Necessary, and Sufficient

In the development of faults, and identifying the contributing lower level events, consider the following tests. For each lower-level event ask if it is:

Immediate Does the event on the next lower level, immediately precede the event in question?
Benefit: It keeps you from jumping ahead and missing causes. Ref. [33] says "The basic paradigm in constructing a Fault Tree is 'think small,' or more accurately 'think myopically.'"

Necessary Is the event on the next lower level necessary to cause the fault in question?
Benefit: It helps maintain the cause and effect relationship and avoids extraneous entries.

Sufficient Are the identified lower-level events sufficient to cause the fault in question?
Benefit: Ensures the higher event can actually happen, given the cited lower-level events.

For the purposes of risk management, we can presume that the design has already been peer reviewed, analyzed, modeled, and tested. Therefore, faults due to designer errors can be excluded.

14.1.2.3 State of Component – State of System

A fault can be a State of Component, or State of System. Ref. [33] defines "a 'state of component' fault to be a fault that is associated uniquely with one component. A 'state of system' fault is a fault that is not uniquely associated with one component. The immediate cause of a 'state of system' fault involves more than one component."

14.1.2.4 Common Cause Failures

Common Cause Failures (CCFs) describe situations where two or more component failures occur due to a common cause. In the paradigm of immediate-necessary-sufficient logic, common causes of the failures are not explicitly modeled in the Fault Tree. Instead, common causes describe an implicit dependency where multiple faults are triggered when the common cause occurs. Once the CCFs are identified, they should be included in the Fault Tree to raise awareness of their contribution.

Examples of CCF:

- Environmental factors, e.g., temperature, humidity, pressure, vibration
- Faulty calibration
- Error in manufacturing, causing all copies of a product to be faulty
- Erroneous work instruction causing all users to operate the device incorrectly

CCFs are particularly important in redundant systems, where safety is based on the presumption of unlikelihood of simultaneous failure of the redundant systems. In such cases, a single cause would simultaneously defeat all of the redundant systems.

14.1.3 Symbols

Fault trees are constructed from logical connection of nodes. The nodes represent various events such as a Basic Event, an Undeveloped Event, etc. The nodes are connected to each other using logic gates. Special symbols are used to represent different types of nodes and gates. Some of the most common symbols are presented in Fig. 19.

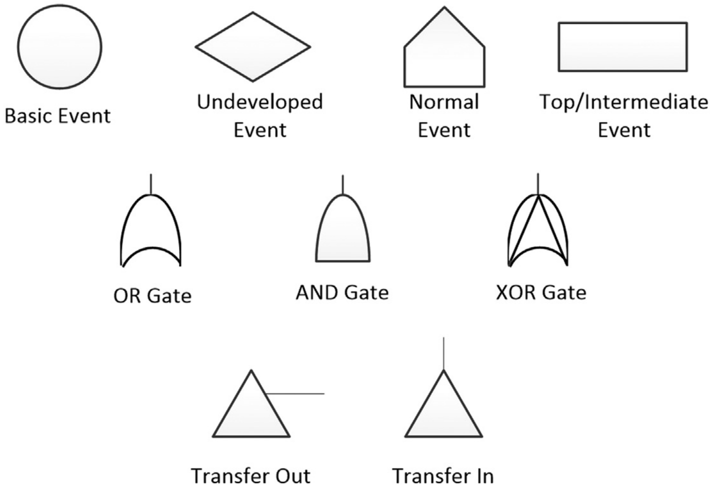


Figure 19 FTA Symbols.

Definitions of FTA symbols:

Basic Event	A basic initiating event, e.g., component faults, requiring no further development
Undeveloped Event	An event that is not further developed due to lack of information, or when the consequences are not important
Normal Event	An event that is normally expected to occur, e.g., the device gets used
Top/Intermediate Event	An event that is further analyzed
OR Gate	Output occurs when one or more of the inputs occur
AND Gate	Output occurs when all of the inputs occur
XOR Gate	Output occurs when only one of the inputs occurs
Transfer	A symbol that shows part of the tree is transferred to another location. Used to manage the size of the tree on a page, and to avoid duplications

For convenience in labeling the events and gates, sometimes the style in Fig. 20 is used, where the descriptive text is entered in the rectangles above the FT symbol.

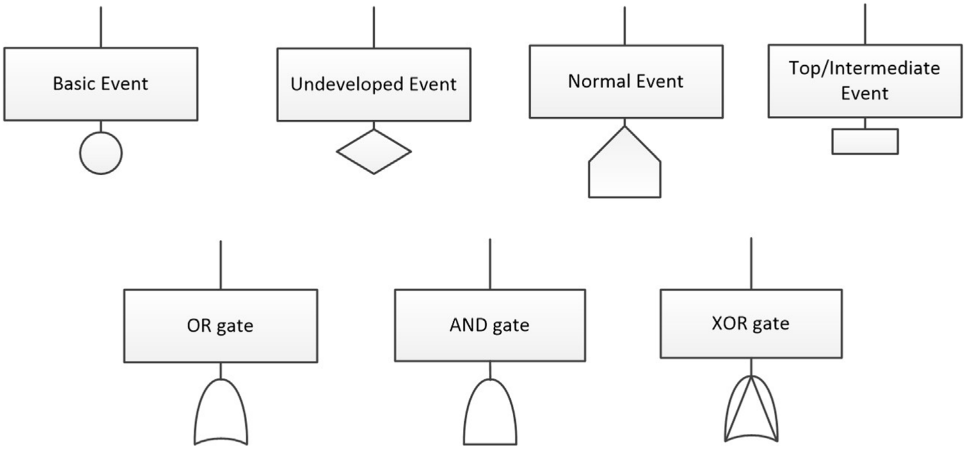


Figure 20 Alternate FTA Symbols.

14.1.4 Methodology

1. Obtain the System requirements and architectural design. Understand the theory of System operation. It is often easier to work from a functional block diagram. If you can't draw a functional block diagram of the system, likely you don't have sufficient understanding of the system to perform a proper FTA.
2. Understand the purpose of the FTA. In risk management, we use FTA to identify the sequences of events that lead to Hazardous Situations, or Harms.
3. Define the boundary of analysis. Know what is in, and what is out. "What is in the analysis will be those contributors and events whose relationship to the top undesired event will be analyzed. What is out of the analysis will be those contributors that are not analyzed" [33]. External interfaces to the boundary of analysis should be included in the analysis as influencers. However, we don't analyze the causes of the behavior of the external influencers. It is also possible to make assumptions about the external influencers. For example, you may assume for a mains-powered device, that mains power frequency will be 60 Hz.
4. Define the Top Events. In risk management these would be Hazardous Situations. You could also use Harms as the Top Events. But in the construct of the BXM method, Harm is presumed in the face of a Hazardous Situation (see Section 4.2).

   The System context, or initial state may need to be specified for the Top Events.
5. For each fault, check to see if it is a state-of-component (SC) fault. If not, it is a state-of-system (SS) fault. (See Section 14.1.2.3 for more details.) Tag the fault with SC or

SS. If it is a state-of-system fault, develop it further. If it is a state-of-component fault, it is caused by primary faults, secondary faults, or command faults. (See Section 14.1.2.1 for more details.) If two or more lower-level faults contribute to the component fault, use an OR gate to flow the lower-level faults to the component fault.

6. Develop each fault – ask what are the immediate, necessary, and sufficient lower-level events that cause the higher-level fault. (See Section 14.1.2.2 for more details.) Using the appropriate logic gates connect the upper-level fault to the lower-level events.
7. Repeat steps (5) and (6) for every fault in the Fault Tree until the until the terminus of the tree is reached. The terminus is where all the events are Basic Events, or Undeveloped Events, or normal events.
8. Identify the components that are susceptible to Common Cause Failures (CCFs), and then properly model the CCF contribution.
9. Look for dependencies of faults.
10. Determine the minimal cut sets. Identify any minimal cut sets that depend on a singular Basic Event.
11. If quantitative data is available for the Basic Events, compute the probability of occurrence of the top undesired events (Hazardous Situations). Also perform an importance and sensitivity analysis.

Information from the Fault Tree can be used in the Preliminary Hazard Analysis (Section 14.3). For example, probability of Hazardous Situations would inform the P1 values; and sequence of events can be created from the causal chains in the Fault Trees.

Passive vs. Active components. Passive components' contribution to the system is more-or-less static. Examples are wires, tubes, and welds. Active components provide a dynamic contribution to the system. Examples of active components are valves and switches. Historically, from a reliability perspective, passive components are two to three orders of magnitude more reliable than active components.

Tip Because passive components are far less likely to fail than active components, you may want to exclude passive components from the Fault Tree analysis, as their contribution to System risk will be small.

It is important to develop a Fault Tree to a sufficient depth to gain meaningful knowledge of failure mechanisms and functional/failure dependencies. Developing Fault Trees beyond that is a waste of effort and potentially distracting.

A common heuristic is to model the system to the depth necessary to identify functional dependencies, and to a level for which failure rate data exists for the components.

14.1.5 Ground Rules

The ground rules listed in this section are intended to facilitate the creation of Fault Trees while minimizing confusion and wasted effort.

14.1.5.1 Write Faults as Faults

Choose the appropriate syntax. State what the fault is, and if conditions of the fault are material, state under what conditions. You may need to be verbose. Write it in a way that in the future, another person or even yourself, can make sense of the fault description. Example: catheter balloon bursts when inflated by the surgeon.

14.1.5.2 No Gate-to-Gate Connections

Gate inputs/outputs should be properly defined. A direct gate-to-gate connection is a shortcut which bypasses defining the lower-level gate's output. While it may be tempting to take such shortcuts, it makes the Fault Tree more difficult for others to read and understand.

14.1.5.3 Mark Low-Likelihood Faults as Basic Events

If it is clear that a fault is of very low likelihood, do not develop it to lower levels. Mark it as a Basic Event.

14.1.5.4 Don't Model Passive Components

Components are either passive, e.g., a wire or a pipe, or active, e.g., a switch or a valve. Historically, it is known that passive components failure rates are two to three orders of magnitude smaller than those of active components. While it is technically possible to model passive component faults, it does not add much value to the Risk Analysis of a product.

14.1.5.5 Be Judicious in Modeling Secondary Faults

Since the purpose of the FTA is identification of credible Hazardous Situations, be cautious about modeling secondary faults. Secondary faults occur under out-of-design conditions. Out-of-design conditions are usually unlikely. Consider the added value of modeling such faults.

Tip Use a skilled facilitator to guide the FTA work sessions. A good facilitator guides the brainstorming and proper Fault Tree construction, and also prevents participant confusion on concepts such as Hazard, Cause, and Basic Event. Facilitation increases the efficiency and effectiveness of the sessions.

14.2 MIND MAP ANALYSIS

14.2.1 Introduction

The use of diagrams to graphically map information is a very old technique. However, the 'Mind Map' was popularized by the British pop psychology author Tony Buzan in the 1970s. A mind map is basically a technique for graphically organizing thoughts and ideas. It is a very useful tool in brainstorming and is an accessible alternative to FTA. See Fig. 21 for a simple example.

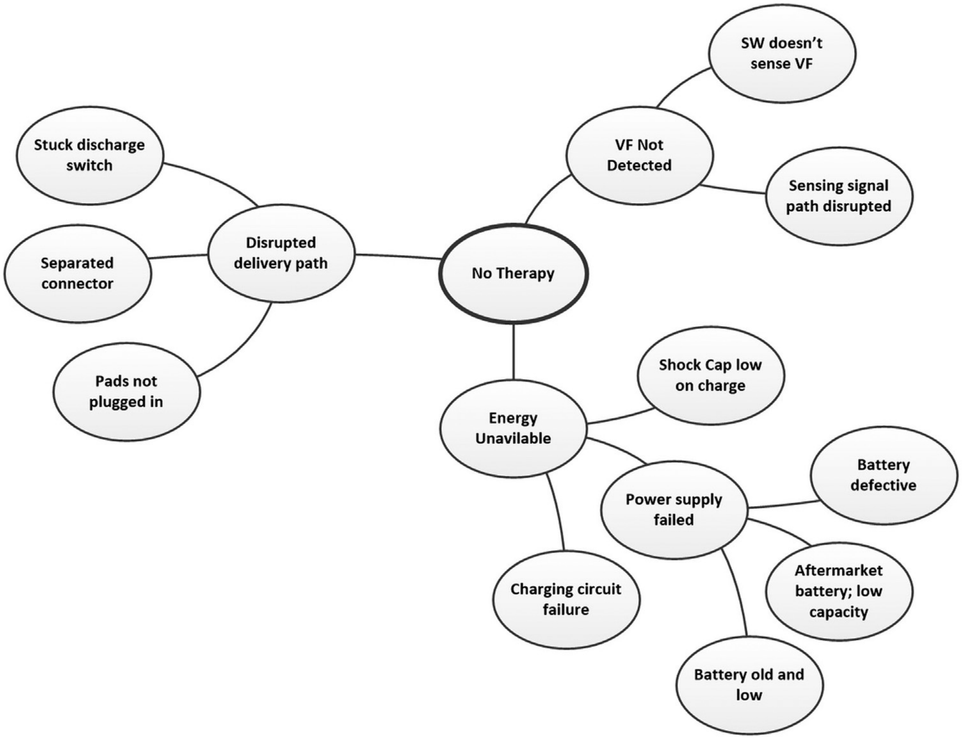


Figure 21 Example Mind Map.

An advantage of Mind Map over FTA is that is it simpler to learn than FTA, and software for Mind Mapping is either free or very low cost.

14.2.2 Theory

Starting from a central theme, which is marked as the central node, second layer nodes are connected to the central node. The second layer nodes comprise all the immediate, necessary, and sufficient pathways to the central node. This pattern repeats for each second layer node, and further nodes successively.

In the absence of FTA specialized nodes, such as Normal Event, and Undeveloped Event, develop each branch to the degree that it makes sense. If an event is undeveloped due to the current lack of information, you can put a TBD in there as a reminder to come back to it.

The main purpose for constructing a Mind Map is to graphically tell the story of how an undesired event can happen. This information will later be captured in the Sequence of Events in the PHA.

Unlike the FTA, Mind Maps do not use logic gates. Implicitly all connections are OR gates. For example, in Fig. 21 under 'VF not detected,' it can happen if either 'SW does not detect VF' OR 'Sensing signal path is disrupted.'

Methodology

Step 1: Obtain the System requirements and architectural design. Understand the theory of System operation.
Step 2: List the top undesired events for the System. These could be the Harms, or the Hazardous Situations.
Step 3: Define the scope of analysis – What's in, what's out.
Step 4: For each top undesired event create a Mind Map. Brainstorm and identify pathways to the Top Event.

Tip Although a Mind Map doesn't model logic gates and the connections are interpreted as OR gates, a work-around would be to create a node called 'AND' where multiple branches feed into it. The output of the AND node would occur if all the incoming branches occur.

14.3 PRELIMINARY HAZARD ANALYSIS

14.3.1 Introduction

ISO/TR 24971:2020 [15] says Preliminary Hazard Analysis (PHA) "…is an inductive method of analysis with the objective of identifying the hazards, hazardous situations and events that can cause harm for a given activity, facility or system."

PHA is a technique that can be used early in the development process to identify the Hazards, Hazardous Situations, and events that can cause Harm when few of the details of the medical device design are known. PHA is essentially a brainstorming forum where you try to imagine all the potential hazards of the systems, estimate their risks, and anticipate Risk Controls. The PHA can often be a precursor to further studies.

With the advance knowledge that is generated by the PHA, it becomes possible to identify the safety-critical parts of the System concept, estimate the potential risks associated with the System, and thus guide the design team to prioritize and focus resources on the highest risk parts of the System.

Performance of a PHA is most effective when people from various functions are engaged to participate. This provides for a multi-perspective analysis leveraging insights from many points of view. Here, risk management can serve as a tool for stimulation of communication among the team members who would ordinarily not have reason to communicate.

R&D engineering benefits from the advance knowledge generated by the PHA to anticipate Risk Controls and design them into the System early, instead of late in the product development process, thus reducing product development costs.

Another significant benefit of the PHA is that it can serve as an advisory to management not to proceed with the development of a product, where it is anticipated that the risks of the yet-undeveloped-device will outweigh its Benefits. It is far less expensive to cancel a project early, than to embark on the project and have to cancel it late in the design and development phase.

Basically, the PHA is an early version of the RACT. In fact, it uses the same RACT template. The main difference is that little actual design information exists at this stage, so the PHA uses a lot of estimations and predictions. The PHA is not a living document. It is only used as guidance to start the project.

It is highly recommended that a PHA be performed, especially for new and novel product development.

It is neither necessary nor useful to retrospectively perform a PHA on legacy products that have been in the field.

14.3.2 Methodology

Inputs to the PHA are:

- System requirements
- Concept architecture
- Intended Use, intended user, and intended use environment
- Risk acceptability criteria (from the RMP)
- CHL
- HAL

If the System is a new version or an iteration of a product that has been previously analyzed for risk, then it is advisable that the previous Risk Analysis be used as an input to the new analysis.

In the following sections the PHA workflow is described.

14.3.2.1 Safety Characteristics

Given the Intended Use, intended user, and intended use environment for the System, and given the concept architecture and System requirements, identify those qualitative and quantitative characteristics that could affect the safety of the medical device. Examples: choice of materials, accuracy of measurement, moving parts, required skill of the user, and the need for calibration/maintenance. Consider the technologies used in the device, and how they can contribute to Hazards. Where appropriate, identify the operational specification limits within which the device can be safely operated.

Include user-interface characteristics that could be related to safety.

Annex A of ISO/TR 24971 [15] provides a list of questions that can be useful aids in this effort.

14.3.2.2 Functional Failure Modes and Effects Analysis

One of the techniques that can provide early insights into the safety of the medical device is a Functional Failure Modes and Effect Analysis. In this methodology, the functions of the system are decomposed into their lower, underlying antecedents. Then each basic function is evaluated for failure modes and effects on the top functions.

14.3.2.3 Identify System Hazards

Using the knowledge gained in Section 14.3.2.1 examine the CHL. Identify the Hazards that are relevant to the System. Exclude the remaining Hazards in the CHL from the analysis and provide rationales for why any Hazard is excluded.

Also, consider potential Hazards that could be encountered under Reasonably Foreseeable Misuse conditions. See Section 4.1.1 for a definition of 'Reasonably Foreseeable Misuse.'

Interfaces are a common source of failures. Pay particular attention to interfaces to parts of the Systems that are designed by an external entity (supplier). Remember to also consider potential Hazards arising from interfaces between use-conditions. For example, the maintenance function is not commonly in the forefront of the mind of medical device designers. Could a maintenance person leave the device in a potentially unsafe state for the clinical user?

Postulate the potential Hazardous Situations for the System and perform a Fault Tree analysis to determine pathways that could lead to the identified Hazardous Situations. This would provide you with the reasonably foreseeable sequences or combinations of events that could lead to Hazardous Situations. See Section 14.1 for instructions on how to perform a Fault Tree Analysis.

Remember to consider the system under both normal and fault conditions.

Populate a RACT template with information from the Fault Tree Analysis. All applicable Hazards from the CHL should appear in the RACT. Each Hazard will have one or more Hazardous Situations associated with it. Document the potential pathways to each Hazardous Situation. These pathways are easily derived from the Fault Tree Analysis.

Identify the anticipated Risk Controls and strategies that will be deployed to minimize the risk to patients. Fill in a P1 value for each pathway to every Hazardous Situation. P1 is the probability of occurrence of the Hazardous Situation. If field data is available for P1, use that. Otherwise, using the collective team judgment, estimate a value for P1. When estimating P1, use a basis that makes sense for your product and facilitates your Risk Control decision-making. For a long-term implantable product, a unit such as *patient-year* is suitable. But for a device that is used repeatedly, *per-use* makes more sense. For example, P1 for the Hazardous Situation of ‘Over-infusion of insulin’ due to an erroneous blood glucose reading could be stated as ‘10^{-3} per use.’

Tip Estimate P1 for one device, not the entire fleet of devices. The reason is that making more devices doesn’t make any single device less safe. If P1 is estimated over the whole fleet of devices, the risk for a given Hazard would appear to continuously grow as more copies of the device are sold.

The next step is to evaluate the Hazardous Situations and identify the potential Harms that could ensue from each of them. A hazardous situation could lead to different kinds and severities of harms depending on the circumstances. In the BXM method, for every Harm there are five P2 numbers, which are the probabilities of sustaining Harm in different Severity classes. See Section 13.7, for more information on the HAL. Look up the P2 probabilities in the HAL and populate the RACT table with their respective values. Compute the risks for each Hazardous Situation by multiplying the P1 for each Hazardous Situation by the five P2 numbers from the HAL. This will result in five risk-numbers — one for each Severity class. If your method uses a single P2 number, then just use that to compute the risk.

Compute the Residual Risks for each Hazardous Situation, and also for the overall System. See Section 17.3 for details on how to do the computation.

At this point the PHA is ready to serve its purpose and answer the following questions:

1. Can the System be built such that its risks are acceptable?

   This is to advise Top Management on whether they should commit resources to design and development of the medical device. Using the risk acceptability criteria in the RMP, evaluate the Overall Residual Risk of the System. Is the Overall Residual Risk acceptable in all Severity classes? Perform a preliminary Benefit-Risk Analysis. Are the Benefits of the device predicted to outweigh the Overall Residual Risks of the device? If not, can the device concept be modified such that that Overall Residual Risk becomes acceptable and the Benefits of the device outweigh its risks? If a change in device concept cannot achieve that, then can a change in the Intended Use of the device achieve acceptability of the Overall Residual Risk, and dominance of Benefits over the Overall Residual Risk? If not, then the project should not be undertaken.

   Some factors may give you early warning of potential future problems. For example, if the concept for an implantable device requires exposure of the patient tissue to a toxic metal such as nickel, you could anticipate the possibility that in the end the Residual Risk of the product may be unacceptable.

2. What are the most safety-critical aspects of the System?

   The answer to this question helps to focus resources on the most important safety-critical aspects of the System. Look for any Hazardous Situation which has a risk in the unacceptable zone. They should be the highest priority areas for the Design and Development team. If all the risks of all the Hazardous Situations are acceptable, then make a subjective judgment on how to prioritize them. For example, you could see how close each Hazardous Situation is to the unacceptability boundary, and prioritize by the distance to unacceptability. In other words, Hazardous Situations whose risk is closest to the boundary of unacceptability should get the highest priority.

14.4 FAILURE MODES AND EFFECTS ANALYSIS

Failure Modes and Effects Analysis (FMEA) is a systematic method of exploring the ways in which an item or a process might potentially fail to achieve its objective, and the effects of such failures on: the performance of the system, or process, or the environment and personnel. FMEA is a forward reasoning process, also referred to as bottom-up or inductive analysis. The FMEA technique was originally developed by the United States military in 1949 as a reliability analysis technique. Later, it was used by NASA in many space programs. Today, many industries, in particular the automotive industry, use this analytical technique to improve the quality of their products.

There are different types of FMEA processes serving different purposes. The BXM method adapts the FMEA for the benefit of medical device risk management and uses four types of FMEA: Design FMEA (DFMEA), Software FMEA (SFMEA), Process FMEA (PFMEA), and Use-Misuse FMEA (UMFMEA). At the service risk management, FMEAs are used to identify Hazards, how they manifest, and estimate the likelihood of their occurrence.

It is important to distinguish two terms: Fault and Failure. A fault is an anomalous condition for a part. A failure is the inability of an entity to achieve its purpose — specified or expected.

- A fault could result in a failure, but not necessarily
- A failure may occur with no faults

With respect to risk management, FMEAs are used to identify Failure Modes which can result in Hazards or Hazardous Situations. It is important to realize that occurrence of faults and failures can result in Hazards, but not necessarily. And Hazards or Hazardous Situations can occur in the absence of any fault/failure. To elucidate — a medical device that is designed for adults, if used on children may create a Hazardous Situation, even though the device is working perfectly according to its design. Or, a medical device may have a fault that doesn't create a Hazard. For example, a cracked display on an infusion pump would be anomalous, but doesn't prevent the proper use of the device.

In the FMEA, the subject of analysis is decomposed into elements. The granularity of this decomposition is subjective and is called the level of indenture. During the course of the analysis, the Failure Modes of each element and consequences of that Failure Mode on the subject of analysis are considered. In general, the identification of Failure Modes and the resulting effects is based on experience with similar products and processes, or on knowledge of the applicable science.

The subject of the FMEA analysis may be the entire medical device, a subsystem, a component, a process, or anything that the analyst chooses.

Tip When choosing the granularity of decomposition of the subject of FMEA (level of indenture) save time and resources by not going deep into the parts of the System that are understood and have a well-known history.

It is important that the scope of analysis be clearly defined and understood. That is, the boundary of analysis, and what is included in the analysis should be clearly defined. Interfaces to the subject of the analysis should also be clearly identified.

Context of operation is important. The same Failure Mode could have starkly different severities, depending on the context of operation. For example, failure of a medical device during functional testing while in production has very different consequences than when the device is implanted in a patient.

14.4.1 Facilitation of FMEAs

Successful execution of FMEAs benefits from skillful facilitation of the FMEA sessions. The facilitator takes responsibility to:

- Convene the FMEA work sessions
- Ensure persons with appropriate competences are present
- Ensure proper resources, materials, and support elements are present at the working sessions
- Ensure the purpose of the FMEA, the ground rules, and context of operation are understood at the start of each working session
- Assist in the discernment of Causes, Failure Modes, Effects, and Mitigations
- Limit lengthy discussions and guide the team to useful conclusions
- Help the team maintain focus, and remain within the scope of analysis
- Manage the working sessions and terminate when productivity of the team declines due to fatigue or other factors.

14.4.2 Hierarchical Multi-Level FMEA

Hierarchical Multi-Level (HML) FMEA is a strategy that you can adopt to enable efficiencies of parallel processing, and modular, reusable analysis. This technique requires a system decomposition based on the system architecture as explained in Section 12.1.

The System, referred to as Level 1, or L1 in Fig. 22, is decomposed into two Level 2 (L2) components. Each L2 component is further decomposed into multiple L3

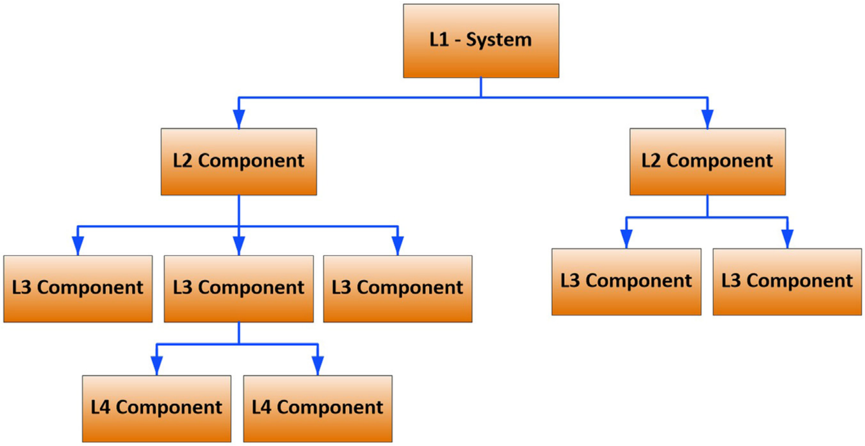


Figure 22 Multi-Level Hierarchy.

components, and so on. You can perform DFMEAs and PFMEAs on the lower-level components. Just as the physical system itself is progressively integrated from lower levels up to the top level, so too can the lower-level FMEAs be progressively integrated until the top-level System DFMEA is generated.

The benefits of this technique are multifold:

1. Parallel Work — Let's consider the example in Fig. 23, which describes an electronic thermometer decomposed into the electronics and the mechanical casing. It would be possible for the electronic team to be working on the FMEA of the electronics, while the mechanical team works on the casing FMEA. Later, the results of their work are integrated in the DFMEA of the Electronic Thermometer System.

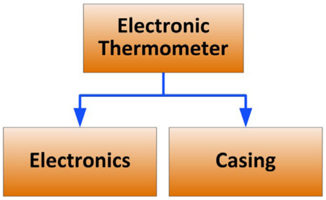


Figure 23 Electronic Thermometer.

2. Modularity and reuse — If in the example of Fig. 23 the manufacturer decides to update the thermometer casing for a fresh look, but keeps the electronics the same, the hierarchical multi-level FMEA technique allows the reuse of the electronics DFMEA, while refreshing only the casing D/PFMEA.
3. Easing of the work of analysis — Another benefit of HML FMEA is that for moderate to high complexity systems, doing one large FMEA is complex, error-prone, and difficult to maintain. HML allows breaking down the analysis into several smaller and more manageable analyses.

To achieve modularity of FMEAs, you must be clear on the architecture and respect the boundaries of analysis.

Specifically, the DFMEAs lend themselves to modular reusability. PFMEAs can be reused in the ordinary sense of basing a new analysis on old work and making revisions thereto. UMFMEAs are unique to each System and any reuse depends on the degree of similarity between the current System and the previous System.

For DFMEAs to be modularly reusable, strict adherence to the scope and boundary of analysis is required. In the DFMEAs, for Failure Modes that have a safety impact, Severity and Detectability ratings depend on the context of use. Therefore, during reuse of DFMEAs, for Failure Modes with safety impact, Severity and Detectability ratings need to be re-examined within the context of use.

For more details on HML FMEA and the integration of DFMEAs see Section 16.1.

14.4.3 Failure Theory

In the context of FMEA the End Effect is the outcome of a chain of events. Fig. 24 shows a model of this concept.

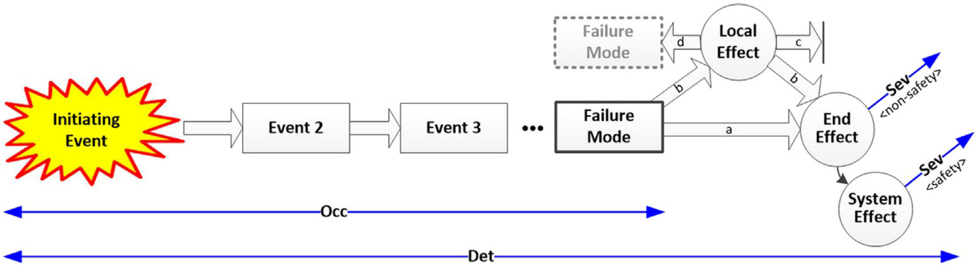


Figure 24 Failure Theory.

An initiating event could start a sequence of events, which lead to the Failure Mode. After the realization of the Failure Mode several scenarios can happen:

- **a)** The End Effect can directly manifest
- **b)** A Local Effect can happen first, which then leads into the End Effect
- **c)** Only a Local Effect can manifest which remains hidden
- **d)** A Local Effect may trigger another Failure Mode within the System

Occurrence (Occ), is the probability of occurrence of the Failure Mode P(FM). It encompasses the entire chain of events from the Initiating Event to the Failure Mode.

Note that the probability of occurrence of the End Effect P(EE) is not the same as P(FM). Some mitigations can serve to reduce the likelihood of the Failure Mode leading into the End Effect. For example, a small oil leak in a car engine can lead to dropped oil pressure. If this is not fixed and the car runs out of oil, the engine may fail (End Effect). But usually, a warning light in the dashboard alerts the driver to the problem. If, in this example, the driver gets the car repaired in time, the End Effect of engine failure will not manifest.

Severity is the property of the End Effect. For non-safety related Failure Modes, Severity is the significance of the worst reasonable consequence of the End Effect at the boundary of analysis. For safety-related Failure Modes, Severity is evaluated at the System level, which is the impact of the medical device on the patient/user. If the subject of analysis is the System, then the End Effect and System Effect are the same.

Detectability is applicable to the entire chain of events, from the Initiating Event to the End Effect. Detection may happen when the initiating event happens; or somewhere along the chain of events; or even after the End Effect has been manifested. In detection, there is an implicit assumption that mitigations are feasible to reduce the Occ or Sev ratings. If detection requires a user action, the user must be able to recognize the detected event; know what to do; and be able to react.

Mitigations could reduce the likelihood of occurrence of the Failure Mode (prevention mitigations), or improve the detectability (detection mitigations), or reduce the Severity of the End Effect (abatement mitigations). The rankings of Sev, Occ, and Det are inclusive of all the cited mitigations. That is, at the time we cite a mitigation, we presume it will be implemented and it will work as intended. If after verification it is found that a mitigation was not implemented, or it was not effective, then the rankings of Sev, Occ, or Det in the FMEA must be revised.

Tip Describe the mitigations with enough clarity that they could be verified.

14.4.4 Ground Rules

Ground rules are a set of understandings and agreements that the FMEA team uses to ensure smooth and productive work sessions. Ground rules can be expanded, refined, or clarified as the process continues.

Below are a set of suggested ground rules. You may adapt and adopt them as you see fit for your purposes.

1. Only one failure is considered at a time.
2. The function/attribute of each item under analysis must be clearly known and stated. (An ambiguous statement of function/attribute makes it difficult to tell whether the item has failed.)
3. Context of operation shall be stipulated.
4. Failure shall be defined. In some cases, it may not be clear how much degradation in the performance of an item would constitute a failure.
5. Only reasonable Causes and Failure Modes are considered.
6. If a failure results in multiple End Effects, each End Effect is listed in a separate row.
7. If a Failure Mode can be caused by different causal chains, each causal chain is listed in a separate row.

8. Designer errors are not included in the analysis as causes of failure. It is assumed that the design meets the requirements specification. It is important not to confuse the process of design with the design. Design is the output of the design process. Designer errors are captured by process, e.g., peer reviews, modeling, simulation, and testing.
9. If a mitigation eliminates a Failure Mode, or makes its likelihood indistinguishable from zero, you may delete that row, or keep that row in the FMEA as historical information for the benefit of future readers/users of the FMEA. If it is decided to keep the row, clearly mark it as not credible, and for informational purposes only.
10. In order to maintain the focus of FMEAs, DFMEA will assume that manufacturing is correct; PFMEA will assume that design is correct.
11. From the risk management perspective, it may be tolerable to have a high-criticality Failure Mode remain in the FMEA. Namely, if the Hazard from the End Effect of that Failure Mode is mitigated elsewhere in the System, such that the patient is kept safe from that Failure Mode.
12. The FMEAs in the hierarchical multi-level structure will use the same methodology and scales for rankings. This is to enable and facilitate integration of the FMEAs.

As stated above, these ground rules are intended to make the FMEA sessions flowing and productive. If for example, analysis of a Failure Mode reveals a missing requirement, or a design error, it doesn't mean you have to ignore it. To the contrary! You should communicate that to the product development team. This is how FMEAs add value to product development process.

14.4.5 Criticality Ranking

The RPN method is a common and historical practice which uses the product of Severity, Occurrence, and Detectability rankings, S × O × D as a means to prioritize the Failure Modes by criticality. Higher RPN indicates higher criticality. This is an easy to understand and implement technique. But there are many drawbacks with the RPN method. Namely,

- **RPN is not continuous**. In a scale where S, O, and D are ranked in five ordinal grades, the RPN range is 1–125. But many of the numbers in this range never manifest. For example: 28, 31, 49, ...
- **RPN sensitivity to other factors**. Let's consider two Failure Modes A and B with Severities 5 and 4, respectively. Case 1 – O=2, D=1. Case 2 – O=4, D=3. RPNs for Case 1 are A:10 and B:8; a difference of 2. RPNs for Case 2 are A:60 and B:48; a difference of 12, for the same difference in Severities: 5 vs. 4.

- **Consecutive ordinal numbers are not linearly spaced**. While for Severity the scale is linearly interpreted, for Occurrence ranking scales are typically logarithmic, e.g., 10^{-3}, 10^{-4}, 10^{-5}. This means in the Occurrence ranking a 3 is 10 times better than a 4.

Typically, RPNs for the Failure Modes in an FMEA are rank-ordered from, e.g., 1–125. Then actions are prescribed for the different ranges of RPN. For example, in Table 3 the range of 1–125 is divided into three levels and for each level certain actions are prescribed.

Table 3 RPN Stratification.

RPN	Action
53-125	Level 3 - Reduce RPN through failure compensating provisions.
13-52	Level 2 - If Safety Impact is Y, reduce RPN as far as possible. If Safety Impact is N, reduce RPN if feasible.
1-12	Level 1 - If Safety Impact is Y, reduce RPN as far as possible. If Safety Impact is N, further RPN reduction is not required.

There have been attempts to improve the RPN method. One such method is called ARPN, where the Severity, Occurrence, and Detectability are placed on a logarithmic scale, and thus instead of multiplying the S, O, and D, they are added together.

Another method which is used in the automotive industry is called Action Priority (AP). The AIAG FMEA Handbook [35] shows a method to prioritize the Failure Modes based on the S, O, and D rankings. The AIAG method resolves the S, O, and D rankings into three levels of action priority: High, Medium, and Low. Table 4 shows an example of the AIAG Action Prioritization schema.

Once the Action Priority levels for each Failure Mode has been determined, specific actions are prescribed, similar to Table 3. The AIAG FMEA Handbook [35] proposes the following actions for each level of Action Priority:

Priority High (H) – Highest priority for review and action. Team needs to either identify an appropriate action to improve Prevention and/or Detection Controls or justify and document why current controls are adequate.
Priority Medium (M) – Medium priority for review and action. Team should identify appropriate action to improve Prevention and/or Detection Controls, or at the discretions of the company justify and document why controls are adequate.
Priority Low (L) – Low priority for review and action. The team could identify actions to improve prevention or detection controls.

Table 4 Action Priority Ranking.[a]

Sev	Occ	Det	Action Priority (AP)
4-5	4-5	4-5	H
		2-3	H
		1	H
	2-3	4-5	H
		2-3	H
		1	M
	1	4-5	H
		2-3	M
		1	M
2-3	4-5	4-5	H
		2-3	M
		1	M
	2-3	4-5	M
		2-3	M
		1	L
	1	4-5	M
		2-3	L
		1	L
1	4-5	4-5	M
		2-3	L
		1	L
	2-3	4-5	L
		2-3	L
		1	L
	1	4-5	L
		2-3	L
		1	L

[a] From the Failure Mode and Effect Analysis: FMEA Handbook (FMEAAV-1) 1st Edition, 2019. Reprinted with permission of AIAG (Automotive Industry Action Group). AIAG makes no representation or warranty as to the accuracy or usefulness of its materials when presented in contexts, with other materials, or for uses, other than as originally published by AIAG. For additional information, or to purchase the referenced AIAG publication, contact AIAG at (248) 358−3003 or http://www.aiag.org.

The BXM method suggests a modified Pareto principle in the use of RPNs. Sort the Failure Modes by descending RPN values. Take the top 20 ± 10% of the Failure Modes. The reason for ± 10% is that usually there is a natural break around 20%. The ± 10% gives the flexibility to find and use that natural breakpoint. In addition to these top-ranked Failure Modes, include any Failure Mode with an End-Effect/System-Effect Severity ranking of ≥ 4 in the high-priority group for mitigations.

As stated above, RPN is a simple, but coarse method for prioritization of criticalities. A finer method is using a criticality matrix, such as Table 5, to customize the criticality rankings to suit your organization. There is no reason why the matrix should be two-dimensional (2D). Addition of a third factor, e.g., Detectability, would make the matrix three-dimensional (3D). While graphical display of a 3D matrix on a page may be less convenient, computers have no problem resolving and ranking criticalities based on your design of the criticality matrix.

Table 5 Example Criticality Matrix.

Criticality		Severity				
		1	2	3	4	5
Occurrence	1	2	2	3	3	3
	2	1	2	2	3	3
	3	1	1	2	2	3
	4	1	1	1	2	3
	5	1	1	1	2	2

14.4.6 Benefits of FMEA

Although in this book FMEAs are used for the benefit of safety risk management, there are many other advantages and benefit to FMEAs. By its nature, FMEA is systematic and exhaustive. It examines every element in the scope of analysis for their Failure Modes and effects. This helps with the detection and mitigation or elimination of product/process Failure Modes, thus improving product reliability and quality, which in turn should improve customer satisfaction.

FMEA is a predictive analytical technique. It enables early identification and handling of Failure Modes, thus reducing product development costs, by avoiding late-stage changes and corrections. Less rework also increases speed to market.

Another benefit of FMEAs is the discovery of missing or inadequate requirements. Designers design devices per the System requirements. Performing an FMEA on the design could reveal missing or inadequate requirements.

Tip If you find it difficult/impossible to distinguish the Failure Modes of an item within the scope of analysis, it is an indication of missing requirement(s) for that item.

Tip Mitigations are typically implemented via design requirements. Traceability analysis can reveal missing requirements, e.g., when a mitigation has no corresponding design requirements.

During the FMEA working sessions, you may discover that some of the assumptions made for the design of the product were not correct, which could lead to higher probability of failure than intended. For example, the designers may have assumed a product will be used in the 10–35°C temperature range, but during the FMEA working sessions it becomes apparent that the max operating ambient temperature will be actually be 50°C. This discovery would reveal an inadequacy in system requirements. Traceability analysis may also reveal inadequacies in the requirements. For example, you may discover that for a cited mitigation the corresponding requirements don't match the intention of the mitigation.

In safety risk management, FMEA is used as a technique for identification of Hazards and the sequences of events that could lead into those Hazards. Also, Occurrence ratings of the Failure Modes are used in System Risk Estimation. FMEAs detect many Failure Modes, some of which have no impact on safety. For example, failure of an electronic thermometer to power up is a reliability issue that could be annoying to a nurse but is not safety critical. Such findings have impact on business, customer satisfaction, etc. but do not create Hazards. It is beneficial to the business to know all Failure Modes of the System – safety-related or not. While safety-related Failure Modes should generally be mitigated as far as possible, the decision on whether, and how much to mitigate non-safety-related Failure Modes is entirely a business decision.

Another benefit of FMEAs is to serve as a connection point between suppliers and customers, and to enable collaboration between them. The End Effects of the suppliers' FMEAs would be the Failure Modes of the supplied part in the customer's FMEAs.

To get the most out of FMEAs, start FMEAs early and iterate during the course of design and development. You can start as soon as a concept and block diagrams are available and do high level, functional analyses. As more details become available you can continue with System FMEA. Later, as sub-system designs become available you can do Design FMEAs, and Use-Misuse FMEAs. When the manufacturing process is designed you can perform Process FMEAs. Product designs commonly evolve and change. This necessitates updating of the FMEAs. Continue to iterate until the end of the design process. This diligence pays off by not only helping the designers with discovery of weaknesses in their design and rectifying them before the product gets into the field, but also after the design is released, as any proposed new changes can be easily evaluated for impact to safety.

14.4.7 FMEA Weaknesses

Despite its power and utility, the FMEA technique has some weaknesses. Below, some of these weaknesses are listed:

- The FMEA is unable to detect End Effects that require multiple independent Failure Modes.
- The FMEA doesn't capture the interactions between Failure Modes.
- Because the FMEA fundamentally treats each Failure Mode individually as an independent failure, Common Cause failure analysis is not well-suited to the FMEA technique.
- The FMEA doesn't catch hazardous End Effects that are not due to failures, e.g., Hazards due to timing issues, physiological variability, etc.
- FMEA is only a qualitative analysis tool and does not have quantitative analysis capability. Even though FMEAs can help with design improvements, they cannot be used to predict reliability numbers, or estimate P1s.
- Performance of FMEAs is time-consuming.
- FMEA is difficult to master.

With the knowledge of the strengths and weaknesses of the FMEA as a technique, you can properly benefit from the value that it offers without being blindsided by its shortcomings.

Tip You can distinguish Common Cause Failures in an FMEA by locating repeated causes in the FMEA rows.

14.4.8 Ownership of FMEA

It is recommended that design engineering owns the DFMEA and SFMEA, usability engineering owns the UMFMEA, and manufacturing engineering owns the PFMEA. Ownership means taking responsibility for the creation and maintenance of the work products. Some of the reasons for this preference are:

1. The recommended owners have the closest knowledge of the workings of the items under their ownership and can best identify the causes of failures and evaluate the corresponding mitigations.

2. Risk management is only one of the beneficiaries of the FMEAs and uses the FMEAs as a technique for detection of the System Hazards. Since risk management is focused on safety, if risk management owns the FMEAs, the attention would be primarily on the safety related Failure Modes and some of the non-safety related Failure Modes may not get the attention that they deserve. Therefore, the knowledge that could be gained and the value that could be delivered to product development may not become realized.

Tip Involve the FMEA reviewers and stakeholders in the production of the FMEAs. Not only the collective participation enriches the analysis, but also the familiarity, which is gained as a result of the participation, will make the review of the FMEAs easier.

Tip FMEA is a project. Manage it like a project — allocate resources, plan the work, schedule the work, assign mitigations to individuals, and track each mitigation to completion and verification. If a mitigation fails verification testing, it should be backed out of the FMEA.

14.4.9 Deciding When to Perform an FMEA

FMEAs cost time and money to perform, and to maintain. How do you decide when performing an FMEA is warranted? If the subject of analysis is simple, well-understood, and low risk, both in terms of safety and product performance, then you could suffice by just addressing the Failure Modes of the item without digging deeply via an FMEA. The reasons to do FMEA include:

- Novel designs/technologies
- High complexity
- High safety risk
- High mission criticality
- Changes to Indications or use conditions
- History of undesirable field issues, e.g., reliability, Use Errors, etc.

You can triage the system design and apply FMEAs to the most critical parts of the architecture. Preliminary Hazard Analysis (Section 14.3) can help identify and prioritize the safety criticality of the system elements.

14.4.10 Making Your Way Through the FMEA

Performing FMEAs on any product of moderate to high complexity takes a large amount of time and resources. Often participants get tired and the quality of their input declines. You could even witness lengthy arguments that don't come to any conclusions. This is one of the reasons people tend to shy away from doing FMEAs. Or, if they do it, they try to get through it as quickly as they can, and just check the box as 'done.'

Here are some of the causes for unsuccessful FMEA sessions:

- The team is sequestered for long sessions over several days.
- The team loses focus on what is the subject of the analysis, or what is the context of operation for the subject of the analysis.
- Only a small part of the FMEA spreadsheet is projected on a screen; people can't see all the columns, or column headings; they get lost.
- One person dominates the conversation; others quiet down and just nod in agreement.
- Participants check their emails, smartphones, or do other work and lose focus.
- People get confused and have trouble distinguishing Causes from Failure Modes, and effects.
- The team is scoring Severity and occurrences as they go; this promotes inconsistencies in ratings, as people's frames of mind drift over time.
- People get stuck in long discussions on some items, which causes some participants' attention to drift off.
- People get tired, creativity ceases, and generic vague answers are put into the analysis.
- The product design process is already finished. There is no opportunity to make any changes. Findings of high significance will cause great pains and costs for the business. Therefore, there is reluctance to do any deep analysis in the fears of finding something significant.
- Granularity in ratings scales is too high. When estimating a rating, a lower granularity scale is better than a higher granularity scale. A high-granularity scale, e.g., a 10-point scale, could lead into unnecessary long debates in choosing between, e.g., a 6 vs. a 7 rating because the differentiation between adjacent ratings may not be so clear.

Below are some tips to help smooth the FMEA process and ensure success.

- First and foremost, use a skilled facilitator for the FMEA. Section 14.4.1 describes some of the responsibilities of an FMEA facilitator. Most FMEA team members participate in FMEA-work only occasionally. Therefore, they become rusty on the mechanics of the technique. With coaching and guidance from the facilitator, most participants climb the learning/remembering curve quickly.

- Where possible, try to reuse existing FMEAs to accelerate the work.
- Keep the duration of the sessions to less than 3 hours. Long sessions lead to fatigue and reduce the quality of work.
- Refresh the participants on the ground rules, definitions of Failure Mode, Local and End Effects, and be vigilant to ensure the entries in the FMEA are properly worded.
- If necessary, give a quick overview of failure theory (Fig. 24), and definitions of Severity, Occurrence, and Detectability (Section 14.4.3).
- Make the definitions of the rankings for Severity, Occurrence, and Detectability easily accessible, e.g., by printing them on posters and posting them on walls.
- Make sure the agenda and objective of the meeting is clear, state it at the beginning of the meeting and post it on a wall.
- Assign pre-work – before coming to the FMEA working session, participants should become familiar with the design under analysis. The FMEA session time is precious and should not be used for explaining the basic understanding of the subject of analysis.
- Have physical samples, models, drawings in the room that participants can touch and use as discussion tools. Simply touching a physical sample is a great thought stimulator. Also, it is much easier to convey thoughts and ideas about Failure Modes using models/drawings. For PFMEA, seeing the manufacturing process in action serves the same purpose.
- To improve consistency of the FMEA, first brainstorm on Failure Modes, causes and effects, then do the rankings and define the mitigations.
- During the brainstorming part, try to maintain momentum by just capturing the ideas and tidy up the spreadsheet after the meeting. It may be beneficial to have a scribe to assist you.
- Control the conversation and maintain focus; avoid sidebar conversations, lengthy war stories, and egotistical debates.
- Use the design architecture to break the FMEA work into pieces that would fit in one working session. Doing large FMEAs is tedious, and the process is error-prone, particularly if much time passes in between sessions.
- A way to keep a stronger focus on the analysis of Failure Modes is to not start the FMEA by displaying the complete FMEA template. Instead, just focus on the items in the scope of analysis, their Failure Modes, mechanisms of failure, and effects. Later, go back and fill the remaining columns.
- Using a database of Failure Modes and End Effects is beneficial for speeding the work and creating consistency in language.

Other advice that could help with the efficiency of the FMEA process:

- Have a lead-person for the subject of analysis pre-fill the Failure Modes and mechanisms of failure as seeds for discussion during the FMEA working session. Caution should be taken in that sometimes seeing the answer to a problem could inhibit the creativity of the other team members from thinking of new Failure Modes and Causes.
- It may be useful to have the designers keep the FMEA template in mind as they do their design work. It could prompt them to think about Failure Modes while they are making design decisions.

Tip Although FMEAs deal with failures under fault conditions, sometimes it may be beneficial to list an End Effect when there is no failure. See the two examples below:

Example 1: a diagnostic test fails to detect a virus. There is no failure — the test simply doesn't have 100% sensitivity.

Example 2: a polishing step leaves a pit in a metal surface. The process didn't fail. Normal metal surfaces sometimes pit.

In both examples, the End Effect is the same as if there was a failure. If there is no failure, there is also no Cause/Mechanism of Failure. In such cases write 'No Fault' in the column 'Causes/ Mechanisms of Failure.' This technique is an extension of the FMEA for the benefit of risk management.

14.4.11 Revisiting FMEAs

FMEAs are living documents that reflect the analysis of the latest product design, or manufacturing process, or other processes, e.g., installation, repair, etc. Therefore, FMEAs need to be revisited and updated from time to time. Reasons to revisit FMEAs include:

- Change to Intended Purpose/Intended Use
- Change to use conditions
- Change to design/process
- Moving of a manufacturing line
- Discovery of new Failure Modes
- Discovery of errors in the FMEA

14.5 FMEA IN THE CONTEXT OF RISK MANAGEMENT

The Hazard Analysis process uses a confluence of FMEAs from lower system-levels into the Risk Assessment and Control Table (RACT). The relation between FMEAs and the RACT is shown in the following figures.

In Fig. 25 integral Systems are modeled. (See Section 4.3 for the description of System types.) For integral Systems, Hazards can come from product-design, or manufacturing-process failures. Failure Modes whose End Effects at the System level are Hazards are captured in the RACT as Hazards. Note that all System Hazards must be found in the CHL.

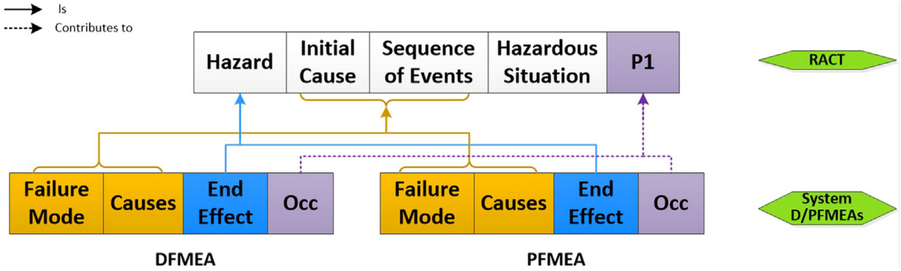


Figure 25 Integral Systems – System D/PFMEA to RACT Flow.

The initial Cause and sequence of events in the RACT are captured from the System FMEAs Causes, and Failure-Modes columns. Essentially, the Initial Cause and Sequence of Events tell the story of how a Hazard can be realized.

In Fig. 26 distributed Systems are modeled, where the relationship between the System DFMEA and the RACT is shown. The final assembly of distributed Systems is done by the user. Therefore, there is no System-PFMEA. Errors by the user in the assembly of the System are captured in the UMFMEA – see Fig. 27. For distributed Systems PFMEAs are carried out up to Level 2, which are the highest integral components of the System. (See Fig. 22 for a depiction leveling numbers.)

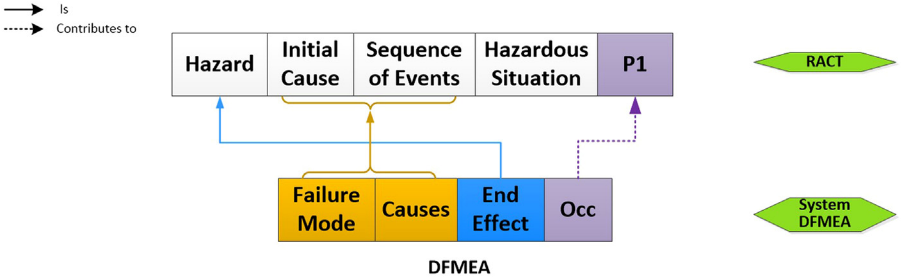


Figure 26 Distributed Systems – System DFMEA to RACT Flow.

A similar relationship exists between the UMFMEA and the RACT. Some of the End Effects of Use Errors lead into Hazards. The End Effects that are Hazards are captured in the RACT. Similarly, the initial Cause and sequence of events are captured from the UMFMEA Causes and Failure-Mode columns. The Initial Cause and Sequence of Events tell the story of how a Hazard can be realized due to a use Failure Mode. Fig. 27 is applicable to both integral and distributed Systems.

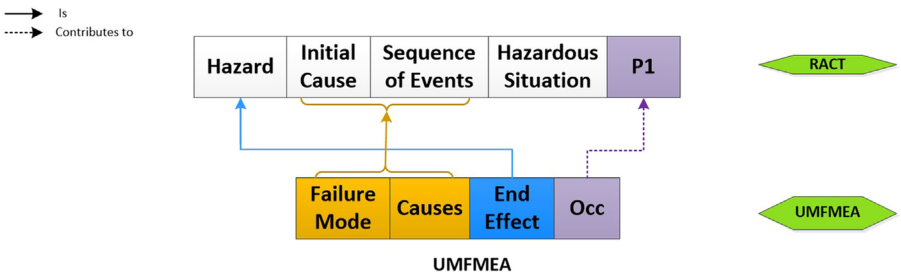


Figure 27 Relationship between UMFMEA and the RACT.

P1, the probability of occurrence of the Hazardous Situation, is influenced by the Occ rating in the System FMEAs. 'Influenced' means that P1 is estimated based on the contributions from all aspects of the System design, and not any single FMEA. For example, imagine an infusion pump. A nurse could erroneously enter a wrong dose on the pump's user interface. But the pump could be linked to the hospital database, which has the prescription for the patient. The pump could cross-check the entered dose against the patient's prescription, and if there is a large-enough variation, the pump could alert the nurse to a possible error. In this scenario, Occ=the probability of the Use Error, is not the same as P1 the probability of patient exposure to an over/under-dose. Also, P1 is the probability of the occurrence of the Hazardous Situation. Occ rating from System FMEAs can only indicate the probability of occurrence of the Hazard, not the exposure to the Hazard(s).

14.6 DESIGN FAILURE MODES AND EFFECTS ANALYSIS (DFMEA)

DFMEA is performed to uncover the design weaknesses that are present in the product and could lead to product failure. As with other FMEAs, DFMEA is a team activity. A suggested composition for the DFMEA team is:

- Design engineering
- System engineering
- Quality
- Clinical/Medical
- Risk management

It is best if DFMEA is done early in the design and development phase. Preliminary DFMEAs can and should be done on high-level designs, before all the details are known.

Not every failure has a safety impact. FMEAs can be used for two benefits:

1. for safety Risk Analysis (Hazard Analysis), and
2. for product Risk Analysis. Product risks have impact on reliability, performance, and project, to name a few, but are distinguished from safety risks.

Each DFMEA/PFMEA at a given level contributes to the next-level-up DFMEA. Failure Modes at a lower-level D/PFMEA become Causes at the next-level-up DFMEA. The End-Effects at a lower-level D/PFMEA become the Failure Modes at the next-level-up DFMEA. Probability of Failure Modes at a lower level, contribute to the probability of a Failure Mode at the next level up. See Fig. 28 for a graphical depiction of this concept.

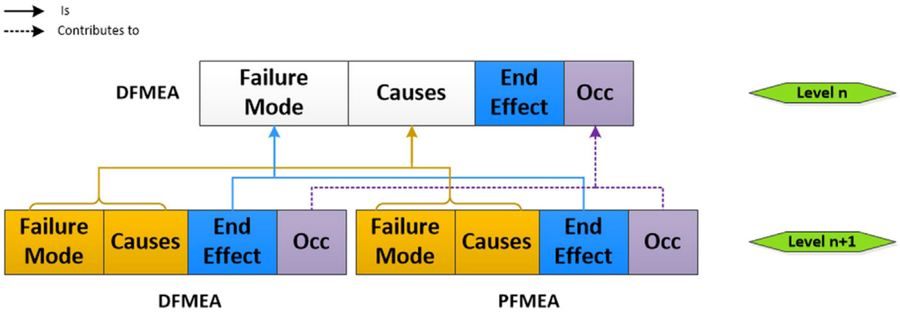


Figure 28 Information Flow between FMEA Levels.

Due to this hierarchical relationship between the levels of FMEAs, the same event could be seen as a Cause, a Failure Mode, or an End Effect depending on the level. As a result, it is easy to confuse Causes, Failure Modes, and End Effects.

Design for manufacturability is key to the success of a product and requires a connection between design engineering and manufacturing engineering. This connection is motivated by the DFMEA and PFMEA of a product.

In addition to vertical information flow between FMEAs, there is also horizontal information flow. Fig. 29 displays the direction and content of information flow among FMEAs.

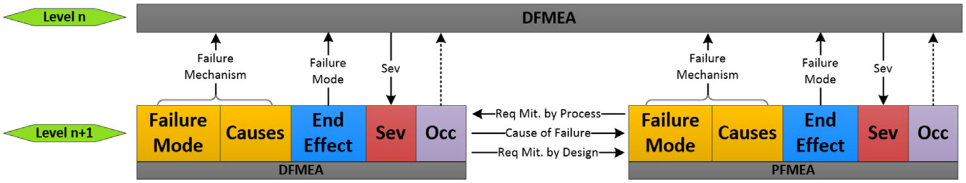


Figure 29 Information Flow Between FMEAs.

Per ground rule number 8 in Section 14.4.4, designer errors are excluded from the DFMEA. Excluding designer errors from the DFMEA does not mean that designers don't make mistakes. Designer errors are detected and corrected by process — which includes peer reviews, modeling, simulations, and testing.

It is possible to analyze the design process for ways in which designers could make mistakes and how those mistakes could escape. But that would be the PFMEA of the design process. The DFMEA analyzes the output of the design and the ways in which it could fail.

At the end of the design-phase in product development, the DFMEAs should be transferred to released-product engineering and maintained by that department. Risk management should be kept apprised of any proposed changes to the DFMEAs as part of any proposed change impact-analysis.

Tip Remember to include packaging of your medical device in the DFMEA.

14.6.1 DFMEA Workflow

In the following sections the workflow for DFMEA is described. The workflow corresponds to the DFMEA template that is provided in Appendix B – Templates.

14.6.1.1 Set Scope

The scope defines the boundary of the analysis, for the subject of analysis. For example, if you intend to analyze a defibrillator, include all parts of the product, including packaging, in the scope of analysis. Then decompose the scope into its constituent elements. The granularity of this decomposition is your choice. You could choose to analyze at the detailed components level (e.g., a capacitor), or at an intermediate architectural level (e.g., power supply). Each element within the scope of analysis should be cited in the DFMEA template as an item and analyzed for its Failure Modes and effects. It is permissible to have different depths of decomposition among the elements in the scope of analysis.

The scope of analysis should include the Failure Modes of each item, as well as Failure Modes of the interfaces among the items.

According to AIAG FMEA Handbook [35] there are five types of interfaces between elements of a system:

1. Physical interface – e.g., mechanical connections
2. Energy interface – e.g., electrical; thermal
3. Data interface – e.g., alerts; information; bit stream
4. Material interface – e.g., fluids; gases
5. Human-Machine interface – e.g., switches; knobs

Energy, data, and mass are typically transmitted via physical interfaces among the elements, e.g., via wires or tubes. Let's call the thing that is transmitted, 'payload.' For instance, the payload for a wire could be electrical energy or data; and the payload for a tube could be a fluid or a gas. The physical interface should be considered an element in the scope of analysis. Let's examine the example in Fig. 30. System D is comprised of elements A and B, pipe C and two connectors: 1 and 2. Element A contains a fluid that is transmitted to element B via pipe C. All three elements, A, B, and C, and the connectors should be in the scope of analysis for System D.

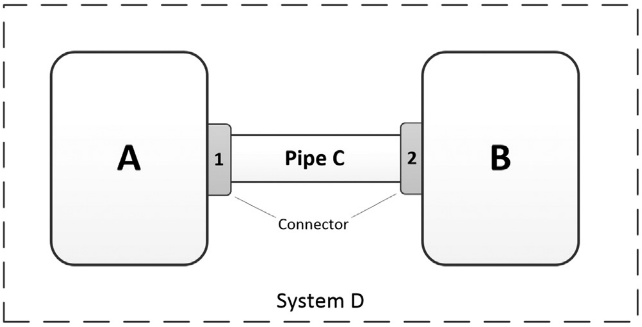


Figure 30 Interface Example.

Now, let's assume we are performing a DFMEA of only element B. Element B requires the fluid for its function, else it fails. Lack of fluid could be due to the failure of element A to provide the fluid; a break in pipe C; or failure of the connectors. If we are using the hierarchical multi-level FMEA, B should be agnostic of the world outside of it. All B cares about is that fluid is delivered to it. To B, lack of fluid is an external influence and would be cited as a Cause of failure. But B has no means of mitigating or controlling the supply of fluid.

There is one subtlety to consider. In whose scope of analysis should connector-2 reside – DFMEA of Pipe C, or DFMEA of element B? The decision is up to the analyst. A reasonable choice would be to include the part of the connection that is integral to B in the DFMEA of B, and the balance in the DFMEA of Pipe C.

Tip There are certain components whose probability of failure is exceedingly small. For example, a properly designed wire that conveys a digital signal is not likely to fail while operating in its design environment. Therefore, the contribution of failure of such a wire to safety risks would be negligible. In such cases, you can choose to exclude that element from the DFMEA.

14.6.1.2 Interface Matrix

Carlson [36] suggests creating a matrix where all the physical elements within the scope of analysis are cited both on the horizontal and vertical axes, and marking the intersections that must be analyzed. This is a good systematic method to avoid missing internal interfaces from the FMEA. A small example for the automobile that is presented in Fig. 41 in Section 16.1 could look like the following matrix.

Car subsystems	Engine	Body	Steering	Braking	Suspension	Electrical	Wheels
Engine		X				X	X
Body					X		
Steering					X		X
Braking					X		X
Suspension							X
Electrical							
Wheels							

External interfaces should also be included in the analysis.

14.6.1.3 Identify Primary and Secondary Functions

The subject of analysis has a number of functions. Segregate the item's functions into primary and secondary subgroups. Primary functions are those that achieve the main mission of the subject of analysis. All other functions are secondary.

The reason for this distinction is that Severity rankings for the End Effect are influenced by the impact of the Failure Mode on the functionality of the subject of analysis. Examination of Table 6 shows how the use of Primary and Secondary Functions can help the team arrive more quickly at a decision on the Severity ranking. In the case of Failure Modes with a safety impact, the Severity ranking is determined based on the System Effect on the patient/user.

14.6.1.4 Analyze

For each item in the scope of analysis identify its functions/attributes and Failure Modes. The functions/attributes are derived from the item's requirements. Use verb-noun constructs and cite any conditions necessary for the functions/attributes. For the Failure Modes answer the question: in what ways can this item fail to meet its design requirements? The Failure Modes could be functional or non-functional.

Example Failure Modes:

- Functional –
  - Doesn't perform the function
  - Performs the function intermittently
  - Delivers only part of the function
  - Delivers unintended/unexpected function
  - Delivers a degraded function
  - Delivers the function too late, too early, too much, too little, too long
- Non-functional – item swells, smokes, etc.

It is important that the use-conditions of the device are known. Consider the Failure Modes under normal use-conditions, as well as Reasonably Foreseeable Misuse conditions. For example, if a component is designed to operate in temperature range of 10–40°C, and it is known that some users operate it in temperatures of up to 50°C, then Failure Modes in the 10–50°C should be considered.

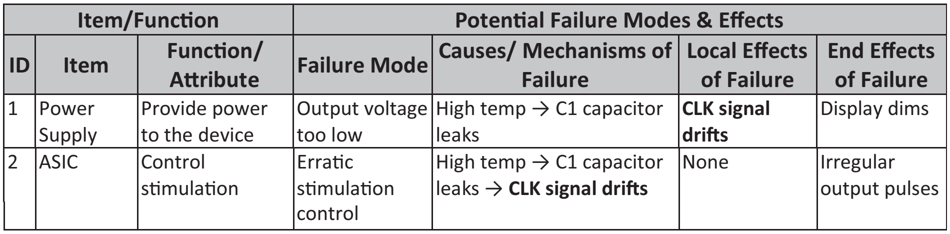
Each mode of failure of the item should go on a separate line in the template.

Describe each Failure Mode clearly and precisely and without judgmental language, e.g., intolerable or terrible. Know what constitutes a failure. Without adequate requirements for an element, it's not possible to tell whether a condition of an element is a failure or not.

Identify the Causes/Mechanisms of Failure including the contributing initial Cause, and realistic chain of events that could lead to the Failure Mode. Include both internal Causes, such as aging of a part, as well as external Causes such as environmental temperature. Include failures in the interactions/interfaces among the elements within the scope of analysis. After writing the Cause/Mechanism of the Failure Mode, read back what you wrote. Does it adequately explain to another reader why the Failure Mode happened?

Identify Local Effect, End Effect, and System Effect of the Failure Modes – see Fig. 24. An End Effect is that which is observable from outside of the boundary of analysis. A System Effect is the effect of the Failure Mode at the System-level. A Local Effect is that which is not observable from outside of the boundary of analysis. It is possible for a Local Effect to become the Cause for another Failure Mode. This is also referred to as Failure Mode interaction. In such cases, it is helpful to write a causal chain in the 'Causes/Mechanisms of failure' column, so it can be used again and built upon. Fig. 31 shows a snippet of a DFMEA where a Local Effect from row ID 1 becomes a Cause for the Failure Mode in row ID 2.

It is possible that a Failure Mode has only an End Effect, and no Local Effect. Denote this by entering N/A, 'none,' or some notation to indicate the absence of a Local Effect. Leaving the cell blank could be misconstrued as incomplete analysis. It is also possible that the End Effect does not create an observable Effect at the System level.



Item/Function			Potential Failure Modes & Effects			
ID	Item	Function/ Attribute	Failure Mode	Causes/ Mechanisms of Failure	Local Effects of Failure	End Effects of Failure
1	Power Supply	Provide power to the device	Output voltage too low	High temp → C1 capacitor leaks	**CLK signal drifts**	Display dims
2	ASIC	Control stimulation	Erratic stimulation control	High temp → C1 capacitor leaks → **CLK signal drifts**	None	Irregular output pulses

Figure 31 Sample DFMEA.

If the Failure Mode could result in a System Hazard, the Severity ranking should be determined based on the System Effect because patients/users interact with the System. In some cases, the System Effect is unknown. Consider the DFMEA for a generic valve. The manufacturer may not know in which medical device the valve will be used, therefore the System and the System Effect would be unknown. What would be known is the End Effect at the valve level, e.g., valve stuck open/closed. The impact of that End Effect depends on how/where the valve gets used.

Depending on the System architecture, the End Effect and System Effect could be the same thing. For example, in the System DFMEA of an X-ray machine, the End Effects are what are observable at the boundary of analysis, which is the X-ray machine itself. Therefore, the End Effect would be the same as the System Effect. But if the subject of the DFMEA is the radiation dose-controller, which is a subsystem of the X-ray machine, then the End Effect of the Failure Modes of the dose-controller would be different from the System Effects of the Failure Modes.

Tip It is advisable to include in the cell for End Effects, any requirements that would be violated. For example, in Fig. 31, row ID 2, Let's say there is a System requirement: Req123, that requires output pulses to be regular. Then cite Req123 in the cell for End Effects. This is a convenience for the design team that would help them with the mitigation of the Failure Modes. And also, if a design change is proposed they can easily trace it back to the FMEAs.

Safety impact relates to the System effect. To be able to determine whether a Failure Mode has a safety impact, we need to know how the subject of the analysis fits in the System. In the hierarchical multi-level FMEAs this can be known only after the integration of the FMEAs into the System DFMEA. But it may be possible to make some estimations of the Safety Impact in advance. For example, if it is certain that the Failure Mode would lead to one of the Hazards in the CHL, it would be a good guess that the Safety Impact will end up being Y. For instance, if the charging circuit in a defibrillator fails to charge the shock capacitor, likely the Safety Impact of that Failure

Mode will be Y, and the System Effect could be identified as loss of therapy. Another way to estimate the Safety Impact of a Failure Mode is if it would result in violating a System requirement which is tagged as: "Safety."

If the Safety Impact of the Failure Mode cannot be determined in advance, you can set the Safety Impact to N as a generic setting and use the 'No-Safety Impact' column in the Ratings tab of the template to determine the Severity rating. As the DFMEA is a living process and goes through iterations, when the FMEAs are rolled up to the System DFMEA, it will become apparent whether a given Failure Mode links-up to any Hazards. After the integration of the FMEAs and creation of the System DFMEA, a cross-check is done to ensure consistency of Safety-Impact ratings in the underlying FMEAs. Any End Effect that traces up to a Hazard must have a Y in the Safety Impact column.

It is possible that the Safety Impact of a Failure Mode changes from a Y to an N, depending on the additional mitigations that are implemented.

Tip Failure Modes whose Occurrence is indistinguishable from zero, are deemed not credible and thus can be excluded from the D/PFMEA. However, to help the reviewers of the D/PFMEA know that the analyst has considered a particular Failure Mode, even though it is not credible, at the discretion of the analyst, it's permissible to cite such Failure Modes in the DFMEA. Failure Modes that are not credible should be clearly delineated and need not be further analyzed.

Assign rankings. Tables 6—8 offer suggestions for rankings of Severity, Occurrence and Detectability, respectively. Let's examine each rating.

For Failure Modes that do not have a safety impact, Severity is the significance of the worst reasonable consequence of the End Effect at the boundary of analysis. For Failure Modes that do have a safety impact, Severity is the most likely degree of Harm to the patient/user at the System-level. Severity ranking definitions are different depending on whether the Failure Mode has a safety impact or not. In the case of no safety impact, use the left column in Table 6, and for those Failure Modes with a safety impact use the right column.

To rank the Severity of End Effects without a safety impact, it is necessary to know the Primary and Secondary Functions of the item under analysis. For example, if a Failure Mode causes the complete loss of the Primary Functions, the Severity ranking would be 4. The Severity ranking is a measure of the effectiveness of the abatement mitigations.

When the Failure Mode has a safety impact, the Severity ranking is based on the System Effect. In the BXM method there are 5 classes of Harm Severity. One could wonder how to choose the Severity ranking for Failure Modes with a safety impact, when the

Table 6 Definitions of DFMEA Severity Ratings.

Severity Criteria (Sev)		
Rank	**Severity Description (No Safety Impact)**	**Severity Description (Safety Impact)**
5	Described Failure Mode will cause immediate failure of the Subject. (Total loss of all functions – primary and secondary)	**Fatal** – Impact of the end-effect at the System level can be death
4	Described Failure Mode will severely impact Subject functionality | Complete loss of primary functions. May also lose secondary functions	**Critical** – Impact of the end-effect at the System level can be permanent impairment or irreversible injury
3	Described Failure Mode will reduce Subject functionality. (Partial loss of primary functions | Complete loss of secondary functions)	**Major** – Impact of the end-effect at the System level can be injury or impairment requiring medical or surgical intervention
2	Described Failure Mode will have temporal or self-restoring impact on functionality | partial loss of secondary functions	**Minor** – Impact of the end-effect at the System level can be temporary injury or impairment not requiring medical or surgical intervention
1	Described component failure will have no impact on functionality | Inconvenience to the user	**Negligible** – Impact of the end-effect at the System level can be at most an inconvenience, or temporary discomfort

System Effect may have a probability of Harm in all 5 Severity classes. The answer is to choose the most probable Severity class. Example: Let's say the failure of the sterile seal of an implantable device could cause contamination of the device, which could lead to infection. In the example that was presented in Fig. 15, Infection had the highest probability of causing a Critical Harm (45.0%). Therefore, in the DFMEA, the sterile seal failure would receive a Severity ranking of 4, Critical. Remember that in the DFMEA, this ranking is used only for criticality determination and the prioritization of resources on mitigating Failure Modes. The risk of Hazards is computed in the RACT and is a different matter.

Tip In the hierarchical multi-level FMEAs, lower-level DFMEAs are associated with the physical components and are reusable. If a component is used in multiple Systems and is a contributor to Hazards in those Systems, it may be that the same component would have different Severity rankings depending on the System in which it is used. The Severity rankings in reused FMEAs will need to be adjusted in the context of the System in which they are reused.

Occurrence ranking can be estimated from a variety of sources. For example:

- Field failure data on the same product
- Failure data for similar items, used under similar conditions
- Published data, e.g., MIL-HDBK-338B
- Data from suppliers
- Expert opinion

The Occ ranking is a measure of the effectiveness of the prevention mitigations. The 1–5 ranking is only a relative ranking of the Occurrence and may not reflect the actual occurrence probability of the Failure Mode. If the quantitative criteria are used to estimate the Occ rating (see Table 7), ensure the probabilities have a meaningful basis for the subject of analysis. Examples: per-use; per device-year, etc.

Table 7 Definitions of DFMEA Occurrence Ratings.

Probability of Occurrence Criteria (Occ)			
Category	**Rank**	**Qualitative Criteria**	**Quantitative Criteria**
Frequent	5	The occurrence is frequent. Failure may be almost certain | constant failure.	$\geq 10^{-3}$
Probable	4	The occurrence is probable. Failure may be likely | repeated failures are expected.	$<10^{-3}$ and $\geq 10^{-4}$
Occasional	3	The occurrence is occasional. Failures may occur at infrequent intervals.	$<10^{-4}$ and $\geq 10^{-5}$
Remote	2	The occurrence is remote. Failures are seldom expected to occur.	$<10^{-5}$ and $\geq 10^{-6}$
Improbable	1	The occurrence is improbable. The failure is not expected to occur.	$<10^{-6}$

In the context of risk management, detectability rating in DFMEA has a special meaning. It relates to **how likely it is for the End Effect to be detected and countermeasures be taken, external to the boundary of analysis, to minimize the risk of Harm**.

To elucidate this, consider the qualifier *external*. If a Failure Mode is detectable inside the subject of the DFMEA, and the designer chooses to devise a mechanism to counteract that Failure Mode, then the new design with the counteracting mechanism becomes the subject of the DFMEA. This means the internal detection is already built into the design. Example: a medical device is mains-powered. If the leakage current exceeds a certain amount, the user will receive an electric shock. The excessive current leakage is internally detectable. The designer designs-in a circuit breaker that senses current leakage and cuts off the power to the medical device to prevent electric shock. The new design, including the circuit breaker is now the target of analysis for the DFMEA. The Detection ranking for DFMEA is not about this type of internal detection of the Failure Mode.

The next point to notice is that '*risk of Harm*' is mentioned. Because we are using DFMEA at the service of safety, the focus is on the reduction of Harm, not necessarily improvements on reliability, customer satisfaction, etc. For example, consider an electrosurgical device that fails and delivers too much energy to the surgical site. If the System Effect of the Failure Mode is detectable by the surgeon, e.g., by an alarm in the device itself, or by observation of burning and smoking of patient tissue, then the surgeon can immediately disengage the device and apply medical care to the wound.

Use of Detection in the DFMEA is not intended to be a Risk Control. Within the domain of DFMEA we seek to prioritize the Failure Modes using Criticality rankings. Given two Failure Modes of equal Severity and Occurrence rankings, Detectability enables us to give higher priority to Failure Modes that are less detectable.

For Failure Modes that do not have a safety impact, Detection is irrelevant from the risk management perspective. For such Failure Modes set the Det rating to 1.

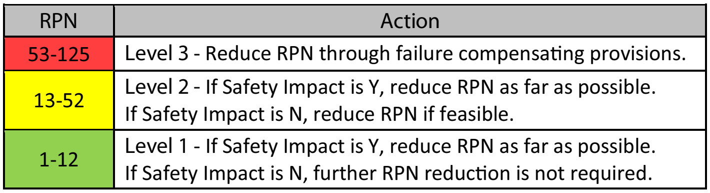
Refer to Table 8 for definitions of detectability rankings. Use quantitative data if available. Otherwise use the qualitative criteria to determine the Detectability rankings.

Table 8 DFMEA Detectability Ratings.

Detection Criteria (Det)			
Category	**Rank**	**Qualitative Criteria**	**Quantitative Criteria**
Undetectable	5	No understanding of physics or mechanics of failure | No detection opportunity | No means for detection | Countermeasures not possible	$<10^{-3}$
Low	4	Inadequate understanding of physics or mechanics of failure | Opportunity for detection is low | Countermeasures are unlikely	$<10^{-2}$ and $\geq 10^{-3}$
Moderate	3	Some understanding of physics or mechanics of failure | Opportunity for detection is moderate | Countermeasures are probable	$<10^{-1}$ and $\geq 10^{-2}$
High	2	Good understanding of physics or mechanics of failure | Opportunity for detection is high and Countermeasures are likely	$<9 \times 10^{-1}$ and $\geq 10^{-1}$
Almost Certain	1	Opportunity for detection is almost certain and Countermeasures are certain	$\geq 9 \times 10^{-1}$

RPN is a measure of criticality of a Failure Mode. RPN is the product of the rankings of Severity, Occurrence and Detection. This number is used to prioritize the Failure Modes and determine the degree of failure compensation that must be exercised. Table 9 offers a suggested stratification of failure compensating actions based on the criticality of the Failure Mode. The boundaries in Table 9 are selected at 12 and 52. But it is up to the manufacturer to decide where to draw the boundaries. Table 9 says that for the highest segment of RPN ratings, Level 3, the RPN must be reduced.

Table 9 DFMEA RPN Table.



RPN	Action
53-125	Level 3 - Reduce RPN through failure compensating provisions.
13-52	Level 2 - If Safety Impact is Y, reduce RPN as far as possible. If Safety Impact is N, reduce RPN if feasible.
1-12	Level 1 - If Safety Impact is Y, reduce RPN as far as possible. If Safety Impact is N, further RPN reduction is not required.

For Level 2, RPN should be reduced as far as possible, for safety-related Failure Modes. But for non-safety related Failure Modes, the decision as to how far to reduce the RPN is a business decision and depends on the feasibility of the actions needed to reduce the RPN.

For Level 1, for safety-related Failure Modes the RPN must be reduced as far as possible, therefore the treatment of RPN is the same as Level 2. However, for non-safety related Failure Modes, further action is not required.

Note that 'As Far As Possible' in Table 9 is inspired by EU MDR [2], and is one of the options for risk reduction that is offered by ISO 14971 [1]. You may adapt the action strategy to suit your QMS.

Reduction of criticality of Failure Modes is achieved via mitigations. Mitigations can eliminate the Failure Mode completely, reduce the likelihood of the Failure Mode, improve detectability, or diminish the Severity of the End Effect/System Effect of the Failure Mode. Examples of design means of mitigating Failure Modes:

- Use of redundancy, or backups
- Use of high-reliability parts
- Choice of proven, biocompatible materials

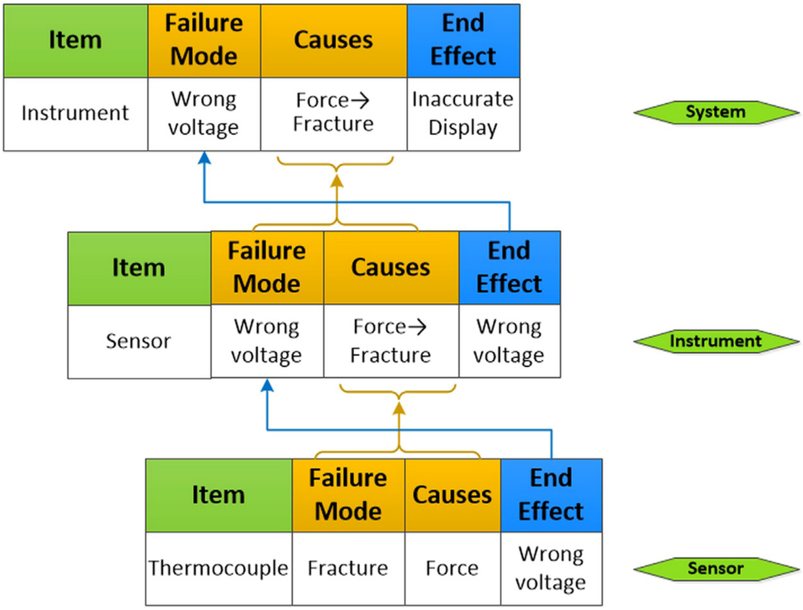
Mitigations should be clearly and specifically described such that they can be verified.

For the initial rankings, take into account the design features that are already included in the design and serve to reduce criticality. Include those features in the Existing

Mitigations column. If the initial criticality rating needs to be further reduced, suggest additional mitigations, and reassess the criticality rating under the Final Rating group.

The Remarks column can be used to document rationales for the choices of rankings, or why further mitigations are not done for a Failure Mode with safety impact, or anything else that could help future reviewers of the DFMEA gain better understanding of the analysis.

In some exceptional cases, the Failure Mode and the End Effect can be the same. For an example see Fig. 32, which models a surgical robot (the System), that uses various Instruments. On some of the Instruments, a temperature sensor is mounted. The Instruments just carry the sensor and pass the sensor signal directly to the System to display the temperature inside the body. For each Instrument, the sensor becomes a component. Let's say a Failure Mode of the sensor is to fracture under force. When that happens, the sensor outputs the wrong voltage. This is reflected in the lower row in Fig. 32. The End Effect of the Sensor FMEA becomes the Failure Mode of the item: 'Sensor' in the Instrument FMEA (blue arrow). This is reflected on the middle row in Fig. 32. Now, the End Effect at the Instrument level is still the output of the wrong voltage. Continuing up to the System level, the wrong voltage causes inaccurate display of temperature. As you see in this example, the Failure Mode and End Effect of the sensor are the same in the context of the Instrument FMEA.



Item	Failure Mode	Causes	End Effect
Instrument	Wrong voltage	Force→ Fracture	Inaccurate Display

Item	Failure Mode	Causes	End Effect
Sensor	Wrong voltage	Force→ Fracture	Wrong voltage

Item	Failure Mode	Causes	End Effect
Thermocouple	Fracture	Force	Wrong voltage

Figure 32 When End Effect and Failure Mode Are the Same.

Although this construct may appear somewhat redundant and laborious — the citation of the sensor failure in the FMEA of the Instrument, creates the possibility of reusable FMEAs. A shortcut would have been to bypass the Instrument FMEA and cite the Sensor directly in the System FMEA. But this would defeat the reusability of the Instrument FMEA.

With the use of software tools for automation of FMEA work, adherence to the BXM method of hierarchical, modular and reusable FMEAs becomes easier and less laborious.

14.7 PROCESS FAILURE MODES AND EFFECTS ANALYSIS (PFMEA)

A process is a sequence of tasks that are organized to produce a product or provide a service. The process is designed to fulfill the intent of the design. PFMEA is a structured approach to identify weaknesses in process-design and assign criticality levels to each step in a process. PFMEA is a powerful prevention technique, since it does not wait for defects to occur, but rather anticipates them and implements countermeasures ahead of time.

For risk management, Process refers typically to manufacturing process, but could also include other processes such as service, repair, maintenance and installation. For the balance of this section, the focus will be on manufacturing, but you can substitute any process that could have an impact on the safety of a medical device.

PFMEA is performed on processes over which we have control and focuses on these questions:

- How can the process fail to deliver a product/part built to its specifications?
- What is the degree of criticality of each process step in the failure of the process to produce a product/part to its specifications?

Each process step is subject to several factors. Kaoru Ishikawa in his fishbone root cause analysis method identified 5 factors, typically called 5 Ms: Man (people), Machine (equipment), Materials, Medium (environment) and Method. Others have added more Ms, e.g., Mission, Management and Maintenance. The AIAG FMEA handbook [35] proposes 4 factors: Man, Machine, Materials, Environment. The hypothesis is that a process step could fail due causes related to any of these factors. This concept is further expanded in Section 14.7.1.4.

Process Failure Modes with undesirable outcomes are mitigated via various means such as design, or process changes. As a matter of practicality, the Failure Modes are prioritized so that the highest-criticality Failure Modes are addressed first.

As in other FMEAs, PFMEA is a team activity. A suggested PFMEA team composition is presented below:

- Manufacturing engineering
- Manufacturing technicians
- Systems engineering
- Quality
- Clinical/Medical
- Risk management

14.7.1 PFMEA Workflow

In the following sections the workflow for PFMEA is described. The workflow corresponds to the template that is provided in Appendix B — Templates.

14.7.1.1 Set Scope

Identify the process that will be the subject of analysis. This defines the boundary of analysis. Does your process include receiving inspection? Does it include warehousing after the completion of manufacturing? Does it include shipping? Be very clear on what is included in the scope of analysis.

14.7.1.2 Identify Primary and Secondary Functions

Identify the primary and secondary functions of the product of the process. Primary functions are those that achieve the main mission of the product of the process under analysis. In other words, primary functions are why the product is purchased. All other functions are secondary. For example, a pacemaker produces stimulation pulses to the heart, but also logs device faults. Both are functions but producing pacing pulses is the primary function of the device, and fault logging is a secondary function.

The purpose and benefit of classifying functions into primary and secondary functions is to accelerate the determination of Severity rankings of End Effects for Failure Modes with no safety impact.

14.7.1.3 Process Flow Diagram

Process Flow Diagrams (PFD) are a graphical way of describing a process, its constituent tasks, and their sequence. A PFD represents the process flow as it physically exists when “walking the process.” A PFD helps with the brainstorming and communication of the process design. The PFMEA process needs a complete list of process steps that comprise the process under analysis. The level of detail can be decided by the team. Including more detail takes time, but it reduces the probability of missing Failure

Modes. For high-criticality process steps it is advisable to be more detailed, while for less critical steps you can be more high-level.

Manufacturing engineering should be able to produce the PFD. A good way to go about creating the PFD is to first log the major tasks of the process. Then add the detailed tasks, and the steps necessary to realize each task. Include re-work and repair steps. Use verb-object construct to describe process steps, e.g., drill hole, wash part. Next, have a walk through the PFD with the stakeholders, e.g., manufacturing engineers and technicians, to debug the PFD. Finally, perform the process per the PFD to verify the PFD. Add any discovered missing steps.

The process steps that are defined in the PFD are input to the PFMEA.

14.7.1.4 Analyze

Cite each step of the process that was described in the PFD, in the PFMEA template.

> *Example process step: rinse casing.*

For each process step, describe the purpose or intent of the step.

> *Example purpose: to remove debris from machined casing.*

Identify the influencing factors for the process step: Man (human operator), Machine (tooling), Materials, Environment. Identify the process characteristics that affect the ability of the process step the achieve the design intent. Process characteristics are measurable, controllable factors that can be monitored during the execution of the process. Process step failures can be deduced from process step function & process characteristics.

For each process step, identify the ways in which it could fail. If there is more than one way to fail, enter each Failure Mode in a separate row.

Failure Modes of a process step could be:

- Complete failure
- Partial failure
- Intermittent failure
- Process drift, which could lead into failure

Process steps can have one of four types of potential outcomes:

1. Desired outcome is achieved.
2. Desired outcome is not achieved. *Example: rinse is incomplete.*

3. Desired outcome is achieved but some deleterious unintended outcomes are also achieved. *Example: rinse is complete, but rinse-head impacts casing.*
4. Desired outcome is not achieved, and some deleterious unintended outcomes are achieved. *Example: casing becomes contaminated due to use of wrong rinse solution.*

Process step outcomes 2, 3, or 4 are process step Failure Modes and are cited in the PFMEA.

Describe the Failure Mode clearly. Descriptions such as "not OK," or "failed" would not be clear enough to prompt appropriate mitigative actions.

In the 'Causes/Mechanisms of Failure' column, describe realistic potential Causes of the failure. *Example: rinse timer drifts.* Describe failure causes clearly and precisely so that the mitigations can be appropriately addressed to the causes. Consider the classic Ishikawa categories of process failure causes:

- Man – causes to do with the person(s) involved in the operation of the function.
- Machine/equipment – causes to do with the equipment used to perform the function, e.g., drill press, welding machine, camera.
- Materials – causes to do with the materials used to perform the function. This could include the additives, e.g., machining oil, cleaning solutions, etc. Or, the material of the product itself, as intended by the designers. For example, a part may be too slippery which could result in the operator dropping it. Note that this is not considered a design error – the materials are as intended.
- Environment – ambient conditions that could cause the function not to be performed as intended, e.g., heat, noise, lighting, dust, etc.

Avoid highly imaginative but improbable Causes. While they may be interesting, or even entertaining, they don't add real value to the product development process and waste valuable engineering time in endless discussions.

After writing the Cause/Mechanism of the Failure Mode, read back what you wrote. Does it adequately explain to another reader why the Failure Mode happened?

Design Failure Modes are excluded as PFMEA failure causes. It is assumed that the design meets the intent of the requirements. It may be that the design is inappropriate for successful manufacturing, which could prompt a design change. But it is not a design failure.

Next determine the Local Effect, End Effect and System Effect of the Failure Mode. An End Effect is that which is visible at the boundary of analysis. Presence of an End Effect implies that the Failure Mode was not detected and trapped within the process. An End Effect is a consequence of the Failure Mode, which is perceivable on the product of the process. *Example: metal debris on casing causes short circuit in the electronics*. Some End Effects may propagate to the System level and create a System Effect. That is something which is perceivable to the patient/user and may be a Hazard. A Local Effect is not perceivable on the product of the process. It may be something internal to the process that could cascade into another Failure Mode in a subsequent process step, which would have its own End Effect. *Example: rinse solution is not discarded*. If the contaminated rinse solution is reused, it could be the Cause for another type of Failure Mode. *Example: damage to tooling*.

Safety Impact is a System effect. To be able to determine whether a Failure Mode has a safety impact, we need to know how the product of the process fits in the System and discern the System Effect of the Failure Mode. In the hierarchical multi-level FMEAs, this can be known only after the integration of the FMEAs into the System DFMEA. But it may be possible to make some estimations of the Safety Impact in advance. If it is certain that the Failure Mode would lead to one of the Hazards in the CHL, it would be a good guess that the Safety Impact will end up being Y. For example, if a toxic solvent is used as a process aid to create a part that will contact patient tissue; and the failure of a cleaning process step could leave toxic residues on the medical component, likely the Safety Impact of that Failure Mode will be Y. Another way to estimate the Safety Impact of a process-step failure is if it would violate a System requirement which is tagged as: "Safety."

If the Safety Impact of the Failure Mode cannot be determined in advance, you can set the Safety Impact to N as a generic setting and use the 'No-Safety Impact' column in the Ratings tab of the template to determine the Severity rating. As the PFMEA is a living process and goes through an iterative process, when the FMEAs are rolled up to the System DFMEA, it will become apparent whether a given Failure Mode links up to any Hazards. After the integration of the FMEAs and creation of the System DFMEA, a cross-check is done to ensure consistency of Safety Impact ratings. Any End Effect that traces up to a Hazard must have a Y in the Safety Impact column.

For Failure Modes that do not have a safety impact, Severity is the significance of the worst reasonable consequence of the End Effect at the boundary of analysis. For Failure Modes that do have a safety impact, Severity is the most likely degree of Harm to the patient/user at the System-level. Severity ranking definitions are different depending on whether the Failure Mode has a safety impact or not. In the case of no safety impact, rank the impact of the Failure Mode on the product of the process, using the left column in Table 10 – No Safety Impact. For the Failure Modes with a safety impact, examine the System Effect and consider the most likely degree of Harm to the patient/user at the System-level. Select a ranking from the right column in Table 10 – Safety Impact, that corresponds with that Harm Severity.

Table 10 PFMEA Severity Rankings.

Severity Criteria (Sev)		
Rank	**Severity Descriptions – Non-Safety**	**Severity Description – Safety Impact**
5	Failure to meet Regulatory requirements | Process line shutdown for extended length of time | Total loss of all functions – primary and secondary | Scrapping >70% of the production	**Fatal** – Impact of the end-effect at the System level can be death
4	Loss or degradation of primary functions | Failure to meet product specification | Scrapping of 50–70% of the production	**Critical** – Impact of the end-effect at the System level can be permanent impairment or irreversible injury
3	Loss or degradation of secondary functions | Reduced reliability but still within Spec | Scrapping of 25–50% of the production.	**Major** – Impact of the end-effect at the System level can be injury or impairment requiring medical or surgical intervention
2	Process delay | Scrapping of 5–25% of the production. | Minor cosmetic or usability impact but still within Spec	**Minor** – Impact of the end-effect at the System level can be temporary injury or impairment not requiring medical or surgical intervention
1	Scrapping of 0–5% of the production | Some of the products have to be reworked	**Negligible** – Impact of the end-effect at the System level can be at most an inconvenience, or temporary discomfort

Ultimately the Severity rating should come from L1 DFMEA. For a supplier, it may not be clear how important is the failure of the part that they supply. The customer must inform the supplier of the Severity ratings for the supplied parts. This knowledge helps the suppliers know what degree of rigor they need to exercise in the production of their supplied parts.

In the BXM method there are 5 classes of Harm Severity. One could wonder how to choose the Severity ranking for the System Effect in an FMEA. The answer is to choose the most probable Severity class. Example: Let's say the Failure Mode of the process step that seals a sterile package for an implantable device, is 'incomplete sealing.' This could lead to contamination of the device, which could lead to infection. In the example that was presented in Fig. 15, the Harm of Infection showed the highest probability in the Critical class (45.0%). Therefore, in the PFMEA, the Failure Mode of process step to seal the sterile package would receive a Severity ranking of 4, Critical.

Remember that in FMEAs, this ranking is used only for criticality determination and the prioritization of resources on mitigating Failure Modes. The risk of Hazards is computed in the RACT and is a different matter.

The ranking in the Occ column of the PFMEA is indicative of the likelihood of occurrence of the Failure Mode. The Occ ranking is a measure of the effectiveness of the prevention mitigations. The 1–5 range is only a relative ranking of the Occurrence and may not reflect the actual occurrence probability of the Failure Mode. Refer to Table 11 for the definitions of the Occurrence rankings. Use quantitative data if available. Otherwise use the qualitative definitions to determine the Occ ranking. If quantitative data is used, ensure the units are defined and consistently applied. The Occ ranking is inclusive of the implementation of all pertinent mitigations. In other words, choose the Occurrence rank assuming the cited mitigations are already implemented and effective. Occurrence ranking may be based on expert opinion, or experience with comparable processes.

Table 11 PFMEA Occurrence Ratings.

Probability of Occurrence Criteria (Occ)			
Category	**Rank**	**Qualitative Criteria**	**Quantitative Criteria**
Frequent	5	The occurrence is frequent. Failure may be almost certain | constant failure.	$\geq 10^{-1}$
Probable	4	The occurrence is probable. Failure may be likely | Repeated failures are expected.	$<10^{-1}$ and $\geq 10^{-2}$
Occasional	3	The occurrence is occasional | Failures may occur at infrequent intervals.	$<10^{-2}$ and $\geq 10^{-3}$
Remote	2	The occurrence is remote | Failures are seldom expected to occur.	$<10^{-3}$ and $\geq 10^{-4}$
Improbable	1	The occurrence is improbable | Failure is not expected to occur.	$<10^{-4}$

Det, or Detectability, is the likelihood of detection of a Failure Mode. It is an estimate of the probability of detecting the Failure Mode before the product is released. Therefore, detection may occur anywhere in the causal chain, from the Cause of Failure Mode, to the Failure Mode itself, to the End Effect. Detection Mitigations together with the corresponding actions serve to make it less likely for the result of a process-step failure to exit the process and manifest the End Effect. Examples of detection mitigations: visual inspection; optical automated inspection; mechanical gauge testing; functional testing. Refer to Table 12 for definitions of detectability rankings.

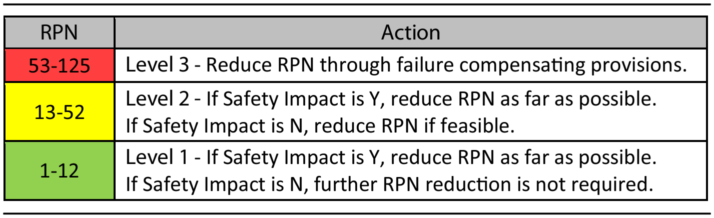
Table 12 PFMEA Detectability Ratings.

Detection Criteria (Det)			
Category	**Rank**	**Qualitative Criteria**	**Quantitative Criteria**
Undetectable	5	No detection opportunity | No means for detection | Physics-of-Failure not understood | Countermeasures not possible	$<10^{-3}$
Low	4	Opportunity for detection is low, e.g., very low sampling | Failure is very difficult to detect | Countermeasures are unlikely	$<10^{-2}$ and $\geq 10^{-3}$
Moderate	3	Opportunity for detection is moderate, e.g., 10% sampling | Detection of process-failure is made through operator measurement and decision | Countermeasures are probable	$<10^{-1}$ and $\geq 10^{-2}$
High	2	Opportunity for detection is high, e.g., 100% visual inspection | Detection of process failure is made through automated in-station controls that will detect the discrepancy and alert the operator | Countermeasures are likely	$<9\times10^{-1}$ and $\geq 10^{-1}$
Almost Certain	1	Failure is obvious | Detection is almost certain, e.g., 100% inspection via automated test equipment or fixturing | Countermeasures are certain	$\geq 9\times10^{-1}$

Use quantitative data if available. Otherwise use the qualitative criteria to determine the Detectability rankings.

RPN is a measure of criticality of a Failure Mode. RPN is the product of the rankings of Severity, Occurrence and Detection. This number is used to prioritize the Failure Modes and determine the degree of failure compensation that must be exercised. Table 13 offers a suggested stratification of compensating actions based on the

Table 13 PFMEA RPN Table.



RPN	Action
53-125	Level 3 - Reduce RPN through failure compensating provisions.
13-52	Level 2 - If Safety Impact is Y, reduce RPN as far as possible. If Safety Impact is N, reduce RPN if feasible.
1-12	Level 1 - If Safety Impact is Y, reduce RPN as far as possible. If Safety Impact is N, further RPN reduction is not required.

criticality of the process Failure Modes. The boundaries in Table 13 are selected at 12 and 52. But it is up to the manufacturer to decide where to draw the boundaries. Table 13 says that for the highest segment of RPN ratings, Level 3, the RPN must be reduced.

For Level 2, RPN should be reduced as far as possible, for safety-related Failure Modes. But for non-safety related Failure Modes, the decision as to how far to reduce the RPN is a business decision and depends on the feasibility of the actions needed to reduce the RPN.

For Level 1, for safety-related Failure Modes the RPN must be reduced as far as possible, therefore the treatment of RPN is the same as Level 2. However, for non-safety related Failure Modes, further action is not required.

14.8 USE/MISUSE FAILURE MODES AND EFFECTS ANALYSIS (UMFMEA)

UMFMEA is a technique with which to analyze the effects of failures in the use of a medical device, and also the effects of misuse of the device. We distinguish Misuse from Use Error. As defined in Section 9.1, a Use Error is the failure of a User to achieve the intended and expected outcome from the interaction with the medical device. A Use Error is not something that the User intends, but Misuse is intended by the User.

The UMFMEA is a System-level FMEA, similar to System DFMEA or System PFMEA. This is because the User interacts with the whole System (the Medical Device). Therefore, the scope of analysis of the UMFMEA is the entire System, and End Effects of the UMFMEA are System Effects, which can be System Hazards. The input to the UMFMEA is the set of System use scenarios, tasks and step actions.

For complex Systems it is possible to break down the System UMFMEA into sections and then integrate them to create the System UMFMEA. This strategy allows both parallel work streams, and reuse of existing UMFMEAs. As an example, consider a surgical robot that uses a number of surgical tools. If a new robot is designed that uses some of the same surgical tools, the UMFMEA of the surgical tools could potentially be reused.

Just as in other FMEAs, the UMFMEA discovers many Failure Modes, only some of which may have a safety impact. Knowledge of the non-safety-related Failure Modes is useful in improvement of the design for better user experience or product effectiveness. Risk management leverages only the Failure Modes that have a safety impact. The UMFMEA is an analytical technique that serves both the risk management and the usability engineering efforts.

Normally the UMFMEA considers the ways in which every task in the normal flow of events could go wrong. But users don't always follow the normal flow. Sometimes the users make mistakes and go down unexpected alternate paths. They may even improvise and create new pathways. Due to the fact that the number of alternate paths may be very large, it may be that task analysis doesn't consider all the possible alternate paths. It's advisable to try to consider the alternate paths that are related to safety critical operations of the device.

UMFMEA does not consider malice in the scope of analysis.

14.8.1 Distinctions

There are many special terms used in the domain of usability engineering and UMFMEA. It is important to have a clear understanding of these terms and their distinctions. Without this clarity, it would not be possible to properly analyze the medical device or communicate your analysis. Below some of the important terms are examined.

Use: using the device for what it was intended and per the supplied labeling.

The outcomes from attempted Use can be:

1. **Successful Use**
2. **Failed Use**
   - **a.** Step action is not performed.
     The user has the intention to perform action but is unable to complete the action.

     Example: UI does not permit the performance of the action, or UI is so confusing that the user cannot perform the action.

   - **b.** Step action is performed, but with difficulty.
     The user has the intention and executes the action, but with difficulty.

     Example: complicated UI causes the user the make mistakes that he/she recognizes and corrects the mistake. The action is ultimately completed but with struggle and errors.

   - **c.** Step action is performed incorrectly.
     The user has the intention and completes the task, but incorrectly. To analyze this outcome let's refer to Fig. 9. To isolate Use Errors from design-failures, we'll focus on the right side of the picture. The potential causes of performing a step action incorrectly are:
     - **i.** Incorrect perception – The User doesn't see/hear/sense the stimuli that is expected to be perceived. Or, the User misunderstands the signal. For example, thinks a letter O is the digit 0.

ii. Incorrect cognition – The user has a wrong mental model of the system, and with the correct perception, makes a wrong decision. Possible causes: lack of knowledge/training, unfamiliarity with the device. Or, user has a memory lapse. That is, the user knows what to do, but forgets momentarily, or makes a mistake.

iii. Incorrect action – The user has the correct perception, cognition and intention but fails to perform the action correctly. For example, a slip of the finger, or physical inability to reach/pull/twist/etc.

Failed use can be both due to action, or lack of action by the User. An unexpected outcome either in the patient physiology or in the medical device is not considered a Use Error. Use the above three types of Failed-Use categories to guide you in the distinction of Use failure from other types of failures.

Abnormal use: [19] Section 3.1: "conscious, deliberate act or deliberate omission of an act that is counter to or violates normal use and is also beyond any further reasonable means of user interface-related Risk Control by the manufacturer."

For example, alteration of a device, disregard of device alarms, or use of the device under conditions that are clearly prohibited by the manufacturer.

Example 1: *Ventilator alarm system is intentionally disconnected, preventing detection of Hazardous Situation. (Source: IEC 62366 [37], Section C.3).*

Example 2: *Contrary to the indications in the accompanying documentation, a medical device is not sterilized prior to implantation. (Source: IEC 62366 [37], Section C.3).*

Reasonably Foreseeable Misuse: Misuse is not Use Error. It is deliberate and well-intentioned. If it is not well-intentioned, then it could be Abnormal use, or Malice. Typically, off-label use of a medical device/drug for the Benefit of patients is seen is foreseeable misuse.

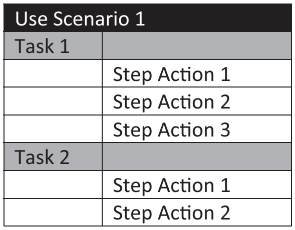
Example: *it has become routine to send patients home with intravenous (IV) infusion pumps. These pumps were originally designed for use in hospitals by trained medical professionals. The manufacturer of a new infusion pump can reasonably foresee that the new infusion pump will be misused, based on the experience with similar products.*

Malice: Use of a device with the intention to Harm the patient or damage the device.

Use Scenario: [19] Section 3.22 "specific sequence of tasks performed by a specific user in a specific use environment and any resulting response of the medical device."

A Use Scenario describes the interaction of a user with the device to achieve a desired outcome.

A Use-Scenario is comprised of one or more Tasks. Each Task is comprised of one or more Step Actions (user interactions). Fig. 33 illustrates this taxonomy.



Use Scenario 1	
Task 1	
	Step Action 1
	Step Action 2
	Step Action 3
Task 2	
	Step Action 1
	Step Action 2

Figure 33 Taxonomy of User Actions.

Tip Use a verb or action phrase for Use-Scenario titles, Tasks, and Step Actions. Examples: check status; deliver shock; remove pad from package.

14.8.2 Use Specification vs. Intended Use

ISO 14971 [1] defines Intended Use and Intended Purpose as "use for which a product, process or service is intended according to the specifications, instructions and information provided by the manufacturer."

IEC 62366 [19] defines Use Specification as "summary of the important characteristics related to the context of use of the medical device

> Note 1: the intended medical Indication, patient population, part of the body or type of tissue interacted with, user profile, use environment, and operating principle are typical elements of the use specification.
> Note 2: the summary of the medical device use specification is referred to by some authorities having jurisdiction as the 'statement of intended use.'
> Note 3 to entry: the use specification is an input to determining the Intended Use of ISO 14971:2019."

While 'Intended Use' and 'Use Specification' are similar, they are not the same thing. Intended Use is what the manufacturer states is the purpose of the device, and how it should be used. Use Specification is more about the context of use of the medical device, which from a usability engineering perspective includes:

- Intended user
- Intended use environment

as well as the Intended Use of the device.

14.8.3 UMFMEA Workflow

In the following sections the workflow for UMFMEA is described. The workflow corresponds to the template that is provided in Appendix B — Templates.

14.8.3.1 Set Scope

Explicitly define the scope of analysis. For UMFMEA the scope should include the System and the users who would interact with the System, e.g., patient, physician, or service personnel. External influences on the scope of analysis are considered as causes to Failure Modes. For example, loud noises, dim ambient lighting, etc.

14.8.3.2 Identify Primary and Secondary Functions

As in the DFMEA and PFMEA, identify the primary and secondary functions of the subject of analysis. Since UMFMEA analyzes the entire System, this step identifies the primary and secondary functions of the medical device. Primary functions are those that achieve the main mission of the System. All other functions are secondary. For example, if a pacemaker logs the history of therapy that it has delivered, the primary function of the pacemaker would be pacing, and the secondary function would be logging therapy history.

14.8.3.3 Analyze

Analysis of the System for use-failures requires knowledge of the System Use-Scenarios and their constituent tasks. A formal usability engineering task analysis is a good basis for the UMFMEA. If a formal task analysis is not available, at a minimum, inventory the Use Scenarios and actors. A graphical representation like Fig. 34 is a handy way to communicate and confer with your team to make sure a complete inventory of the Use Scenarios and actors is achieved.

Next, for each identified Use Scenario, list the Tasks and Step Actions by the Actors. This can be tabular or a graphic flow chart. For each Step Action, hypothesize the ways in which the Step Action could be done incorrectly, and the realistic causes thereof. Consider the distinctions that are described in Section 14.8.1. Use hypotheses such as: user is unable to see/hear, interpret, press, etc. Log this information in the UMFMEA spreadsheet.

List the potential effects of the Failure Mode. Local Effects may not be perceivable from outside the System but create an internal effect within the System. End Effects are observable from outside the System. For a UMFMEA End Effects are the same as System Effects.

List all the existing mitigation that serve to prevent the Failure Mode, in the ‘Existing Mitigations’ column.

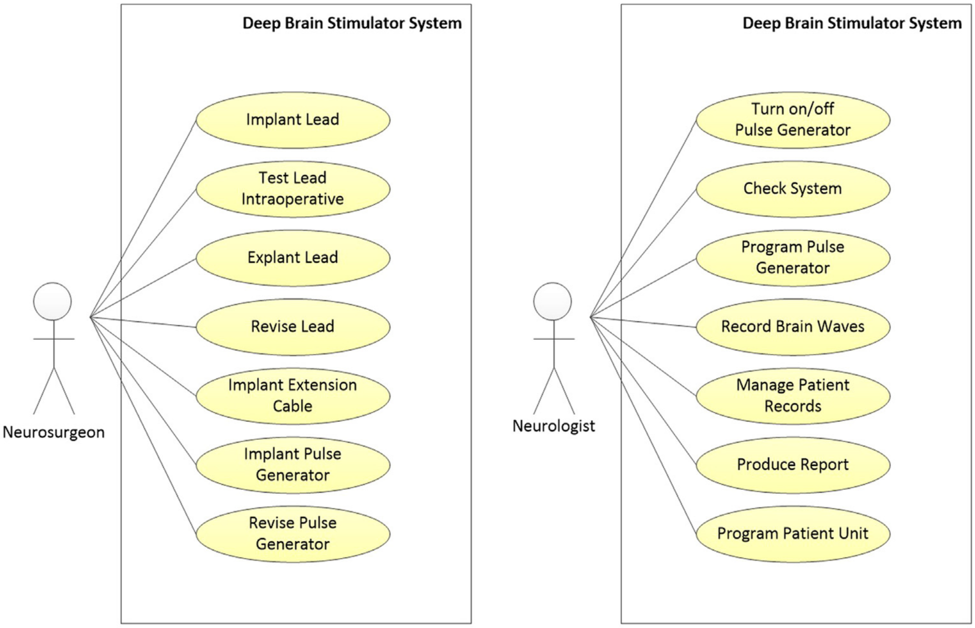


Figure 34 Use-Scenario Inventory.

If the End Effect is a Hazard in the CHL, then the Safety Impact is yes. Else, it is no.

Assign rankings. Tables 14–16 offer suggestions for rankings of Severity, Occurrence and Detectability respectively. Remember that the rankings are inclusive of all the existing mitigations. Let's examine each factor.

Severity is the significance of the worst reasonable consequence of the End Effect at the System level. Severity ranking definitions are different depending on whether the End Effect has a safety impact or not. For End Effects that do not have a safety impact, use the left column in Table 14, and for those with a safety impact use the right column.

To rank the Severity of End Effects without a safety impact, it is helpful to know the primary and secondary functions of the item under analysis. Use the information from Section 14.8.3.2 to determine the primary and secondary functions. For example, if a Failure Mode causes the complete loss of the primary functions, using the qualitative criteria in Table 14, the Severity ranking would be 4.

To rank the Severity of an End Effect that has a safety impact, consider the impact on the patient/user. If you use a single-value Severity ranking for Harms, then match that ranking to the right column of Table 14 and choose the ranking number.

In the BXM method there are 5 classes of Harm Severity. As described in the DFMEA Section 14.6.1, choose the most probable Severity class from the HAL.

Table 14 Definitions of UMFMEA Severity Ratings.

Severity Criteria (Sev)		
Rank	Severity Description (No Safety Impact)	Severity Description (Safety Impact)
5	Described Failure Mode will cause immediate failure of the Subject. (Total loss of all functions – primary and secondary)	**Fatal** – Impact of the end-effect at the System level can be death
4	Described Failure Mode will severely impact Subject functionality | Complete loss of primary functions. May also lose secondary functions.	**Critical** – Impact of the end-effect at the System level can be permanent impairment or irreversible injury
3	Described Failure Mode will reduce Subject functionality. (Partial loss of primary functions | Complete loss of secondary functions)	**Major** – Impact of the end-effect at the System level can be injury or impairment requiring medical or surgical intervention
2	Described Failure Mode will have temporal or self-restoring impact on functionality | partial loss of secondary functions	**Minor** – Impact of the end-effect at the System level can be temporary injury or impairment not requiring medical or surgical intervention
1	Described component failure will have no impact on functionality | Inconvenience to the user	**Negligible** – Impact of the end-effect at the System level can be at most an inconvenience, or temporary discomfort

Example: Let's say a Step Action is to examine the packaging of an implantable device for damage. Let's say the user fails to notice a damage to the sterile seal of the packaging of an implantable device. This could result in the implantation of an unsterile device, which could lead to infection. In the example HAL seen in Fig. 15, the infection outcome with the highest probability is Critical (45.0%). Therefore, in this example you would choose the Severity ranking of 4, Critical.

Occurrence ranking signifies the estimate of the highest likelihood of occurrence of a use failure. The Occ ranking is a measure of the effectiveness of the prevention mitigations. The 1–5 range is only a relative ranking of the Occurrence. The Standard [19] indicates that quantitative estimation of Occurrence should not be made unless you have data to support your estimation. In the absence of data, you can make qualitative estimates of the potential for a use failure based on the descriptions in Table 15.

Remember that this ranking is used only for criticality determination and the prioritization of resources on mitigating Failure Modes. The safety risk of Hazards is computed in the RACT and is a different matter.

Table 15 Definitions of UMFMEA Occurrence Ratings.

Probability of Occurrence Criteria (Occ)		
Category	**Rank**	**Qualitative Criteria**
Frequent	5	The occurrence is frequent. Experienced by almost every user.
Probable	4	The occurrence is probable. Experienced by most users.
Occasional	3	The occurrence is occasional. Experienced by some users.
Remote	2	The occurrence is remote. Experienced by few users.
Improbable	1	The occurrence is improbable. Has not been observed; not expected to be experienced by any user.

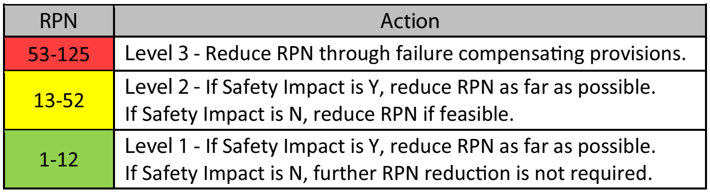
Detectability, is the likelihood of detection of the use failure. Detection may occur anywhere in the causal chain, from the initial Use Error, to an intermediate effect, to the final End Effect at the System level. Use Table 16 to select a ranking for Detectability. **Important: consider the ability of the user to take countermeasures to prevent the Hazardous Situation, or take actions to minimize Harm Severity**. Detection of the End Effect where there is nothing that the user can do to minimize the risk of Harm is of little value. In such cases, choose a ranking of 5.

Table 16 Definitions of UMFMEA Detectability Ratings.

Detection Criteria (Det)		
Category	**Rank**	**Qualitative Criteria**
Undetectable	5	Effect is not immediately visible or knowable | Countermeasures not possible
Low	4	Effect can be visible or knowable only with expert investigation using specialized equipment | Countermeasures are unlikely
Moderate	3	Effect can be visible or knowable with the moderate effort by user | Countermeasures are probable
High	2	Highly Detectable — Effect can be visible or knowable with simple action by user, from the information provided by the system itself | Countermeasures are likely
Almost Certain	1	Almost certain detection — Effect is clearly visible or knowable to user without any further action by user | Countermeasures are certain

RPN is a measure of criticality of a Failure Mode. RPN is the product of the rankings of Severity, Occurrence and Detection. This number is used to decide the degree of failure compensation that must be exercised. Table 17 offers a suggested stratification of compensating actions based on the criticality of the Failure Mode. The boundaries in Table 17 are selected at 12 and 52. But it is up to the manufacturer to decide where to draw the boundaries. Table 17 says that for the highest segment of RPN ratings, Level 3, the RPN must be reduced.

Table 17 UMFMEA RPN Table.



RPN	Action
53-125	Level 3 - Reduce RPN through failure compensating provisions.
13-52	Level 2 - If Safety Impact is Y, reduce RPN as far as possible. If Safety Impact is N, reduce RPN if feasible.
1-12	Level 1 - If Safety Impact is Y, reduce RPN as far as possible. If Safety Impact is N, further RPN reduction is not required.

For Level 2, RPN should be reduced as far as possible for safety-related Failure Modes. But for non-safety related Failure Modes, the decision as to how far to reduce the RPN is a business decision and depends on the feasibility of the actions needed to reduce the RPN.

For Level 1, for safety-related Failure Modes the RPN must be reduced as far as possible, therefore the treatment of RPN is the same as Level 2. However, for non-safety related Failure Modes, further action is not required.

Note that 'As Far As Possible' in Table 17 is inspired by EU MDR [2], and is one of the options for risk reduction that is offered by ISO 14971 [1]. You may adapt the action strategy to suit your QMS.

Reduction of criticality of Failure Modes is achieved via mitigations. Mitigations can eliminate the Failure Mode completely, reduce the likelihood of the Failure Mode, improve detectability, or diminish the Severity of the End Effect of the Failure Mode. Examples of mitigations:

- Use of larger fonts and higher contrast
- Design of the system to suit the 5th to 95th percentile of the user population
- Redesign of a Task to eliminate an error-prone Step Action

Mitigations should be clearly and specifically described such that they can be verified.

If it is decided to perform additional mitigations, list them in the 'Additional Mitigations' column, and re-estimate the rankings. The final rankings are inclusive of all mitigations, existing and additional.

It is possible that the safety impact of a Failure Mode may be Y in the initial analysis but becomes N due to the additional mitigations.

The Remarks column can be used to document rationales for the choices of rankings, or why further mitigations are not done for a Failure Mode with safety impact, or anything else that could help future reviewers of the UMFMEA gain better understanding of the analysis.

14.9 P-DIAGRAM

P-Diagrams, or Parameter Diagrams, are another technique that can be used at the service of Risk Management. P-Diagrams model a system and its behavior under various conditions. P-Diagrams can help with the development of FMEAs. The Error States can help with the identification of the Failure Modes in an FMEA, and Noise Factors can help identify the Causes of the Failure Modes in the FMEA.

Fig. 35 shows the construct of a P-Diagram. The main blocks in this diagram are the Input Signals, the System, the Control Factors, the Noise Factors, the Ideal Function, and the Error States.

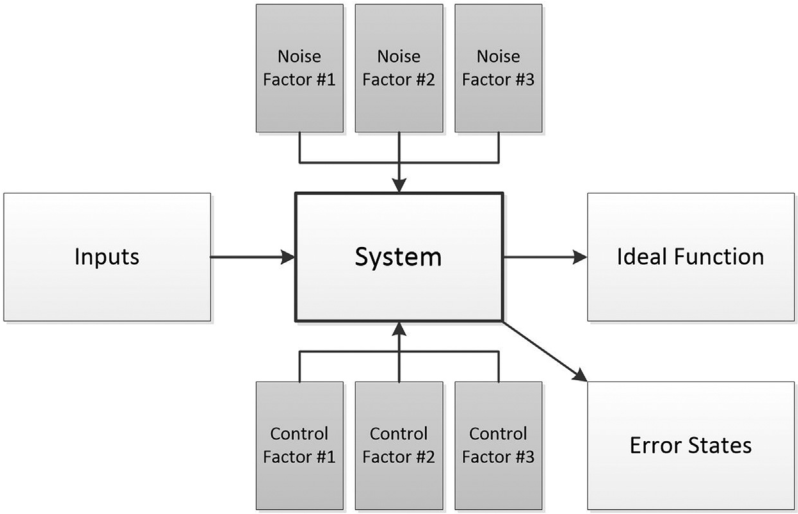


Figure 35 P-Diagram.

14.9.1 Input Signals

Input signals describe the items that the System needs to fulfill its objective. Examples of Input Signals: energy, data, materials.

14.9.2 System

The System is the entity that processes the Inputs, under the Control Factors and the Noise Factors, and delivers the output.

14.9.3 Control Factors

Control Factors are the factors over which we have control and can be changed as desired to influence the System function. Examples: quantity of input materials, temperature of oven, duration of curing, etc.

14.9.4 Noise Factors

Noise Factors are things that can influence the output of the System, but over which we do not have control. Examples: piece-to-piece variation, unintended customer usage, environmental conditions.

Noise Factors are typically grouped in 5 categories:

- Piece-to-piece variation
- Change over time/use
- Customer usage/duty cycle
- External Environment
- System interactions with other systems

14.9.5 Ideal Function

This is the intended output of the System – the way the designers designed the System. Naturally, things don't always work the way you want them to, as Noise Factors play a role.

14.9.6 Error States

These are the unintended outputs of the System. They are the result of Noise Factors' influence on the operation of the System.

14.9.7 Workflow

Use the following steps to create a P-Diagram

1. Identify the intended function of the System under analysis, and the expected Outputs
2. Identify the Input Signals – what are the inputs to the System? The things that the System needs in order to produce its output: the Ideal Function.
3. Identify the Error States – what are the ways in which the System can produce an output that is different from what is expected?
4. Identify the Noise Factors – what are the inputs, or influencers to the System function, over which you don't have control?

5. Identify the Control Factors – what are the inputs, or influencers to the System function, over which you do have control?

P-Diagram analysis provides a systematic way to consider a function's Error States and Noise Factors, as well as the methods that can be used to control them.

As in FMEA, the level of granularity of analysis is the analyst's choice. At the highest level 'System' would be the entire medical device system. Or, 'System' could be subsystems, or lower-level components of the System.

P-diagram analysis can help you identify Hazards and their Causes. By examining the Noise Factors, you can create a causal chain that would explain how a hazardous output could be realized. You will likely find overlaps between FMEA and FTA findings and P-Diagram analysis. Ultimately it is your choice as to how many techniques to use. While extra analyses consume more resources, they also reduce the likelihood of missing some Hazards and their causal chains.

14.10 COMPARISON OF FTA, FMEA

FTA and FMEA are both useful and important analytical techniques in risk management. They both play a role, and it is best if they are used in a complementary fashion. As each technique has strengths and weaknesses, the combinatorial application leverages the best that each technique has to offer.

FTA is a top-down deductive analytical technique that starts with the Top Event, e.g., a Hazardous Situation, and works backwards towards the root cause(s). It seeks to answer the question: 'How can this Hazardous Situation occur?'

FMEA is a bottom-up inductive analytical technique that starts at the basic elemental level and works forward toward the Top Event to answer the question: 'What is the End Effect of the failure of the item in question?'

The FTA is more suitable for:

- Early in the product development process, when only high-level knowledge of the device is available.
- When there are few Top Events of interest, e.g., for derivative products when the predicate device is already well-analyzed and understood, and the derivative only adds a few new Top Events.
- When a Top Event can be caused by multiple initiating Causes, or where there are many interactions and relationships among the components.
- Detection of Common Cause Failures.
- Systems with redundancies in the design.

The FMEA is more suitable for:

- Systems that are novel, or complex, and not well-understood.
- When there are a large number of Top Events that can result from bottom events.
- Where occurrence of the Top Events do not require multiple faults.
- When there is a need for fail-safe operation.

First-order cut sets in the FTA should also appear in FMEAs as single-point failures that can result in the Top Event.

Tip Use FTA to prioritize FMEA work for complex products. FTA can more efficiently identify safety-critical parts of the System. Use this knowledge to prioritize the FMEA work.

CHAPTER 15

Software Risk Management

Abstract

Software can have a strong influence on the safety of medical devices. This includes new software as well as legacy software, and SOUP. IEC 62304 offers guidance and strategies that support the creation of safer software. These strategies in concert with ISO 14971 allow management of risks due to software failures. SFMEA as one of the tools of software risk management is expounded in this chapter, and special tips are offered for successful development of safety-critical medical software.

Keywords: Software risk management; software FMEA; SFMEA; legacy software; SOUP; software safety classification

Software can have a strong influence on the safety of medical devices. Software can be viewed either as a component of a medical device, an accessory to another device, or as a medical device in and of itself (SaMD). IMDRF [38] defines SaMD as software intended to be used for one or more medical purposes that performs these purposes without being part of a hardware medical device. As a component of a medical device, software actuates the hardware. A SaMD, on the other hand, provides information that is used for treatment, diagnosis, or clinical management of patients.

The *21st Century Cures Act*, which was signed into US law in 2016 helped clarify which kind of software is not a medical device.

a. Software used for administrative support purposes (e.g., billing, scheduling, admissions, inventory management)
b. Software intended "for maintaining or encouraging a healthy lifestyle and is unrelated to the diagnosis, cure, mitigation, prevention, or treatment of a disease or condition"
c. Software that serves as electronic patient records if created by a healthcare provider as equivalent of paper medical record, and not intended to interpret or analyze patient data for diagnostics or treatment
d. Software used to transfer, store, convert, or display clinical data, including laboratory test results, and findings by a healthcare professional
e. Software which provides clinical decision support, unless it:
- performs analysis of medical images, IVD data, or "signals from a signal acquisition system" (sensor data); or
- performs diagnostics, or provides treatment recommendations which the healthcare professional cannot independently verify.

DOI: https://doi.org/10.1016/B978-0-323-85755-0.00015-1

Software for complex Systems is difficult to correctly specify, implement, and verify. Errors in software requirements specification, and software design and implementation are the main contributors of software-caused System Hazards. Though deterministic, software is not necessarily predictable for complex Systems. This makes risk management of software a particularly difficult challenge. The most effective way to manage risks due to software is to consider the role of software before System design is completed. IEC 62304 [10] suggests three major principles to promote software safety:

- Risk management
- Quality management
- Software engineering

Further, the Standard IEC 62304 [10] provides a framework for the safe design and maintenance of medical device software including:

1. Software risk management
2. Software configuration management
3. Software problem resolution process

Software risk management is discussed in the subsections below. Software configuration management, and problem-resolution process are/should be part of the Quality system and are not discussed in this book.

15.1 SOFTWARE TYPES

With respect to functionality in medical devices, three types of software can be identified:

1. Software that provides a clinical function
2. Software that is used as a Risk Control measure
    a. For hardware failures
    b. For software failures
    c. For Use Errors
3. Other software
    a. Software whose failure could create a safety impact
    b. Software whose failure would not create a safety impact

Of the above types of software only 3.b is not safety-related, and the rest should be included in the software risk management process. According to IMDRF [38] software that is used to make or maintain a device (testing, source code management, servicing, etc.) is not considered software with a medical purpose.

As depicted in Fig. 36, Hazards are the consequence of a chain of events. Exposure to Hazards can cause Harm. Since exposure to software cannot cause Harm, software

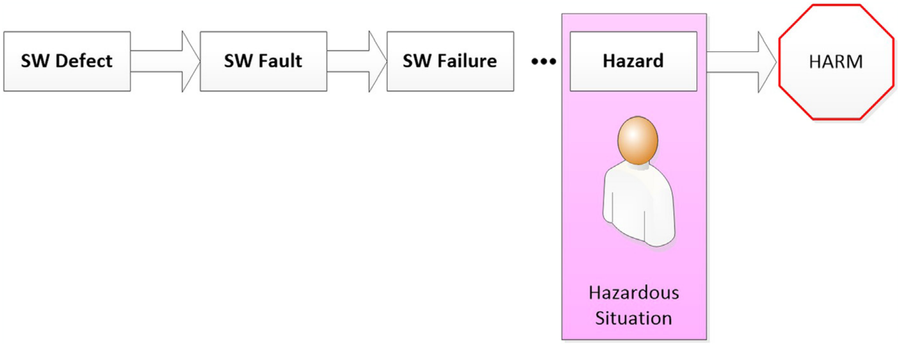


Figure 36 Contribution of Software to Hazards.

itself is not a Hazard. But software failures can cause Hazards in the System context. To determine the risks due to software, we'll need to identify the Harms that could result from software failures.

Understanding the contribution of software to Hazards and Harms can be achieved via top-down System analyses, e.g., Fault Tree Analysis. This requires knowledge of the System architecture, Indication for use, Intended Use, and the context within which the System operates. Starting with potential Harms of the System, deductively analyze the pathways which could lead to those Harms. If no pathway contains software, you can conclude that software in that System is not a contributor to Harms.

If it is established that software is a contributor to Hazards and device risks, it is beneficial to analyze the software architecture to determine the roles and contributions of the various Software Items to risk. For simple devices, the manufacturer may choose to treat the software as a black box and bypass the software architectural analysis.

Before we proceed, it is important to understand some relevant vocabulary. Three important terms are:

Software System	An integrated collection of Software Items organized to accomplish a specific function or set of functions [10]
Software Unit	Software Item that is not subdivided into other items [10]
Software Item	Any identifiable part of a computer program, i.e., source code, object code, control code, control data, or a collection of these items [10] All levels of software composition can be called Software Item, including the top-level: Software System, and the bottom-level: Software Unit.

The analysis of software at the software-architectural level enables us to plan architectural-level Risk Controls, such as introducing protective Risk Control measures that are external to the software. Beyond introduction of architectural Risk Control measures, applying the methods that are prescribed in IEC 62304 [10] provides process-based Risk Control measures that can reduce the probability of software failures.

IEC 62304 [10] B.7 says, "Software risk management is a part of the overall medical device risk management and cannot be adequately addressed in isolation." Since software is not a Hazard by itself, it doesn't have risk. Risks of software failures can only be estimated in the context of the System.

Software risk in a System is the aggregation of the risks of all the Hazards that are caused by software failures.

Software safety must be approached within a multi-disciplinary context including: System design, software engineering, mechanical and electrical design, and usability engineering.

Before delving deeper into software risk management, certain key terms need to be defined.

Software Defect: An error in design/implementation of the software. Also known as a "bug."

Software Fault: A software condition that causes the software not to perform as intended.

Software Failure: A software condition that causes the System not to perform according to its specification. (System here means the medical device.)

The following clarifications should facilitate a deeper understanding of the above terms:

- A Software Defect does not necessarily cause a Software Fault
  i.e., software with known bugs can still perform as intended
- A Software Fault does not necessarily cause a Software Failure
  i.e., software may not be performing as intended, but the System could still work as intended
- A Software Failure does not necessarily create a System Hazard
  i.e., Software Failure may cause a system malfunction, which is not unsafe
- Software could fault in the absence of Software Defects
  e.g., due to bad software requirements, flawlessly designed and coded software my fail to perform as intended
- Software could fail in the absence of Software Faults
  e.g., due to bad System requirements, flawless software may fail to enable the system to deliver its intended therapy

Fig. 37 shows the chain of software events that could lead into a System Hazard. The dotted arrows imply that there may be intervening events between software failure and System Hazards.

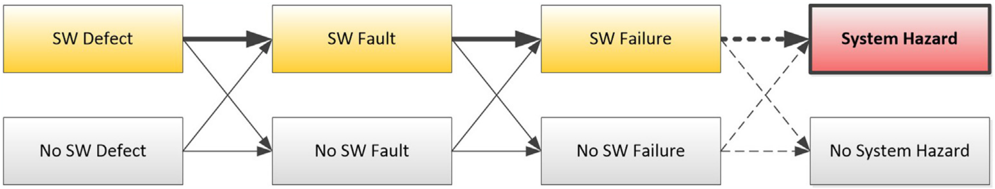


Figure 37 Software Chain of Events to System Hazards.

In the context of software risk management, in this book we will only consider risks due to software failures. In other words, the progression depicted by the dark arrows in Fig. 37 is considered because that is where software risk management can have an influence. The light arrows indicate either no problems with software, or no System Hazards, and are thus not considered in software risk management. As shown in Fig. 37, even when the software works perfectly according to its specification, the System can present safety risks. Those risks are managed in the System risk management per ISO 14971 [1].

In the case of SaMD, software is the System (medical device). Therefore, Software Fault is equivalent to Software Failure. As stated above, software is not a Hazard in itself. Therefore, software failure in a SaMD can at most, create a cause for a Hazard, not a Hazard itself. For example, an error in a radiological image analysis software system (a SaMD) that gives a false-negative on a cancerous tumor, could result in a patient not receiving cancer therapy. Exposure to the erroneous diagnosis doesn't cause Harm. But the erroneous diagnosis could be the cause to the subsequent inappropriate therapy.

Software does not wear out, corrode, or fatigue. Most software failures are the result of software requirements or design errors, not coding errors, and tend to remain latent until the right conditions manifest them. No amount of rigor in software design or implementation would be able to correct for erroneous software requirements. Defects in software requirements can be detected by the use of tools such as simulation and modeling, and methods such as structured peer reviews. Software Defects are systemic, not random in nature.

Because software and digital systems are not continuous, as opposed to analog systems, boundary testing is insufficient. Complete testing of software requires testing of all possible states of the digital system. In even a moderately complex software system, the number of possible states would be astronomically large such that it would take thousands of years to test all possible states. It is, therefore, infeasible to completely test complex software. Software testing can catch only a proportion of Software Defects.

The limited human cognitive ability to comprehend complexity, together with the seemingly unlimited ability to introduce complexity in software leaves us with the inevitable fact that some defects will likely remain in the software.

Risk management per ISO 14971 [1] requires planning. Likewise, software risk management requires planning and documentation. The software Risk Management Planning documents can be separate or combined with the System risk management documents.

As in other kinds of risk management, management of software risks entails the identification of Hazards, estimation of risks of the Hazards, control of the risks and evaluation of the risks. In the sections below elements of software risk management, such as software safety classification, software Hazard identification and topics unique to software such as handling of Software of Unknown Provenance (SOUP), are discussed.

15.2 SOFTWARE RISK ANALYSIS

Software Risk Analysis starts with the identification of the intended purpose of the System. Without this knowledge, it is not possible to determine whether a particular Software Failure is hazardous or not. Knowing the intended purpose of the System and the System architecture, it is possible to postulate potential Hazardous Situations and analyze for contributions of the various elements of the Systems, including software. This activity is not truly completed until the software architecture is determined and Software Items are identified. With the knowledge of software architecture, it becomes possible to determine the contribution of individual Software Items to the Hazardous Situations.

Analysis of risk involves the identification of Hazards, and estimation of their risks. As in hardware risk-analysis, in software risk-analysis Hazards must be identified and their risks estimated. In hardware, Hazards are sometimes rooted in physical hardware failures. But software doesn't fail in the same ways as hardware. It doesn't wear out, corrode, or fatigue.

Table B.1 of IEC TR80002-1 [39] offers examples of Causes of Software Faults that could introduce Hazards. The Causes are grouped by functional areas and guiding questions are provided to help the analyst uncover missing or inadequate safety requirements. Table B.2 of [39] identifies examples of Software Failure Causes that can have broad impact on the System operation. Examples: divide by zero, or errant pointers. With these kinds of errors, failures that originate in non-safety-critical Software Items can impact safety-critical Software Items. Table B.2 [39] offers suggestions for verification methods to trap such failure Causes. For these types of Software Failures, requirements-based testing is not very effective.

An analytical technique that can be used to identify software-related Hazards is the Software FMEA (SFMEA). Section 15.3 describes the usage of this technique.

Estimating the risk of a Hazard involves estimating the likelihood of occurrence of the Hazard and the related Hazardous Situation. In the case of software-caused Hazards, IEC 62304 [10] says that there is no consensus on a method to estimate the probability of occurrence of Software Failures and suggests to conservatively set the probability of occurrence of Software Failures to 100%. Ref. [10] continues and suggests focusing on the identification of software-caused Hazards and implementing Risk Control measures, instead of trying to estimate the risk of Software Failures. ISO 14971 [1] Section A.2.5.5 corroborates and suggests listing such Hazardous Situations separately and focusing on reducing Risks.

To get some sense of the relative Risks from software-caused Hazards, IEC 62304 [10] suggests relying on the Severity of Harms alone. However, IEC 62304 [10] acknowledges that it may be possible to quantitatively estimate the probability of occurrence of Software Failures for legacy software, based on the usage of legacy software and examination of Post-Production data.

Medical device software can be classified in two categories: new software, or legacy software. Legacy software is software that has been in use in the field and for which Post-Production history data may be available. New software is software that has not been released for use in the field yet and has no Post-Production history.

The Standard, IEC 62304 [10] recognizes that application of appropriate levels of rigor to software development does reduce the probability of failure of Software Items, presumably due to detection and elimination of Software Defects. Using these preventive measures is wise but does not yield the risk of Harm due to Software Failures. Without this knowledge it is not possible to include the software-induced risks in the quantitative Overall Residual Risk calculations.

It should be understood that setting P(Software Failure)=1 doesn't necessarily mean that P1=100%. It means: if software is an element in the causal chain that leads to the Hazardous Situation, set the probability of Software Failure to 100%.

$$\text{Risk} = \text{P(Hazardous Situation)} \times \text{P(Harm)} = \text{P1} \times \text{P2}$$

$$\text{P1} = \text{P(Hazardous Situation)} = \text{P(Hazard)} \times \text{P(Exposure)}$$

$$\text{P(Hazard)} = \text{P(Software Failure)} \times \text{P(additional intervening events)}$$

Using the above equations, risk of Software Failures can be computed. If P(Software Failure) is set to 1, then P(Hazard)=P(additional intervening events).

It is understood that this method of risk computation yields an exaggerated estimation of software risk, because P(Software Failure) is conservatively set to 1.

15.2.1 Does Software Fail 100% of the Time?

The Standard [10] says that there is no consensus on a method to estimate the probability of occurrence of Software Failures and suggests to conservatively set the probability of occurrence of Software Failure to 100%.

A closer examination of this statement reveals more depth. Consider Fig. 37, and the definitions provided in Section 15.1 for Software Defect, Software Fault, and Software Failure. For each failure, fault, or defect to manifest, proper conditions are necessary.

- Software Failures require the proper conditions and potentially a Software Fault
- Software Faults require the proper conditions and potentially a Software Defect
- Software Defects, which we presume to be present, require the proper conditions to manifest

We can deduce that Software Failures do not manifest unless the proper conditions are present. These conditions may be internal to software or external. Clearly, the proper conditions are not always present otherwise software would fail 100% of the time, which is empirically not true. So, even though the Standard [10] suggests to conservatively set the probability of occurrence of Software Failure to 1, a more reasonable approach would be to set to 1: the probability of existence of Software Defects or bad software/system requirements, and estimate the probability of occurrence of the proper conditions to manifest a Software Defect, or a Software Fault, or a Software Failure. This would allow the use of a probability number less than 100% for Software Failures, which is more in line with the reality of life.

15.3 SOFTWARE FMEA (SFMEA)

FMEAs are a common and ubiquitous technique for Hazard Analysis. SFMEA is a variation of the DFMEA. When used for software Hazard Analysis, FMEAs are applied in a slightly different manner than in hardware FMEAs. Software FMEAs are applied to software architectural elements, or Software Items. This requires the knowledge of the software architecture and inputs to the software.

Systemic Causes/mechanisms of Software Failure such as design or implementation errors, or hardware anomalies, like bit flips are analogous to Common-Cause Failures in hardware and should be mitigated globally for the whole software system, not cited for every row of the SFMEA.

15.3.1 SFMEA Workflow

The following explanation of the SFMEA is based on the SFMEA template that is provided in Appendix B – Templates.

Entries in the 'Item' column are the elements within the scope of analysis. 'Source' column captures where the Failure Mode was identified. In hierarchical multi-level FMEAs, this refers to the underlying FMEAs whose End Effects were rolled up to the current SFMEA. In a single-level SFMEA, or in the lowest level of a hierarchical multi-level FMEA, this column would be blank.

The item's function is derived from the requirements of the item. Use active verb and noun constructs and keep in mind any necessary conditions to achieve the function.

The entries in the 'Failure Mode' column of the FMEA would be the answers to the question: 'In what ways can this Software Item fail to perform its intended function?' One way to do this is to list the requirements of the Software Item and consider how not meeting each requirement affects the Software Item's intended function.

Software Failure Modes can have direct and/or indirect Causes. Direct Causes are local to the Software Item at hand, and do not necessarily affect other Software Items. Examples: incorrectly implemented algorithms, errors in input processing, and errors in output processing of the Software Item. Indirect Causes include: stack overflow, uninitialized pointers, and race conditions. Indirect Causes are more unpredictable than direct Causes. Other indirect Causes of Software Failures are: bit flips, low-power condition, or software sources such as operating systems, libraries, and SOUP.

Unlike DFMEA, SFMEA entries in the column 'Causes/Mechanisms of Failure' would not be things like aging, fatigue, or wear out. Items that go in this column are external factors, or systemic Causes. Since the object of the analysis is a Software Item, the question would be: 'What factors could cause this Software Item not to perform its function?' For example, consider a Software Item that is supposed to pressurize a tank to 10 psi and a pressure sensor provides the tank pressure as input to the Software Item. If the pressure sensor input to the Software Item is incorrect for any reason, the Software Item would fail to meet its function.

The entries in the 'End Effect' column would be the consequences of the Software Item's Failure Mode at the boundary of analysis. Boundary of analysis is chosen by the analyst, and could be for example, a software subsystem, or the entire software system. If the scope of analysis is the software system (as a component of the medical device), then the question is: 'How would the Failure Mode of the Software Item in question affect the behavior of the software system?' System Effect is the impact of the software Failure Mode on the medical device. Local Effects are not visible from outside the boundary of analysis but are noteworthy because they may cascade into other End Effects. It is possible that there would not be any Local Effect.

Determination of whether the Software Failure Mode has a Safety Impact can only be made at the System (medical device) level. Examination of the System Effect is helpful in the determination of the Safety Impact. If the System Effect is unknown, in the hierarchical multi-level FMEAs the Safety Impact can be known after the integration of the FMEAs into the System DFMEA. It may be possible to make some estimations of the Safety Impact prior to the integration of multi-level FMEAs. For example, if it is certain that the Failure Mode would lead to one of the Hazards in the CHL, it would be a good guess that the Safety Impact will end up being Y. Another way to estimate the Safety Impact of a Failure Mode is to determine whether it would violate a System requirement which is tagged as "Safety."

If the Safety Impact of the Failure Mode cannot be determined in advance, you can set the Safety Impact to N as a generic setting and use the 'No-Safety Impact' column in the Ratings tab of the template to determine the Severity ranking. As the SFMEA is a living process and goes through an iterative process, when the FMEAs are rolled up to the System DFMEA, it will become apparent whether a given Failure Mode links up to any Hazards. After the integration of the FMEAs and creation of the System DFMEA, a cross-check is done to ensure consistency of Safety Impact ratings. Any End Effect that traces up to a Hazard must have a Y in the Safety Impact column.

Cite all the existing mitigations in the 'Existing Mitigations' columns. Systemic Causes should be universally mitigated, and not repeated in every row. When estimating the rankings, assume the existing mitigations are implemented and effective.

There are three factors that are typically used to estimate the criticality of a Failure Mode: Severity, Occurrence, and Detectability.

For Failure Modes that do not have a safety impact, Severity is the significance of the worst reasonable consequence of the End Effect at the boundary of analysis. Severity Ranking definitions are different depending on whether the End Effect has a safety impact or not. For End Effects that do not have a safety impact, use the left column in Table 18, and for those with a safety impact use the right column.

IEC 62304 [10] Annex B, Section 4.4 states that unless a quantitative estimation of the probability of Software Failure is done, the probability for Software Failure should be presumed to be 1. This is true for systemic failures. However, in the SFMEA we consider contribution of external factors to Software Failures. Therefore, the Occ column would include the likelihood that the Software Item could fail due to external factors. In the case of legacy software with available data for the probability of systemic

Table 18 Definitions of SFMEA Severity Ratings

Severity Criteria (Sev)		
Rank	Severity Description (No Safety Impact)	Severity Description (Safety Impact)
5	Described Failure Mode will cause immediate failure of the Subject. (Total loss of all functions — primary and secondary)	**Fatal** — Impact of the end-effect at the System level can be death
4	Described Failure Mode will severely impact Subject functionality | Complete loss of primary functions. May also lose secondary functions.	**Critical** — Impact of the end-effect at the System level can be permanent impairment or irreversible injury
3	Described Failure Mode will reduce Subject functionality. (Partial loss of primary functions | Complete loss of secondary functions)	**Major** — Impact of the end-effect at the System level can be injury or impairment requiring medical or surgical intervention
2	Described Failure Mode will have temporal or self-restoring impact on functionality | Partial loss of secondary functions	**Minor** — Impact of the end-effect at the System level can be temporary injury or impairment not requiring medical or surgical intervention
1	Described component failure will have no impact on functionality | Inconvenience to the user	**Negligible** — Impact of the end-effect at the System level can be at most an inconvenience, or temporary discomfort

Software Failure, Occ would compound the likelihood of Software Failure with the likelihood of the external factors. Let's say for example that historical data show that legacy software fails at a rate of 0.01% per 10,000 hours of operation. In the tank pressurization example above, if legacy data show that the pressure sensor fails at a rate of 0.02% per 10,000 hours of operation, then the likelihood Software Failure due to a systemic failure OR a sensor failure would be 0.03% per 10,000 hours of operation.

Alternatively, IEC 62304 [10] Section B.4.3 states that "Subjective rankings of probability can also be assigned based on clinical knowledge to distinguish failures that a clinician would be likely to detect from those that would not be detected and would be more likely to cause Harm." So, a subjective ranking by experts with clinical knowledge is also feasible.

If Occurrence is based only on Software Failure rate, and there is no available data on Software Failure rate, then leave the Occ rating blank. Otherwise, use the qualitative, or quantitative guidelines in Table 19 to estimate a ranking for Occ. The Occ rating is a measure of the effectiveness of the prevention mitigations. The 1—5 ranking is only a relative ranking of the Occurrence and may not reflect the actual occurrence probability of the Failure Mode.

Table 19 Definitions of SFMEA Occurrence Ratings

Probability of Occurrence Criteria (Occ)			
Category	**Rank**	**Qualitative Criteria**	**Quantitative Criteria**
Frequent	5	The occurrence is frequent. Failure may be almost certain | constant failure.	$\geq 10^{-3}$
Probable	4	The occurrence is probable. Failure may be likely | repeated failures are expected.	$<10^{-3}$ and $\geq 10^{-4}$
Occasional	3	The occurrence is occasional. Failures may occur at infrequent intervals.	$<10^{-4}$ and $\geq 10^{-5}$
Remote	2	The occurrence is remote. Failures are seldom expected to occur.	$<10^{-5}$ and $\geq 10^{-6}$
Improbable	1	The occurrence is improbable, e.g., due to low complexity. The failure is not expected to occur.	$<10^{-6}$

Detectability in SFMEA has a similar connotation as in the DFMEA — it is an indication of how likely it is for the End Effect to be detected and countermeasures be taken, external to the boundary of analysis, to minimize the risk of Harm. This concept was elucidated in DFMEA workflow analysis, Section 14.6.1.4. A Software Failure Mode with a safety impact, is of relative lower criticality if it can be externally detected and countermeasures taken to minimize Harm.

Internal detection and mitigations, such as CRC checks and error corrections, are considered part of good design and serve to systemically reduce Occ ranking.

Refer to Table 20 for definitions of detectability rankings. Use quantitative data if available. Otherwise use the qualitative criteria to determine the Detectability rankings.

Similar to DFMEA, an RPN value is computed as the product of Sev, Occ, and Det rankings. Higher RPN indicates higher criticality. This number is used to prioritize the Failure Modes and determine the degree of failure compensation that must be exercised.

Table 21 offers a suggested stratification of compensating actions based on the criticality of the Failure Mode. The boundaries in Table 21 are selected at 12 and 52. But it is up to the manufacturer to decide where to draw the boundaries. Table 21 says that for the highest segment of RPN ratings, Level 3, the RPN must be reduced.

For Level 2, RPN should be reduced as far as possible, for safety-related Failure Modes. But for non-safety related Failure Modes, the decision as to how far to reduce the RPN is a business decision and depends on the feasibility of the actions needed to reduce the RPN.

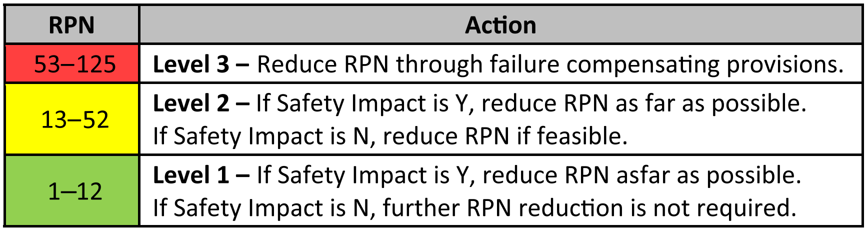
Table 20 SFMEA Detectability Ratings

Detection Criteria (Det)			
Category	**Rank**	**Qualitative Criteria**	**Quantitative Criteria**
Undetectable	5	No detection opportunity | No means for detection | Countermeasures not possible	$<10^{-3}$
Low	4	Opportunity for detection is low | Countermeasures are unlikely	$<10^{-2}$ and $\geq 10^{-3}$
Moderate	3	Opportunity for detection is moderate | Countermeasures are probable	$<10^{-1}$ and $\geq 10^{-2}$
High	2	Opportunity for detection is high | Countermeasures are likely	$<9 \times 10^{-1}$ and $\geq 10^{-1}$
Almost Certain	1	Opportunity for detection is almost certain | Countermeasures are certain	$\geq 9 \times 10^{-1}$

For Level 1, for safety-related Failure Modes the RPN must be reduced as far as possible, therefore the treatment of RPN is the same as for Level 2. However, for non-safety related Failure Modes, further action is not required.

Note that 'As Far As Possible' in Table 21 is inspired by EU MDR [2], and is one of the options for risk reduction that is offered by ISO 14971 [1]. You may adapt the action strategy to suit your QMS.

Table 21 SFMEA RPN Criticality Table



RPN	Action
53–125	**Level 3 –** Reduce RPN through failure compensating provisions.
13–52	**Level 2 –** If Safety Impact is Y, reduce RPN as far as possible. If Safety Impact is N, reduce RPN if feasible.
1–12	**Level 1 –** If Safety Impact is Y, reduce RPN asfar as possible. If Safety Impact is N, further RPN reduction is not required.

If the Occ ranking is unknown and is left blank, then only Severity and Detectability rankings are available to determine the criticality of a Software Failure Mode. In such cases, the template offers a two-dimensional criticality matrix. See Table 22. This criticality matrix also stratifies the criticality of Software Failure Modes into three levels. The disposition of the three levels can follow the same action recommendations as are found in Table 21.

The purpose of SFMEA is the identification of software-caused Hazards, and to prioritize Software Failure Modes for mitigation. General mitigations such as static code

Table 22 SFMEA S-D Criticality Table

Criticality		Severity				
		1	2	3	4	5
Detectability	5	2	2	3	3	3
	4	1	2	2	3	3
	3	1	1	2	2	3
	2	1	1	1	2	3
	1	1	1	1	1	2

checks, structured walkthroughs, and peer reviews benefit all of the software. But for Software Failures with high criticality, additional mitigations, like external hardware or external independent software mechanisms, should be devised.

As with other FMEAs, SFMEAs serve two benefits: safety and reliability. For safety, all we need to determine is whether a Software Item can precipitate a Hazardous Situation. But for reliability, it is of interest to know the areas of software whose failure could impact product performance.

15.4 SOFTWARE SAFETY CLASSIFICATION

Manufacturers of medical devices that include software, including SaMD are required to assign a safety classification to the Software System, based on the potential risk of Harm to people from the Software System, in a worst-case scenario. According to Ref. [10],

"The Software System is software safety class A if:

– the software system cannot contribute to a Hazardous Situation; or
– the Software System can contribute to a Hazardous Situation which does not result in unacceptable risk after consideration of Risk Control measures external to the software system.

The Software System is software safety class B if:

– the software system can contribute to a Hazardous Situation which results in unacceptable risk after consideration of Risk Control measures external to the Software System and the resulting possible Harm is non-serious injury.

The Software System is software safety class C if:

– the Software System can contribute to a Hazardous Situation which results in unacceptable risk after consideration of Risk Control measures external to the Software System and the resulting possible Harm is death or serious injury."

Naturally these definitions necessitate the need to know what 'Serious Injury' is. IEC 62304 [10] Section 3.23 defines Serious Injury as:

> *"injury or illness that:*
>
> ***a**. is life threatening, or*
>
> ***b**. results in permanent impairment of a body function or permanent damage to a body structure, or*
>
> ***c**. necessitates medical or surgical intervention to prevent permanent impairment of a body function or permanent damage to a body structure*
>
> *NOTE Permanent impairment means an irreversible impairment or damage to a body structure or function excluding trivial impairment or damage."*

These definitions are not well aligned with the definitions of seriousness of Harm as offered in ISO/TR 24971 [15] and cited in Table 27. In fact, IEC 62304 [10] states that its software safety classification scheme is not intended to align with the risk classifications of ISO 14971. Being able to correlate the classifications of the two standards is beneficial in that it would facilitate the determination of software safety classes, based on safety risk to patients. One could roughly align the definition of Serious Injury in IEC 62304 [10] with a combination of Critical and Serious from ISO/TR 24971 [15].

All Harms have an associated Hazardous Situation. If the Hazardous Situation can manifest solely due to Software Failure, then P1 for that Hazardous Situation can be presumed to be 100% and risks are equal to the P2 numbers for each Harm Severity class. According to IEC 62304 [10] Section 7.2.2, the safety class of software that is intended to be a Risk Control is based on the risk that the risk-control-measure is controlling. If the software Risk Control is controlling the risk of a Software Item, then its class would be the same as the class of the controlled software. If the software Risk Control is controlling the risk of a hardware item, then use the following algorithm to determine the software safety class for the Risk Control software.

1. What Harm(s) can the hardware-failure cause? Utilizing the HAL, identify the Harm Severity class that has the highest probability. If more than one Harm is identified, choose the highest class among all the Harms.
2. Using Table 23 select the software safety class that correlates to the hardware Severity class from step 1.

Example – Consider Fig. 15. Imagine a hypothetical System in which a single hardware failure could cause both Harm.3 and Harm.4. In this System, there is a software Risk Control for that hardware failure. We want to know the safety class of the software Risk Control. The highest likelihood Harm for Harm.3 is the Minor class. The highest likelihood Harm for Harm.4 is the Critical class. Per step 1 of the algorithm above, we select Critical class. Consulting Table 23, we see that Serious class correlates to Software Safety Class: C.

Table 23 Harm Severity vs. Software Safety Class

Harm Severity Class	Software Safety Class
Fatal	C
Critical	C
Major	C
Minor	B
Negligible	A

By this point, we have determined whether software has a contribution to safety and have assigned a software safety class to it. If the software System performs many tasks, only some of which warrant a safety class of C or B, a manufacturer may desire to focus their engineering resources on those parts of the software system that are responsible for the safety-critical functions. To do this requires the knowledge of the software architecture.

Only after the software architecture is completed, the full set of Software Items, and their contributions to safety can be known. Given the top-down System analysis that was done earlier, we can deduce which Software Items contribute to which Hazardous Situations.

If the software architecture and design strategy allow segregation and discrimination among the Software Items, then a separate safety classification can be assigned to each Software Item within the software System. If this strategy is chosen, segregation must be shown to be effective. That is, a mechanism that adversely affects one Software Item, must not be able to adversely affect another, segregated Software Item. Examples of segregation strategies include use of separate microprocessors, and partitioned memory. The adequacy/strength of the segregation strategy should be based on the level of risk involved.

The manufacturer may find that the cost and complexity of the segregation strategy is too high and instead opt to treat all of the software as the highest software safety class of the Software System.

Fig. 38, which is an adaptation of Figure 3 of IEC 62304 [10], provides a decision process for the determination of the safety risk class of the Software System. In the beginning, all software is assumed to be Class C by default. Following the process in

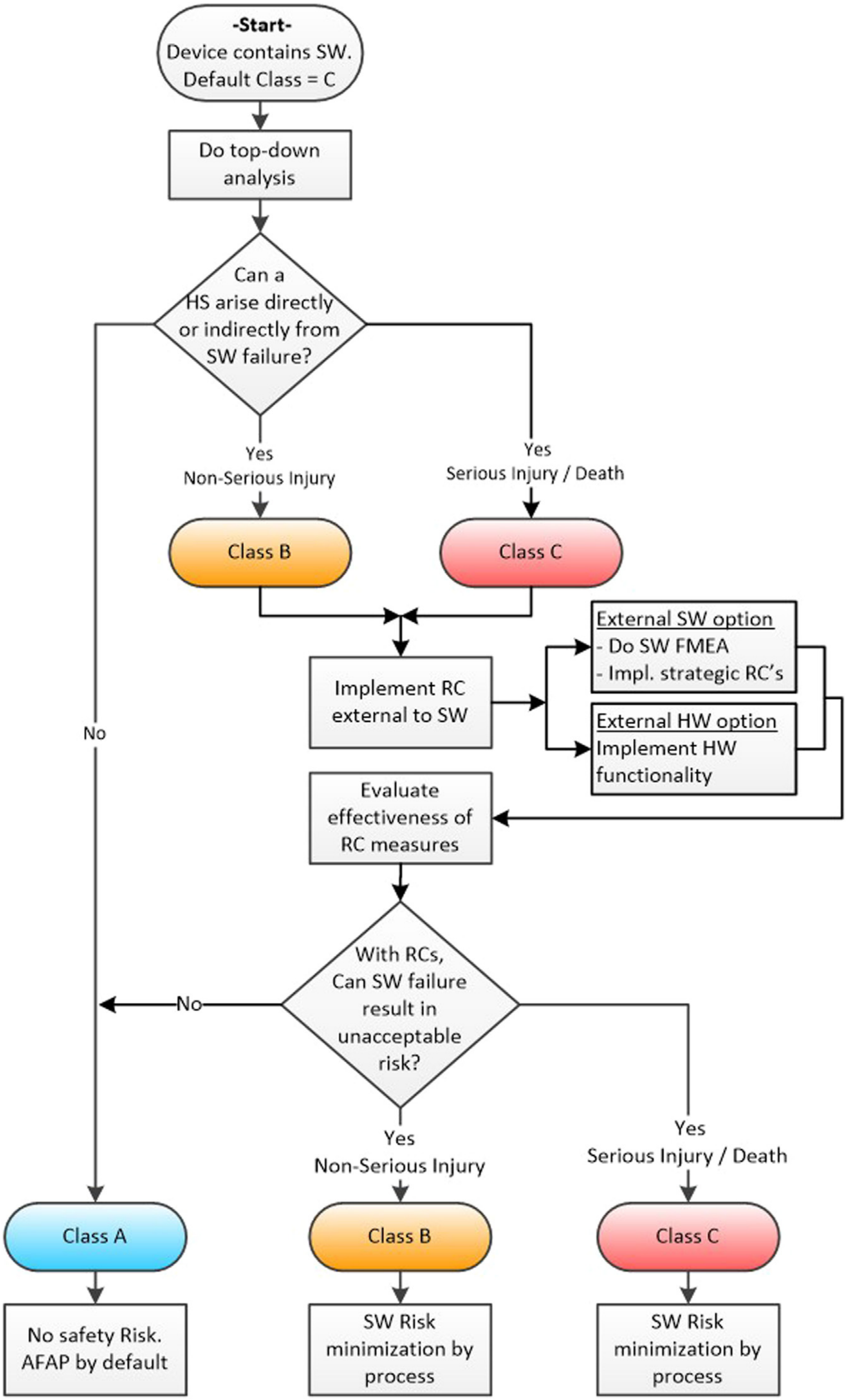

-Start-
Device contains SW.
Default Class = C
Do top-down analysis
Can a HS arise directly or indirectly from SW failure?
Yes
Non-Serious Injury
Yes
Serious Injury / Death
No
Class B
Class C
Implement RC external to SW
External SW option
- Do SW FMEA
- Impl. strategic RC's
External HW option
Implement HW functionality
Evaluate effectiveness of RC measures
With RCs, Can SW failure result in unacceptable risk?
No
Yes
Non-Serious Injury
Yes
Serious Injury / Death
Class A
Class B
Class C
No safety Risk. AFAP by default
SW Risk minimization by process
SW Risk minimization by process

Figure 38 Software Safety Classification Process.

Fig. 38, if software is initially determined to be class B or C, an external Risk Control measure is considered. This external Risk Control may be software or hardware. If the software option is chosen, doing a software FMEA allows the identification of the safety-critical software-items, and thus strategic application of Risk Controls to the highest risk software-items. It is also permissible to treat the software as a black box and apply the software Risk Controls to the entire software-system. If the hardware option is chosen, then appropriate functionality must be designed and implemented to be able to protect against the Software Failure.

After implementation of the external Risk Controls, the effectiveness of the Risk Controls is evaluated to judge the software contribution to overall device risk. If the software is still capable of producing unacceptable levels of risk, then the software development process should follow the different levels of rigor that are defined in IEC 62304 [10].

The software safety classification(s) and their rationale must be documented in the RMF.

Risk Controls serve to prevent or reduce the probability of the occurrence of software-induced Hazardous Situations, or to reduce the Severity of the ensuing Harms.

The Standard [10] clarifies that in addition to external hardware and independent software means, the external Risk Control could be a healthcare procedure, or even other means that can help reduce the contribution of software to the creation of Hazards.

15.5 THE BXM METHOD FOR SOFTWARE RISK ANALYSIS

In Section 15.2, two categories of software were identified: new software and legacy software. Per IEC 62304 [10] there is no consensus on a method to estimate the probability of occurrence of Software Failures in new software. Ref. [10] also acknowledges that for legacy software, it may be possible to quantitatively estimate the probability of occurrence of Software Failures, based on the usage of legacy software and examination of Post-Production data. This creates two distinct pathways for software risk management:

Case 1. where the probability of Software Failure can be estimated – e.g., for legacy software.

Case 2. where the probability of Software Failure cannot be estimated – e.g., for new software, or legacy software for which Post-Production data is unavailable or is of questionable quality.

In this section, the BXM method for software Risk Analysis for each case is laid out.

15.5.1 Case 1 — Probability of Software Failure Is Available

If Post-Production data of adequate quality exist where the manufacturer can derive the probability of occurrence of Software Failures, then the estimation of risk due to Software Failures is possible and is similar to hardware Risk Analysis. That is, after the identification of software-induced Hazards, the probability of occurrence of the Hazard is computed by following the sequence of events as depicted in Fig. 2, where one of the events leading to a Hazard is a Software Failure with a known probability.

Alternatively, using the method described in Section 15.2.1 you may be able to estimate the probability of the manifestation of a Software Failure, and from that derive the P1.

The Risk Estimation follows the quantitative method as described in Section 17.3.

15.5.2 Case 2 — Probability of Software Failure Is Not Available

For Case 2, the probability of occurrence of Software Failure cannot be estimated. As depicted in Fig. 2, in Hazard theory, Software Failure would be an event in the chain of events leading to the realization of the Hazard, and the Hazardous Situation. Without knowing the probability of occurrence of the Software Failure, P1 cannot be estimated, therefore risk cannot be computed. Following the guidance in ISO/TR 24971 Section 5.5.3 [15] focus on preventing the Hazardous Situation from occurring, or preventing the Hazardous Situation leading to Harm. If this is not possible, the aim should be to reduce the Severity of the Harm.

The steps of the BXM method for software risk management for Case 2 are:

1. **Ensure software requirements are correct**. Tools: modeling, simulation, peer reviews.
2. **Define the software architecture, and classify all Software Items** per IEC 62304 [10].
3. **Ensure software implementation is correct**. Tools: structured walkthroughs, peer reviews, testing, automation, use of robust processes and levels of rigor prescribed by IEC 62304 [10] for the different software safety classifications.
4. **Reduce safety classification of Software Items** (to the degree possible) via the use of Risk Controls that are external to the software.
5. **Implement mechanisms**, where possible, to reduce the likelihood of exposure to software-induced hazards, or reduce the Severity of the potential Harm.

Develop the software in compliance to IEC 62304 [10] and do not estimate the risks due to software-induced Hazards. It follows that without an estimate of software risks, software risks cannot be included in the computation of the Overall Residual Risks.

15.6 RISK MANAGEMENT FILE ADDITIONS

Implementation of IEC 62304 [10] introduces additional documentation requirements. The resulting artifacts are to be stored in the Risk Management File. Table 24, lists these additional entries in the Risk Management File.

Table 24 Additional Documents for the Risk Management File

IEC 62304:2006 Reference	Additional Software-Related Documentation Entries to the Risk Management File	Safety Class
4.3 c)	Software safety class assigned to the software system	N/A
4.3 d), e)	Software safety class for each Software Item, if the class of the Software Item is different from the class of the Software Item from which it was created by decomposition	N/A
4.3 f)	Rationale for using a lower software safety class for a Software Item in the software system	N/A
4.4.5	The version of the legacy software used, together with the rationale for the continued use of the legacy software	N/A
5.1.7	Software Risk Management Plan	A, B, C
5.2.1	Software system requirements, as derived from the System-level requirements	A, B, C
5.2.6	Verification of the following: – software requirements implementation, and traceability to parent System requirements – that software requirements are not contradictory – that software requirements are unambiguous – that software requirements are testable – that software requirements are unique	A, B, C
5.3.2	Architectural design of the interfaces among the Software Items and also interfaces between Software Items and external entities (hardware or software)	B, C
5.3.6	Verification of the software architecture to implement both System and software requirements, support the required interfaces, and support the proper operation of any SOUP items	B, C
5.4.2	Software design with sufficient detail to enable correct implementation of the software	C
5.4.3	Interface design among the software units and also interfaces between software units and external entities (hardware or software). Include sufficient detail to allow the correct implementation of the software	C
5.4.4	Verification of software detailed design to show that the software implements and doesn't contradict the software architecture	C
5.5.5	Verification of software units	B, C

(*Continued*)

Table 24 (Continued)

IEC 62304:2006 Reference	Additional Software-Related Documentation Entries to the Risk Management File	Safety Class
5.6.3, 5.6.7	Software integration test results	B, C
5.7.5	Software system test cases, methods, tools, configurations, results, dates, and identity of the testers	A, B, C
5.8.2	All known residual anomalies	A, B, C
5.8.4, 5.8.5	Versions of the medical device software that have been released, and the procedure and the environment required to create them	A, B, C
6.2.1.2, 9.2	Post-production monitoring of complaints, feedback, and documentation of the outcome of any investigation and evaluation	A, B, C
7.1.4, 7.2.1	Potential causes of the software contribution to hazardous situations, and the relevant risk controls	B, C
7.3.3	Traceability from each hazardous situation to Software Item to software cause to risk control measure to verification of the risk control measure	B, C
8.1.2	If SOUP items are used, document the SOUP title, name of manufacturer, and unique SOUP identifier	A, B, C
8.1.3	The configuration items and their version that comprise the software system configuration	A, B, C
9.5	Records of problem reports and their resolution including their verification	A, B, C

15.7 RISK CONTROLS

Risk Controls fall in three categories:

1. Inherent safety by design and manufacture
2. Protective measures
3. Information for safety and, where appropriate, training to users

See further elaboration in Section 18.2, on Risk Control option-analysis.

Below, examples are given for each of the above three Risk Control categories:

1. Inherent safety by design and manufacture: limiting software authority by hardware, e.g., physical limit to the maximum torque that a motor could deliver would mean that even if the software failed and gave a command for too much torque, it would be physically impossible for the motor to deliver too much torque.
2. Protective measure: algorithmic validity checking of inputs; password checks
3. Information for safety and, where appropriate, training to users: warning-messages; alarms; simulators for training

Additional general safety strategies that can be employed in software development include: pointer initialization, use of checksums on critical data, and avoidance of dynamic memory allocation. See Section 15.12 for many more tips for developing safety-critical software.

15.8 LEGACY SOFTWARE

Legacy software is defined as "medical device software which was legally placed on the market and is still marketed today, but for which there is insufficient objective evidence that it was developed in compliance with the current version of this standard" [10]. Note that legacy software is not the same thing as SOUP. See Section 15.9 to learn more about risk management of SOUP.

A manufacturer may intend to continue to use existing legacy software in their medical devices. In this case, objective evidence supporting the claim of safe continued use of the legacy software is required. Evidence may be derived from comprehensive assessment of available Post-Production field data. Sources of Post-Production field data include:

- Complaints and feedback on the device
- Reported adverse events that are attributable to the device
- Anomalies that are found in-house during testing

When a new product uses legacy software, that software is still subject to IEC 62304 [10].

Legacy software may be used without change, or may be modified to create new software, or it may be integrated into a new software system. In case of modification or integration into a new software system, new risks may be introduced. Analysis must identify, estimate, and evaluate any potential additional risks.

To demonstrate compliance of legacy software with IEC 62304 [10] perform the following steps:

1. "Assess any feedback, including Post-Production information, on legacy software regarding incidents and/or near incidents, both from inside manufacturer's own organization and/or from users."
2. Evaluate the legacy software for:
   - **a.** integration in the overall device architecture
   - **b.** continued validity of the Risk Control measures that are implemented in the legacy software
   - **c.** any Hazardous Situations associated with the continued use of the legacy software
   - **d.** any potential Causes that could induce Hazardous Situations via the legacy software

3. Define Risk Controls for each potential cause that could induce Hazardous Situations via the legacy software.
4. Perform gap analysis
   a. Examine the required deliverables per IEC 62304 [10] for the safety class of the legacy software.
   b. Compare what is required vs. what is available. Where gaps are identified, evaluate the potential reduction in risk resulting from the generation of the missing deliverables and associated activities. Based on this evaluation, determine what additional deliverables and activities to perform. At a minimum, Software System test records should be made available (see IEC 62304 [10] Section 5.7.5).

      Note – ensure that any Risk Controls that are implemented in the legacy software are included in software requirements.
   c. Assess the continuing validity of the available deliverables.
   d. Evaluate the adequacy of existing risk management documentation vis-à-vis ISO 14971 [1].

15.9 SOFTWARE OF UNKNOWN PROVENANCE

Software of Unknown Provenance, or Unknown Pedigree (SOUP) refers to software that is obtained from a third party, for which adequate documentation and records of development process are not available. SOUP is of particular interest in areas where software plays a pivotal role in the safety of the System.

Most medical device software uses some SOUP, as it is not practical to always produce software from scratch. So, managing the risk of SOUP becomes a fact of life.

FDA Guidance [40] states that "It may be difficult for you to obtain, generate, or reconstruct appropriate design documentation as described in this guidance for SOUP. Therefore, we recommend that you explain the origin of the software and the circumstances surrounding the software documentation. Additionally, your Hazard Analysis should encompass the risks associated with the SOUP regarding missing or incomplete documentation or lack of documentation of prior testing. Nonetheless, the responsibility for adequate testing of the device and for providing appropriate documentation of software test plans and results remains with you."

IEC 62304 [10] requires that the software configuration, integration, and change management plan include SOUP.

With respect to risk management, the functional and performance requirements of SOUP, and hardware and software that is necessary for the proper function of SOUP must be identified.

If failure or unexpected results from SOUP could potentially contribute to a Hazardous Situation, at a minimum evaluate any anomaly list that is published by the supplier of the SOUP to determine if any of the known anomalies could potentially create a System Hazard or lead to a Hazardous Situation.

15.10 SOFTWARE MAINTENANCE AND RISK MANAGEMENT

For most medical devices, software is continuously updated over time. The reasons could be bug fixes, feature improvement, or cybersecurity fixes. Changes to software can disrupt existing Risk Control measures, and/or introduce new Causes and Hazards. Formal and effective Quality management is essential to control software changes and assess their impacts.

One of the issues for software maintenance releases is that in many cases, the team that produces the maintenance-releases is not the same as the team that produced the original software. As such, they may be unfamiliar with the rationales for the original work or the Risk Controls that are in place.

Strategies to reduce risks due to software maintenance include: good documentation, and organizational strategies, e.g., to keep some of the staff who worked on the original software available for consultation.

15.11 SOFTWARE RELIABILITY VS. SOFTWARE SAFETY

A fact to consider is that reliable software is not necessarily safe. Reliability is defined as the ability to deliver the intended function for a certain length of time, under certain operating conditions. Software that is designed to the wrong requirements could be implemented with no defects, operate as intended 100% of the time, and still be unsafe.

Conversely, unreliable software may be safe. Consider an automatic sphygmomanometer (blood pressure monitor) (Fig. 39). Imagine that this device has an over-pressure sensor that detects if the device applies too high a pressure to the cuff, possibly injuring the patient. Now consider a condition where the control-software incorrectly interprets the over-pressure sensor and unnecessarily deactivates the device as a safety Risk Control. In this example, the software is unreliable, but it does not create a safety Hazard — it creates annoyance and frustration to the user.

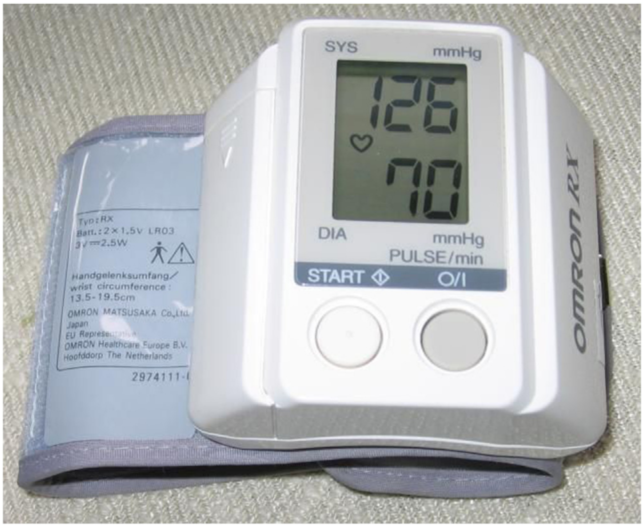


Figure 39 Automatic Sphygmomanometer.

15.12 TIPS FOR DEVELOPING SAFETY-CRITICAL SOFTWARE

In this section, general tips and advice are provided to aid in the successful development of safety-critical medical software.

- Do not postpone software Risk Analysis until late in the product development process. Retrospective software Risk Analysis cannot effectively reduce risk.
- When adding new software features, analyze for introduction of new Hazards, or compromising existing software Risk Controls.
- Consider platform evolution, e.g., operating system upgrades in your risk management process.
- Ensure that good software configuration management, and safety impact analysis due to software changes are a part of your QMS. This would help detect changes with unexpected consequences.
- If possible, separate the safety-critical Software Items and keep them as simple and small as possible. The separation can be architected to various degrees, depending on the criticality of the software.
- IEC TR 80002-1 [39] Table C.1 offers advice on avoiding pitfalls in the development of software for medical devices.

NASA JPL lead scientist, Gerard J. Holzmann produced a set of 10 rules to help guide the development of safety-critical software. Below, the 10 rules are summarized. For further details, see Ref. [41]. These rules are directed at C programming language, but you can benefit from them in other programming environments as well.

1. *Rule*: Restrict all code to very simple control flow constructs – do not use *goto* statements, *setjmp* or *longjmp* constructs, and direct or indirect *recursion*.
2. *Rule*: All loops must have a fixed upper-bound. It must be trivially possible for a checking tool to *prove* statically that a preset upper-bound on the number of iterations of a loop cannot be exceeded. If the loop-bound cannot be proven statically, the rule is considered violated.
3. *Rule*: Do not use dynamic memory allocation after initialization.
4. *Rule*: No function should be longer than what can be printed on a single sheet of paper in a standard reference format with one line per statement and one line per declaration. Typically, this means no more than about 60 lines of code per function.
5. *Rule*: The *assertion density* of the code should average to a minimum of two assertions per function. Assertions are used to check for anomalous conditions that should never happen in real-life executions. Assertions must always be side-effect free and should be defined as Boolean tests. When an assertion fails, an explicit recovery action must be taken, e.g., by returning an error condition to the caller of the function that executes the failing assertion. Any assertion for which a static checking tool can prove that it can never fail or never hold violates this rule. (That is, it is not possible to satisfy the rule by adding unhelpful "*assert(true)*" statements.)
6. *Rule*: Data objects must be declared at the smallest possible level of scope.
7. *Rule*: The return value of non-void functions must be checked by each calling function, and the validity of parameters must be checked inside each function.
8. *Rule*: The use of the preprocessor must be limited to the inclusion of header files and simple macro definitions. Token pasting, variable argument lists (ellipses), and recursive macro calls are not allowed. All macros must expand into complete syntactic units. The use of conditional compilation directives is often also dubious, but cannot always be avoided. This means that there should rarely be justification for more than one or two conditional compilation directives even in large software development efforts, beyond the standard boilerplate that avoids multiple inclusion of the same header file. Each such use should be flagged by a tool-based checker and justified in the code.
9. *Rule*: The use of pointers should be restricted. Specifically, no more than one level of dereferencing is allowed. Pointer dereference operations may not be hidden in macro definitions or inside *typedef* declarations. Function pointers are not permitted.

10. *Rule*: All code must be compiled, from the first day of development, with *all* compiler warnings enabled at the compiler's most pedantic setting. All code must compile with these setting without any warnings. All code must be checked daily with at least one, but preferably more than one, state-of-the-art static source code analyzer and should pass the analyses with zero warnings.

CHAPTER 16

Integration of Risk Analysis

Abstract

Once the System is decomposed, it is possible to perform a hierarchical multi-level Failure Modes and Effects Analysis (FMEA) on the System components. Lower level components' FMEAs, as well as input from supplier FMEAs, roll up into higher level FMEAs. This process continues to the System Design Failure Modes and Effects Analysis, from which System hazards can be derived.

Keywords: Integration; hierarchical multi-level FMEA; supplier risk management

16.1 HIERARCHICAL MULTI-LEVEL FMEA

Once the System is decomposed, it is possible to perform a hierarchical multi-level Failure Modes and Effects Analysis on the System components. Lower-level components' FMEAs roll up into higher level FMEAs. This process continues until the L1, System DFMEA. See Fig. 22.

Fig. 40 illustrates the connectivity between consecutive decomposition levels. The rationale for this construct is that a lower-level component can fail due to design issues, or manufacturing issues. From the perspective of an upper level DFMEA, what matters is that the lower-level component has failed. Whether it was due to a design or a manufacturing issue is only relevant when the Cause of that failure is documented.

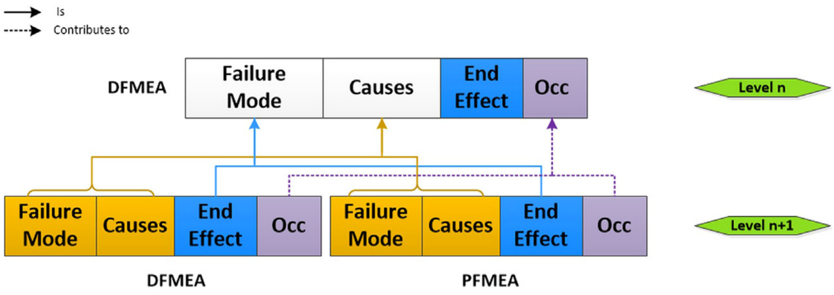


Figure 40 FMEA Integration.

This concept is elucidated below in an example of an automobile System. An automobile is comprised of several subsystems. See Fig. 41. For this example, let's focus on the propulsion system – the Engine.

DOI: https://doi.org/10.1016/B978-0-323-85755-0.00016-3

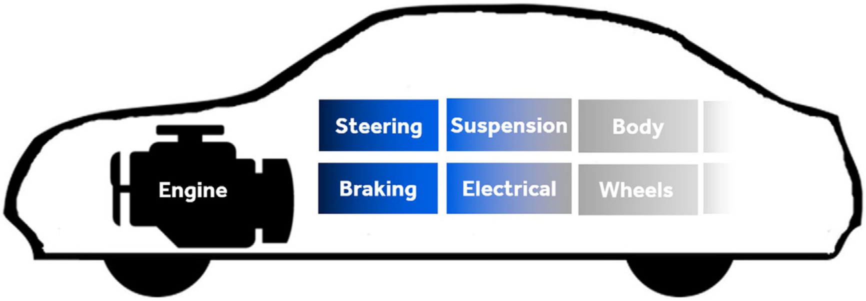


Figure 41 Automobile Sub-Systems.

In the illustration in Fig. 41 the Engine is a black box. But the Engine itself is comprised of many other subsystems. In Fig. 42 a number of Engine subsystems are illustrated. Let's focus on the cooling system — the Water Pump.

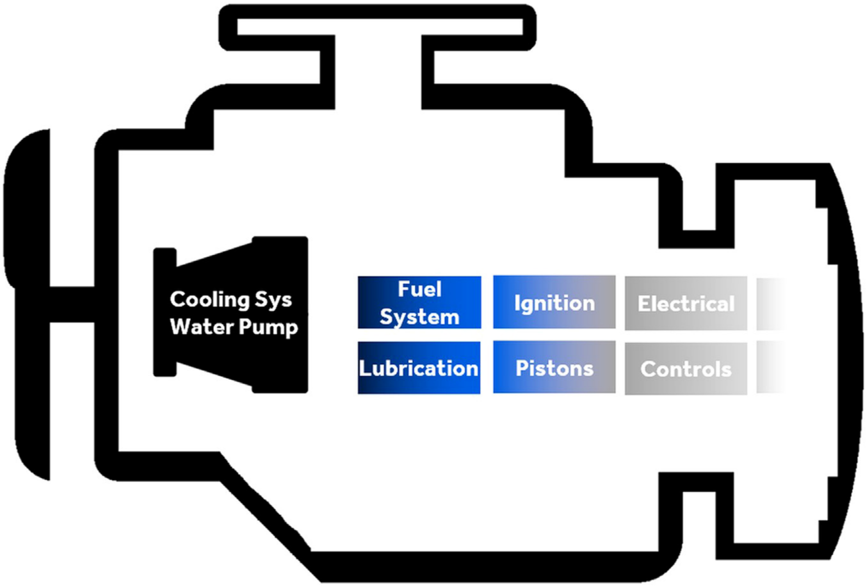


Figure 42 Engine Sub-Systems.

In the illustration in Fig. 42 the Water Pump is a black box. But the Water Pump itself is comprised of many other parts. In Fig. 43 the Water Pump is decomposed to its constituent parts. We will not further decompose the Water Pump parts.

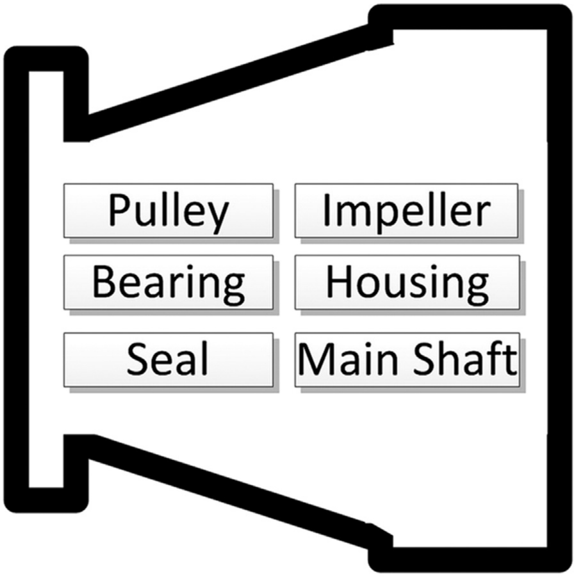


Figure 43 Water Pump.

To this point, we have followed a decomposition model similar to what is illustrated in Fig. 12. Now let's consider the Failure Mode of one of the Water Pump parts: the Pulley. If the Pulley breaks up, the water pump can no longer receive torque from the engine, and it stops pumping water. Not pumping water is the End Effect of the pulley break-up on the Water Pump. See Fig. 44.

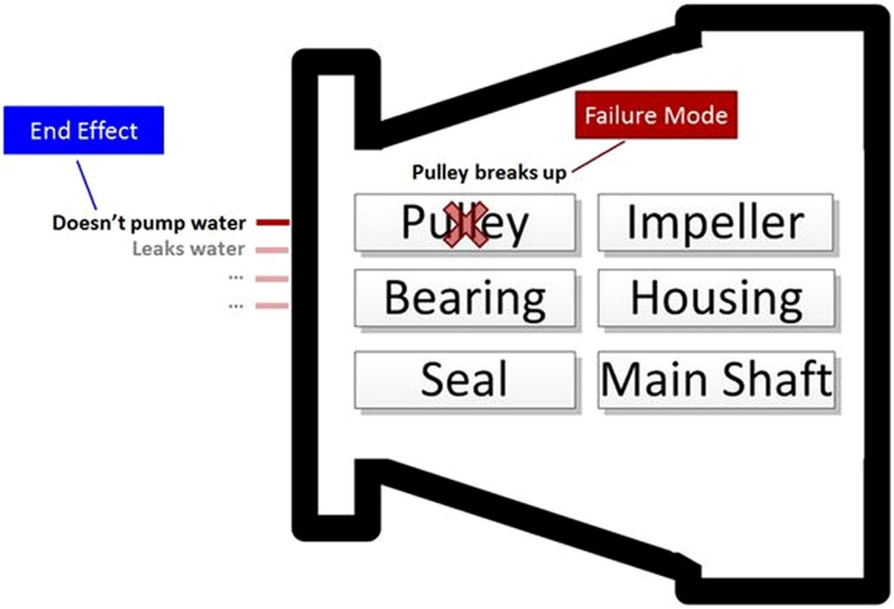


Figure 44 Failure Mode of the Pulley.

Now let's move up one level to the Engine. To the Engine, the Water Pump is a black box component, whose Failure Mode is: *Doesn't Pump Water*. See Fig. 45. Notice that what was the End Effect: *Doesn't Pump Water* from the Water Pump perspective, has now become the Failure Mode of the Water Pump from the engine perspective.

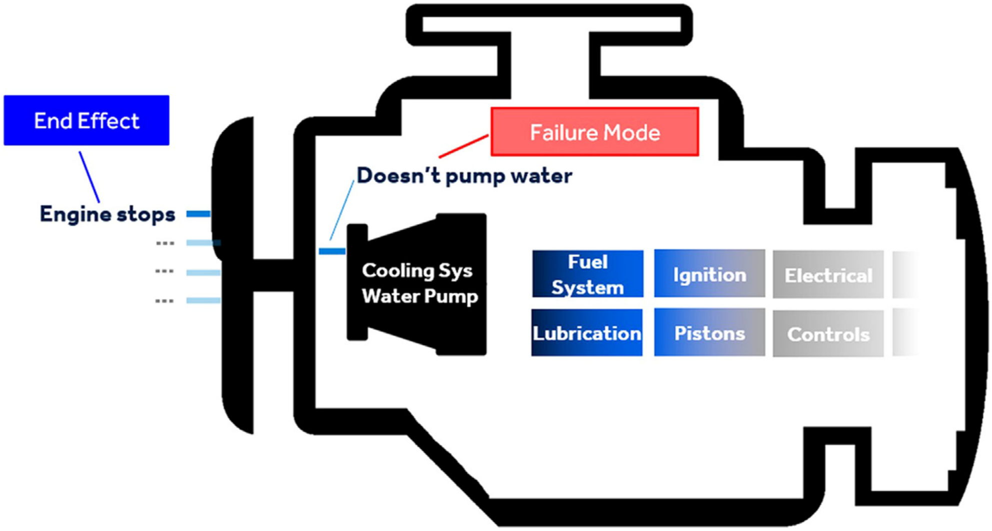


Figure 45 Failure Mode of the Water Pump.

The same construct can continue upward to the car-level, where the End Effect of *Engine Stops* at the engine level (Fig. 45) can become the Failure Mode of the engine from the perspective of the car (Fig. 46). Again, what was the End Effect: *Engine Stops* from the engine perspective, becomes the Failure Mode of the engine from the car perspective, which sees the engine as a black box component.

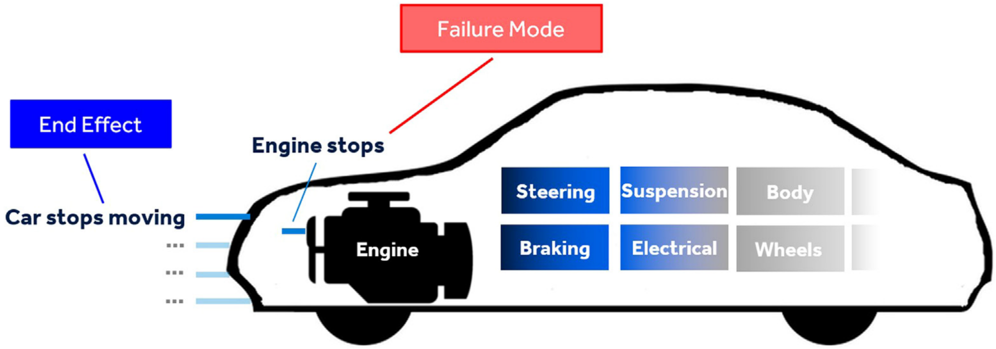


Figure 46 Failure Mode of the Engine.

As the hierarchical multi-level FMEA is integrated in an upward direction, the story of how System hazards manifest is built up. The mechanisms of failure in the System DFMEA are the compounding of all the lower-level mechanisms of failure, and express the sequences of events that could lead to the System Hazards.

16.2 INTEGRATION OF SUPPLIER INPUT INTO RISK MANAGEMENT

Most medical device manufacturers use suppliers to produce parts of their medical devices. The design and manufacturing of the supplied parts plays a role in the safety of the medical device. Surprises can occur when a supplier is notified of the criticality of the supplied part, after the part has been produced. Significant program delays can happen due to either the redesign of the part, or the redesign of the system around the part. Close communication between the medical device system designers, architects and engineers, and suppliers is essential.

The input from the supplier must be incorporated in the risk management of the medical device. At a minimum, what is needed from the suppliers are the Failure Modes of the parts that they supply, and the occurrence ratings of the Failure Modes. With that information the manufacturer can incorporate the contribution of the supplied part to the risk management of the System under analysis. Occurrence rating helps us derive P1. Knowledge of the causes of the Failure Modes of the supplied parts can help with estimation of P1s, and also with the design of Risk Controls. Recognize that what is a Failure Mode to the customer, is the End Effect in the supplier's FMEA.

It is important that boundaries of responsibility for the FMEAs are clearly defined. If a supplied part interfaces with your medical device, who is responsible for the analysis of the interface? The supplier, or the customer?

Knowledge of other entries in the supplier Risk Management File would be interesting for R&D engineering, Supply chain, and Quality departments, but not required from the risk management perspective.

As manufacturers, you should ensure that your Quality agreements with your suppliers stipulate specific responsibilities for the performance of FMEAs, deliverables, and communications. You may need to use contractual mechanisms, e.g., Non-Disclosure Agreements, to facilitate the free flow of information.

CHAPTER 17

Risk Estimation

Abstract

According to ISO 14971, risk is a combination of the probability of occurrence of Harm and the severity of that Harm. In this chapter three methods are presented for risk estimation: qualitative, semi-quantitative, and quantitative. In the BXM method, a high-resolution approach to risk estimation is used where the risks of harms are estimated in 5 severity classes. Also, situations where risk cannot be estimated are discussed.

Keywords: Risk estimation; qualitative; semi-quantitative; quantitative; high-resolution risk estimation

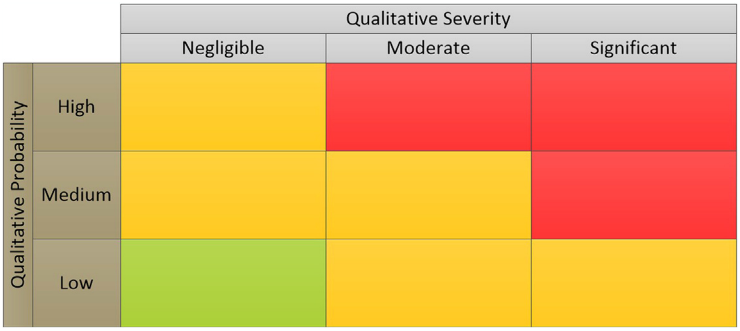
According to ISO 14971 [1] risk is a combination of the probability of occurrence of Harm and the Severity of that Harm.

A medical device poses individual risks, which are the result of exposure to individual hazards. And also, the medical device poses an overall risk, which is the aggregate of all the individual risks.

Three methods are commonly used to estimate the risk of Harm. In increasing order of preference, they are: Qualitative, Semi-Quantitative, and Quantitative. Each method is described below.

17.1 QUALITATIVE METHOD

The qualitative method is used when quantifiable data is unavailable, or confidence in the available data is low. In such cases use an N × M matrix such as the example in Fig. 47 to



		Qualitative Severity		
		Negligible	Moderate	Significant
Qualitative Probability	High	🟨	🟥	🟥
	Medium	🟨	🟨	🟥
	Low	🟩	🟨	🟨

Figure 47 Example 3 × 3 Qualitative Risk Matrix.

Safety Risk Management for Medical Devices
DOI: https://doi.org/10.1016/B978-0-323-85755-0.00017-5

stratify the risks. In this example a 3 × 3 matrix is used to stratify the risks into three zones: high (red), medium (yellow), and low (green). High-Severity, high-probability harms present the highest risks, and conversely low-Severity, low-probability harms present the lowest risks.

In order for the qualitative method to work, very good definitions for each probability and Severity level should be given to ensure repeatability and consistency of ratings by different analysts, at different times. Tables 25 and 26 offer examples of language that could be used to promote consistency in Severity and probability ratings.

Table 25 Example 3-Level Definitions for Severity

Term	Definition
Significant	Death, or permanent impairment/injury
Moderate	Reversible or minor injury
Negligible	Discomfort or inconvenience

Table 26 Example 3-Level Definitions for Probability

Term	Definition
High	Likely to happen | often | frequent
Medium	Can happen, but not frequently
Low	Unlikely to happen | rare | remote

You can estimate individual risks by plotting their place in a qualitative matrix such as Fig. 47.

17.2 SEMI-QUANTITATIVE METHOD

The semi-quantitative method is similar to the qualitative method, but with the difference that data is available for probability of occurrence of Harm. Generally, this is true for products that have been in the field for a significant length of time and about which a lot of field data has been collected.

The scales for probability of occurrence of Harm would be different for different products. Examples: 'per use,' 'per activation,' or 'per hour of use.'

Each Hazard would have an estimated risk based on the available data for the probability of occurrence of Harm, and the estimated Severity of that Harm.

ISO/TR 24971 [15] offers a 5 × 5 example for ranking Severity and probability. Tables 27 and 28 are based on the definitions in ISO/TR 24971 [15].

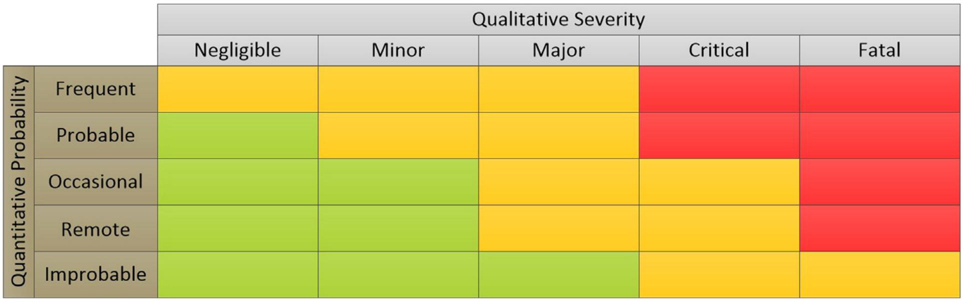
Table 27 Example 5-Level Definitions for Severity

Rank	Term	Definition
5	Fatal	Results in death
4	Critical	Results in permanent impairment or irreversible injury
3	Major	Results in injury or impairment requiring medical or surgical intervention
2	Minor	Results in temporary injury or impairment not requiring medical or surgical intervention
1	Negligible	Results in inconvenience or temporary discomfort

Table 28 Example 5-Level Definitions for Probability

Rank	Term	Definition	Probability
5	Frequent	Will occur frequently	$\geq 10^{-3}$
4	Probable	Will likely occur repeatedly	$<10^{-3}$ and $\geq 10^{-4}$
3	Occasional	May occur occasionally	$<10^{-4}$ and $\geq 10^{-5}$
2	Remote	Seldom expected to occur	$<10^{-5}$ and $\geq 10^{-6}$
1	Improbable	Not expected to occur	$<10^{-6}$

Fig. 48 depicts an example 5 × 5 risk matrix which stratifies the risks in the: high (red), medium (yellow), and low (green) zones. Similar to the qualitative method, High-Severity, high-probability harms present the highest risks, and conversely low-Severity, low-probability harms present the lowest risks.



		Qualitative Severity				
		Negligible	Minor	Major	Critical	Fatal
Quantitative Probability	Frequent	🟨	🟨	🟨	🟥	🟥
	Probable	🟩	🟨	🟨	🟥	🟥
	Occasional	🟩	🟩	🟨	🟨	🟥
	Remote	🟩	🟩	🟨	🟨	🟥
	Improbable	🟩	🟩	🟩	🟨	🟨

Figure 48 Example 5 × 5 Risk Matrix.

You can estimate individual risks by plotting their place in a semi-qualitative matrix such as Fig. 48.

17.3 QUANTITATIVE METHOD

ISO 14971 [1] Annex C presents a concept for quantification of risk. This concept is presented in Fig. 49, where it is indicated that risk is the product of P1, the probability of occurrence of a Hazardous Situation, and P2, the probability of a Hazardous Situation leading to Harm. The problem with this method is that manufacturers typically conservatively consider the most severe Harm that could ensue from the

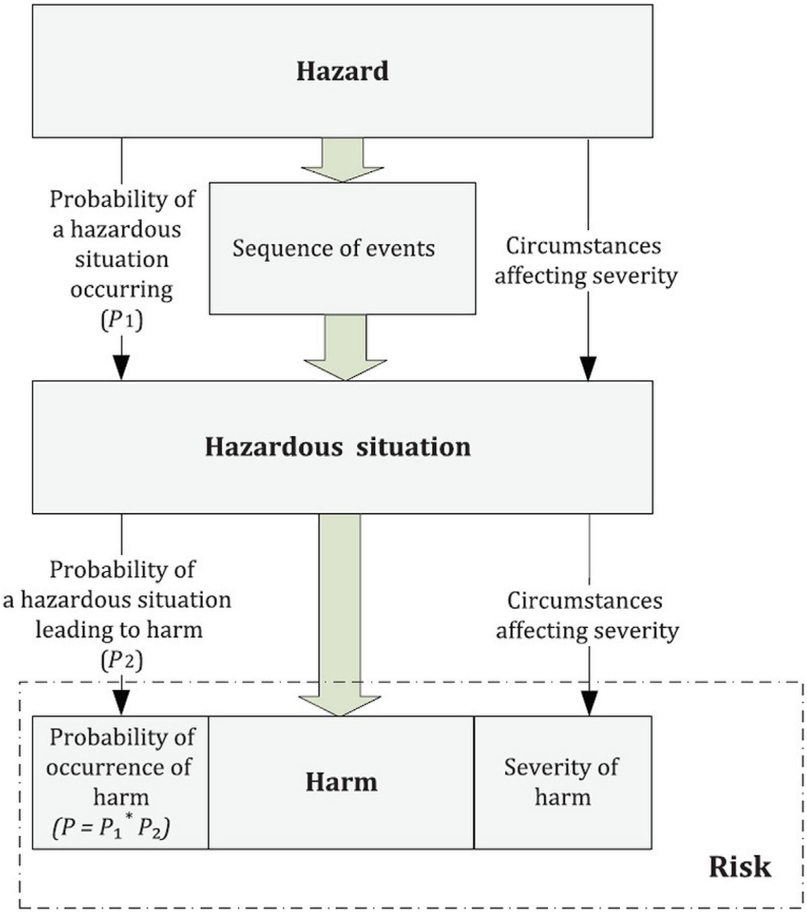

Hazard
Probability of a hazardous situation occurring (P1)
Sequence of events
Circumstances affecting severity
Hazardous situation
Probability of a hazardous situation leading to harm (P2)
Circumstances affecting severity
Probability of occurrence of harm (P = P1 * P2)
Harm
Severity of harm
Risk

Figure 49 ISO 14971, Fig. C.1 — Quantification of Risk.

Hazardous Situation. Clearly, the most severe Harm doesn't happen every time. Considering only the worst Harm distorts risk management in two ways:

1. If the worst-case Severity of Harm is unlikely to happen, but a moderate Severity of Harm is more likely to happen, then the estimated risk for the worst-case Harm would be a smaller value (due to the smaller P2), than the risk of a moderate-Severity Harm. The result of this distortion is that the manufacturer would incorrectly rank the true risks of the medical device.
2. Most Harms could result in death — at least with a small probability. Estimating risks based on the worst outcome for every Harm would create an illusion that the medical device is deadly. This could create an impossible situation for the manufacturer because unless a Hazardous Situation is eliminated, no matter how much P1 is reduced, there would still be a risk of death, since P2 would be non-zero.

The BXM method uses a quantitative method that computes risk in five classes of Harm Severity: fatal, critical, major, minor, and negligible. This is depicted in Fig. 50. The advantage of this method is that the entire spectrum of Harm Severities is considered and regardless of the Severity of the Harm, the highest risk is identified.

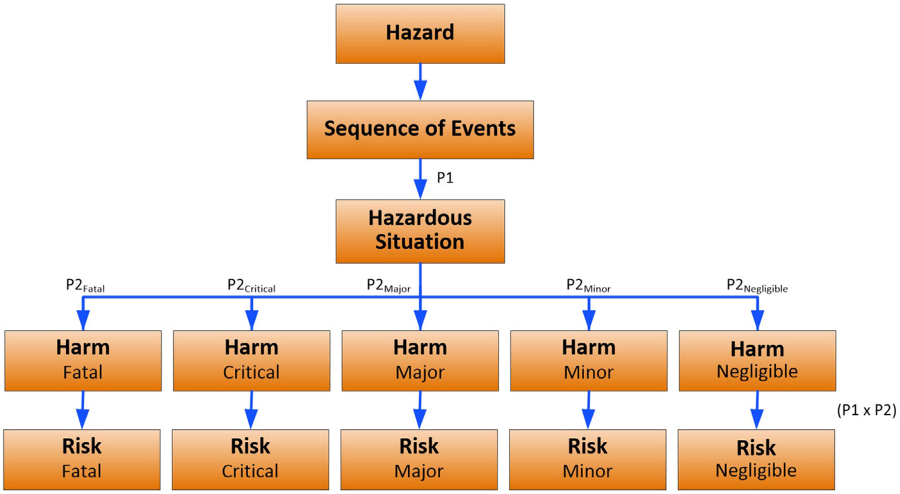


Figure 50 The BXM 5-Level Risk Computation Method.

Vis-à-vis the Hazard theory that was presented in Section 4.2, since the accounting for Harm encompasses the entire spectrum from death to no-Harm, and the sum of all P2s is 1, it can be said that P1 = Probability of occurrence of Hazardous Situation=probability of occurrence of Harm.

As in the semi-quantitative method, P1 is presumed to be known.

Consider this hypothetical example: based on field data it is known that patients are exposed to too-high X-ray radiation dosage in 1 out of 100,000 (10^{-5}) applications of an X-ray machine.

Now, given that a patient is exposed to too high X-ray radiation dosage, we can ask:

- What is the probability that the patient experiences Fatal Harm; $P2_{FATAL}$
- What is the probability that the patient experiences Critical Harm; $P2_{CRITICAL}$
- What is the probability that the patient experiences Major Harm; $P2_{MAJOR}$
- What is the probability that the patient experiences Minor Harm; $P2_{MINOR}$
- What is the probability that the patient experiences Negligible Harm; $P2_{NEGLIGIBLE}$

In other words, given all the reported cases of X-ray overexposure, how many died; how many suffered permanent irreversible injury; and so on. This exercise produces five P2 numbers.

In this hypothetical example, we have P1, the probability of X-ray overexposure (10^{-5}), therefore we can compute the risk of Harm from X-ray overexposure in five Severity classes:

Risk of Fatal Harm=$P1 \times P2_{FATAL}$
Risk of Critical Harm=$P1 \times P2_{CRITICAL}$
Risk of Major Harm=$P1 \times P2_{MAJOR}$
Risk of Minor Harm=$P1 \times P2_{MINOR}$
Risk of Negligible Harm=$P1 \times P2_{NEGLIGIBLE}$

This yields the estimated individual risks, each in five Severity classes.

It should be noted that all statistics are approximations of the truth. Therefore, since both P1 and P2 are estimates, then Risk (R) is also an estimate.

In practice, we find that field-data may not be available for all P1s and P2s. In such cases, we will have to rely on alternative means of data-gathering, such as published scientific papers, registries, etc.

Note that the use of P1 and P2 is not mandatory. The goal is to identify the risk of Harm. It might be possible to directly compute the risk of Harm in five Severity categories if appropriate data is collected. Let's say in 100 reported cases of a balloon catheter failure to deflate, resulting in vascular damage, 1 person died; 4 persons suffered a stroke that resulted in permanent impairment; 35 persons required emergency surgery but recovered; 45 persons had minor vascular damage; and 15 persons had no injuries, though the procedure took an average of 2 minutes longer to complete. You could compute the risk of vascular damage due to catheter balloon failure to deflate to be:

Harm	Fatal	Critical	Major	Minor	Negligible
Vascular damage due to balloon catheter failure to deflate	1%	4%	35%	45%	15%

Tip 'Severity' as used in Risk Estimation refers to the impact on health and safety. Severity as used in the FMEA refers to the significance of the worst reasonable consequence of the End Effect, which might be unrelated to safety. Don't conflate the two.

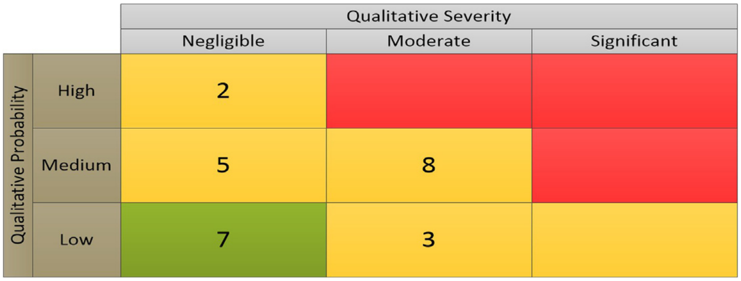
17.4 INDIVIDUAL AND OVERALL RESIDUAL RISKS

ISO 14971 [1] requires the estimation and evaluation of individual Residual Risks, and the Overall Residual Risk. The three methods of qualitative, semi-quantitative, and quantitative can be used to estimate both individual and Overall Residual Risks

Estimation of individual risks in all three methods was described in Sections 17.1—17.3. Below, methods for estimation of Overall Residual Risk by each method are described.

Qualitative Method

Plot a dot for each individual risk in the qualitative risk matrix. Count the dots in each cell of the matrix. This creates a risk-signature that is indicative of the Overall Residual Risk. Fig. 51 is an example of qualitative Overall Residual Risk estimation.

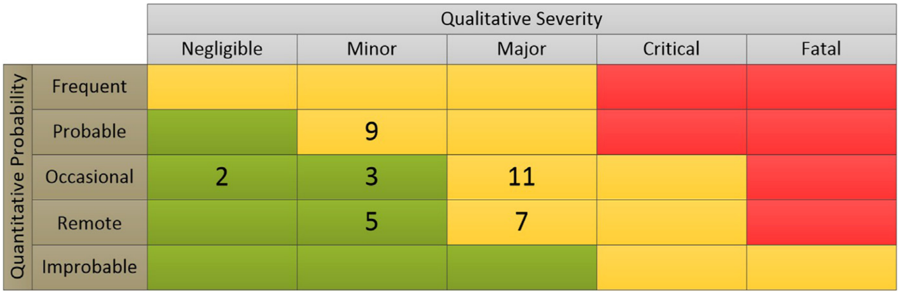


		Qualitative Severity		
		Negligible	Moderate	Significant
Qualitative Probability	High	🟨 2	🟥	🟥
	Medium	🟨 5	🟨 8	🟥
	Low	🟩 7	🟨 3	🟨

Figure 51 Example Qualitative Overall Risk Estimation.

Semi-Quantitative Method

Similar to the qualitative method, you can plot each individual risk in the semi-quantitative risk matrix and count the total number of individual risks in each cell of the matrix. This creates a risk-signature that is indicative of the Overall Residual Risk. Fig. 52 is an example of Semi-Quantitative Overall Residual Risk estimation.



		Qualitative Severity				
		Negligible	Minor	Major	Critical	Fatal
Quantitative Probability	Frequent	🟨	🟨	🟨	🟥	🟥
	Probable	🟩	🟨 9	🟨	🟥	🟥
	Occasional	🟩 2	🟩 3	🟨 11	🟨	🟥
	Remote	🟩	🟩 5	🟨 7	🟨	🟥
	Improbable	🟩	🟩	🟩	🟨	🟨

Figure 52 Example Semi-Quantitative Overall Residual Risk Estimation.

Quantitative Risk Estimation

In the quantitative method the Overall Residual Risk can be objectively computed using Boolean algebra. Table 29 presents an example of quantitative method for three harms that are independent of one another.

Table 29 Example Quantitative Overall Residual Risk Computation

Risk Class	Fatal	Critical	Major	Minor	Negligible
Harm 1 Residual Risk	1%	4%	35%	45%	15%
Harm 2 Residual Risk	5%	10%	40%	30%	15%
Harm 3 Residual Risk	2%	8%	60%	20%	10%
Overall Residual Risk	7.8%	20.5%	84.4%	69.2%	35%

Using the quantitative method one can answer the question, for example, "Overall, what is the estimated risk of patient death using a medical device?"

17.5 PRE/POST RISK

Although ultimately what matters is the level of risk after the implementation of Risk Controls, traditionally, some members of the risk management community look for Risk Estimations before and after the implementation of Risk Controls.

Experienced medical device designers apply their knowledge of medical devices to their preliminary designs to ensure that the product is as safe as possible. Therefore, it is entirely possible that the initial design of the product is the best and final design. ISO/IEC Guide 51 [9] says "During the preliminary design of a product or a system, inherently safe design measures are usually intuitively applied. Therefore, the Risk Evaluation for some hazards might lead to a positive outcome at the first iteration and no further risk reduction is required."

Determination of risk pre-Risk Controls is sometimes not practical. For example, let's say the designers specified good, biocompatible materials for an implantable device from the preliminary stages of design. To answer the question of 'what was the risk before choosing biocompatible materials,' would require one to hypothesize the use of bio-incompatible materials. But which material? There are a range of toxic materials that could be selected. And what benefit would this exercise deliver?

Another dilemma is the definition of post-Risk Control. Consider a first draft of a design that creates an unacceptable risk. The design is improved with some Risk Controls, and a second draft is created. The risk of the second draft also is judged to be unacceptable. A third draft is created with yet more Risk Controls. Now the risk of the third and final draft of the design meets the acceptability criteria. Which is the post-risk? Risk of draft 2, or risk of draft 3?

There are two ways to handle this matter.

1. Suffice it to provide the risk of the final design, as that is what matters to the patient.
2. Take the risk of the first draft of the design and call it pre-risk. Keep it static. If this risk is acceptable, copy it in the post-risk column, so the pre- and post-risks are the same. If the pre-risk is not acceptable, then populate the post-risk column with the risk of the final design, regardless of how many iterations occur between draft 1, and the final draft.

17.6 RISKS THAT CANNOT BE ESTIMATED

ISO 14971 [1] requires that the criteria for risk acceptability be documented in the RMP, including when the probability of occurrence of Harm cannot be estimated. Examples are harms due to systemic faults, or due to Use Errors. Systemic faults can be present in hardware or software and can be introduced during the device's design, manufacture, or maintenance. These are the kind of faults that typically remain latent until the right conditions manifest. Some examples of systemic faults:

- Software design doesn't account for a certain unusual combination of parameters and produces the wrong results; this unusual combination doesn't get tested in development

- An erroneous instruction in the IFU would cause all users to create a Hazardous Situation
- An implantable device is designed for correct operation at up to 1 bar of pressure. If a patient scuba dives, the device will fail

For more discussion and examples see ISO/TR 24971 [15] Section 5.4.5.

ISO 14971 [1] Section 5.5 says when the risks cannot be estimated, "the possible consequences shall be listed for use in Risk Evaluation and Risk Control." Without knowing the extent of a risk, it cannot be evaluated, but it can be controlled.

ISO 14971 [1] Annex A, Section 2.5.5 says although there is no consensus on how to calculate the risks from systemic faults, the related Hazardous Situations should still be listed to allows the manufacturer to focus on reducing the risks due to these Hazardous Situations.

Examples of situations where risk cannot be estimated:

- Risks due to systemic latent hardware or Software Defects
- Risks due to deliberate intention to cause harm, e.g., sabotage, hacking, tampering
- Risks due to unimagined/unexpected user actions
- Risks due to unimagined/unexpected changes to use-conditions

In situations where the risk of Harm cannot be estimated, the Risk Control measures should focus on reducing the risk by either reducing the probability of occurrence of the Hazardous Situation, or reducing the Severity of the consequent Harm. An inverse relationship can be presumed between the rigors of product design, manufacture, and maintenance and the likelihood of systemic faults remaining undetected. Conformance to standards such as IEC 62304 [10] for software is useful in reducing risks of systemic faults.

Similarly, conformance to IEC 62366 [19] for usability engineering can reduce the risks of Use Errors, even when it is difficult to estimate the probability of a Use Error.

The BXM method uses quantitative methods for Risk Estimation. But when there are hazards whose risk cannot be estimated, a hybrid method is used. In the hybrid method where it is possible to quantitatively estimate risks, we do so and account for all those risks in the Overall Residual Risk estimation. Where it is not possible to estimate risks, we reduce those risks consistent with the approach in the RMP, e.g., As Far as Possible. Naturally, risks that cannot be estimated cannot be included in the quantitative estimation of Overall Residual Risk. However, in the final judgement of the Benefit-Risk acceptability all risks are considered.

CHAPTER 18

Risk Controls

Abstract

Risk Controls are the overt actions and measures by which risks are reduced to, or maintained within, specified levels. Three types of risk control measures are offered, and techniques for distinguishing the different risk control types are presented. Information-for-Safety as a type of Risk Control is discussed in detail. Sample Risk Controls are provided as examples. Also, the concept of single-fault-safety is expounded in this chapter.

Keywords: Risk controls; risk control option analysis; information for safety; completeness of risk controls; single-fault-safe

Once the risks of a medical device are estimated, measures must be taken to reduce the risks, if the risks are deemed unacceptable. These measures are called Risk Controls.

Risk Controls can be viewed over two horizons:

1. Risk Controls performed prior to release of the product
   These Risk Controls are discussed in Section 18.2.
2. Risk Controls performed after the release of the product

These are Risk Controls that are done at the customer site. Examples: personal protective equipment, organizational procedures, training.

In general, Risk Controls attempt to prevent the realization of Hazards, or exposure to Hazards. These types of Risk Controls reduce P1. Some Risk Controls attempt to reduce the Severity of the Harm after exposure to Hazards. These types of Risk Controls reduce P2.

> Example of P1 reduction – sterilization of implantable medical devices reduces the likelihood of exposure to microbes.
> Example of P2 reduction – Medtronic TYRX™ Absorbable Antibacterial Envelope is a device that doesn't prevent exposure to bacteria, but should bacteria get into the wound, it reduces the probability of receiving Harm from the bacteria.

18.1 SINGLE-FAULT-SAFE DESIGN

ISO 14971 [1] requires that the device risks under both normal and fault conditions be managed. IEC 60601-1 [7] requires that medical devices be designed such that they are

Safety Risk Management for Medical Devices
DOI: https://doi.org/10.1016/B978-0-323-85755-0.00018-7

single-fault-safe. IEC 60601-1 [7] Section 4.2.2 further clarifies that 'fault condition' includes single-fault condition, but is not limited to it. The concept of single-fault-safe has a built-in assumption of independence of faults. If the occurrence of the initial fault will necessarily cause the occurrence of a secondary fault, then they count as one fault. For example, if the failure of a device's user interface (fault #1) will certainly lead to the inability of the user to operate the device (fault #2), then these count as one fault.

A common interpretation of 'single-fault-safe' is that as long as a medical device is acceptably safe under a single-fault condition, the device risks are acceptable. But in fact, this is not true. Consider a device that can fail due to a single fault, and whose failure creates an unsafe condition. Assume the likelihood of occurrence of the single fault is high. Now a secondary means of protection is added, such that when the primary fault happens, the secondary means would transition the device to a safe state. Theoretically this device is single-fault-safe because it takes two independent faults to create an unsafe condition. But what if the likelihood of failure of the secondary means is also high? Can you envisage a situation where both the primary fault, and the failure of the secondary means have occurred simultaneously? Given the knowledge that the likelihood of both the primary fault and the failure of the secondary means is high, you can surmise that the safety risk of the device would not be low.

A closer scrutiny of IEC 60601-1 [7] Section 4.7 reveals that Ref. [7] accepts a single means of risk reduction as single-fault-safe, if the probability failure of that single means is negligible. In designs in which arriving at an unsafe condition requires two faults, Ref. [7] clarifies that single-fault-safe condition is met, if the initial fault is detected before the secondary fault has occurred. Single-fault-safe condition is also met if the probability of failure of the secondary means is negligible, during the expected service life of the device. From the risk management perspective, what matters is that the Overall Residual Risk of the device be acceptable, irrespective of one, two, or more faults.

In summary, the risk of the medical device must be acceptable during the mission of the device. Mission could be the expected service-life of the device. Or, if routine maintenance is done during which the failure of the secondary means would be detected, mission would be the time between maintenance events. Note the assumption of detection of failure of the secondary means, and the implicit repair/replacement of a failed secondary means during the maintenance event.

With this interpretation, we can compute the device risk based on the probability of occurrence of both the primary fault, and the failure of the secondary means of protection during the mission of the device.

18.2 RISK CONTROL OPTION ANALYSIS

ISO 14971 [1] identifies three methods of controlling risk as listed below in decreasing order of preference.

1. Inherently safe design and manufacture
2. Protective measures in the medical device itself or in the manufacturing process
3. Information for safety and, where appropriate, training to users

Consider if it is possible to eliminate a Hazard. If so, change the design so that the device is inherently safe from that Hazard. For example, substitute non-toxic materials for toxic materials, if possible. If elimination of the Hazard is not possible, then consider protective means in the design, or the manufacturing process to protect the patient/user from Harm. Additionally, if providing information for the safe operation and use of the device could help with reducing the risks of the device, provide such information. Similarly, if training of the users could help with reduction of the risks of the device, provide relevant training.

Document the Risk Control option-analysis and the decisions made on the selection and implementation of the Risk Controls.

After the first pass through Risk Analysis, it may be determined that additional Risk Controls need to be implemented. For every additional Risk Control that is implemented determine if any new Hazards are introduced, or if the any of the current risks are increased. For example, adding a warning beep in a device which is used in an ICU, may actually increase the risk to the patient in that the attending nurse could be subjected to too many beeps from many devices and not be able to discern what to do in an emergency.

18.3 DISTINCTIONS OF RISK CONTROL OPTIONS

Sometimes it may not be easy to distinguish the type of a particular Risk Control measure: inherently safe by design/manufacture, or a protective measure, or information for safety. Below, the different options are distinguished.

Inherently Safe by Design and Manufacture – The device behaves in a safe manner without any action or knowledge required from the user. The user cannot easily defeat the Risk Controls.

> **Example** – An implantable device is built using biocompatible materials.
>
> **Example** – In a car with automatic transmission, it is possible to start the car only if the gear shift selector is in Park, or Neutral positions. This prevents the operator from starting the engine in gear and causing possible unexpected vehicle movement.

Protective Measure – Device behaves in a safe manner without the need for user intervention, but the protective measure(s) can be easily defeated by the user.

> **Example** – Hypodermic needles come with a protective cap. The user does not need to take any action to make the product safe, as it is delivered. However, the user can easily remove the protective cap.
>
> **Example** – Surgeons are provided with lead aprons to protect them against X-ray radiation of fluoroscopes. But, the surgeon can choose not to wear the lead apron.
>
> **Example** – Inspection testing during the manufacturing process. Inspection may be skipped.

Information for Safety and, where appropriate, training to users – Provides knowledge to the user and expects action by the user.

> **Example** – Instruction for cleaning and sterilization of a reusable surgical tool, provides knowledge to the user and requires action from the user in order to use the device safely.
>
> **Example** – A single-use catheter has a label warning against reuse.

18.4 INFORMATION FOR SAFETY AS A RISK CONTROL MEASURE

Information for safety can take many forms. For example: screen displays, IFUs, labels attached to the device, and online help.

Information for safety is distinct from disclosure of the Residual Risks. Disclosure of the Residual Risk enables a user to make an informed decision as to whether to use a medical device. Whereas information for safety enables a user to safely use a device after he/she has decided to use the medical device. Disclosure of the Residual Risk can also be used by the user of the medical device to better prepare for possible side effects or hazards that can occur during or after the use of the medical device.

Disclosure of Residual Risk is informative, while information for safety is instructive.

18.4.1 Criteria for Information for Safety

If you choose to use information for safety as a Risk Control measure, there are certain considerations. The information for safety must be perceivable, comprehensible, and actionable by the user, and be effective in reducing risk.

Guide 51 [9] states "The content of an instruction should provide product users with the means to avoid harm caused by a product hazard that has not been eliminated or reduced, enable product users to make appropriate decisions concerning the use of the product...."

When using information for safety as a Risk Control, consider the following:

To whom – To whom will you be communicating? A trained clinician? A home user? Elderly? Youth? How well is it perceived and comprehended?

How – Will you be using words? Icons? What type of media (printed, digital screen)? What location/timing of the information? What level of detail?

What – What are the hazardous conditions? What are the consequences of exposure and what should be done to prevent Harm? In what priority should actions be taken?

Information for safety can be in many forms, such as Warnings, Cautions, contraindications, and instructions. The location for information for safety could be in user manuals, in labeling that is attached to the medical device, in graphical user interfaces such as screens, or even in the form of audio or tactile annunciations.

The FDA guidance on medical device patient labeling [42] defines Warning as a labeling that alerts the reader about a situation which, if not avoided, could result in death or serious injury. It may also describe potential serious adverse reactions and safety hazards. Warnings are reserved for the most significant safety risks.

The FDA guidance [42] states that the word Caution is generally used as the signal word for a Precaution statement. The term Precaution is used for the statement of a Hazard alert that warns the reader of a potentially Hazardous Situation which, if not avoided, may result in minor or moderate injury to the user or patient or damage to the equipment or other property.

The primary intention should be avoidance of Hazardous Situations, either by prevention of Hazards, or by prevention of exposure to Hazards. Secondarily, information for safety should offer guidance on remedial actions if Harm has happened. The priority of actions should be commensurate with the level of risk, and be properly communicated to the users. Use of word such as: "Danger," "Warning," "Caution," "Alert," "Note," etc. could indicate the priority of the information for safety.

The three guiding principles in the utilization of information for safety as Risk Control are:

Inform Motivate Enable

According to Guide 51 [9] labeling should be:

- "conspicuous, legible, durable and understandable;
- worded in the official language(s) of the country/countries where the product or System is intended to be used, unless one of the languages associated with a particular technical field is more appropriate;
- concise and unambiguous."

With respect to legibility, consider the user population. What visual acuity can be expected? Under what lighting conditions will the user typically use the device? Use AAMI HE75 [27] for guidance on font sizes for visual displays.

The labeling should be durable and not fade, rub off, smear, or separate from its intended location during the expected life of the device.

Whether in audio or visual format, the information for safety should be understandable by the users. In today's global economy, with so many languages and cultures this is a challenging requirement. Even the choice of colors may convey one thing in one culture, and another in a different culture. For example, in the American culture the color yellow is usually an indication of a Warning. But in the Japanese culture yellow is an indication of sickness and ill health.

Translations are a sensitive and critical aspect of communication of information for safety. In many companies the information for safety is drafted in a central language, usually English, and then translated to other languages. The problem is that not all concepts can be directly translated from one language to another. Here are some examples of potential sources of confusion in translations:

English: Bend the wire into a J, or hockey stick shape.
Problem: Many languages don't have the letter J. Many cultures are unfamiliar with hockey.
English: When the alarm goes off do . . .
Problem: Does this mean when the alarm begins, or when the alarm ends?

Sometimes a translated word has one connotation in one geography, and another in a different geography. French in France is not the same as French in Canada; Portuguese in Portugal is not the same as Portuguese in Brazil, and English in the USA is not the same as English in the UK. For example:

First Floor
USA: Ground floor
UK: The floor above the ground floor
Chips
USA: Thinly sliced, deep-fried, baked, or kettle-cooked crunchy potatoes (crisps in the UK)
UK: Cut and deep-fried potatoes, as in Fish and Chips

Another element of the guidance from Guide 51 [9] is *conciseness and unambiguity*. This is a challenge for technical writers, particularly with respect to product labeling and screen user-interfaces where space is limited.

As stated earlier, an important requirement for information for safety is that it must be demonstrated to be effective. This demonstration is typically done as part of summative usability testing. Through objective evidence, it must be shown that users will refer to, comprehend, and use the information for safety, such that it produces the expected reduction in risk.

18.5 DISTINCTION OF TYPES OF INFORMATION FOR SAFETY

FDA Guidance [42] says: by the time users get to the point of reading the information on Warnings and Precautions, they have probably already decided to use the device. At this point they need specific information to safely use the device. But how to decide which type of information to provide for the users? Below, an explanation of the meaning and intention of each type of information for safety is provided as an aid in the choice of the type of information for safety.

- **Contraindications** – those are the uses for which we have objective evidence that Benefits do not outweigh the risks. In other words, these are the DON'T DO things.
- **Limitations** – those are boundaries for the Intended Uses. For example, a device may be suitable for adults, but not suitable for a child with the same disease. So, age would be a limitation. The difference with Contraindication is that here we have objective evidence that Benefits outweigh the risks for the uses within the limitations, but do not have objective evidence for uses outside the limitations.
- **Warnings** – a message to alert the user that certain actions or conditions could result in significant unintended injuries to patients/users. "Significant" could be interpreted as an injury in the Severity classes of Fatal, Critical, or Major. Note that some medical devices such as electrosurgery devices cause injuries (tissue cut) as the Intended Purpose of the device. Here, significant injuries would be injuries that are beyond the expected clinical use of the medical device.
- **Precautions** – a message to the users to inform them of preparatory actions to avert injury to patients/users. The FDA definition uses Precautions for minor to moderate injuries. Examples: have an empty stomach; do not take blood thinners; how to predict device failure/expiration; etc.
- **Cautions** – a message to alert the user that certain actions or conditions could result in minor to moderate unintended injuries to patients/users.

18.6 SAMPLE RISK CONTROLS

Risk Controls should be understandable by Regulatory reviewers. Writing highly technical safety requirements may obscure the essence of the Risk Control. A way to achieve understandability is to write the Risk Control as a narrative of intention to reduce the risk of a Hazard. Such intentions are achieved via various means, such as System Requirements, operating procedures, conformance to recognized standards, etc. Below are some example Risk Controls that can be used as models.

- The device maintains a targeting accuracy of ± 0.1 mm
- Current leakage in the applied part is limited to 100 μA per IEC 60601-1
- The device can withstand up to 10N of tensile pull-force
- Access-door interlock shuts down emitter
- Standard of care is to take the product out of sterile-pack with sterile gloves in the sterile-field, in the OR

Traceability analysis would link the stated Risk Controls to all of their means of implementation, and their verifications of implementation and effectiveness.

18.7 RISK CONTROLS AND SAFETY REQUIREMENTS

It is best to link Risk Controls to product requirements. This takes advantage of the formality with which requirements are tracked, change-controlled, traced, and verified. This formality also assures that Risk Controls will be implemented and that if any change to a requirement is contemplated, the impact of that change on the Risk Control will be evaluated.

When a requirement is linked to a Risk Control, it becomes a safety requirement. It is a good practice to tag safety-requirements for ease of discernment for the benefit of other functional groups such as: R&D, Quality, Test Engineering, and Regulatory.

The connection between safety requirements and risk management is maintained via traceability. Fig. 55 depicts the connections between safety-requirements and Risk Controls.

18.8 COMPLETENESS OF RISK CONTROLS

ISO 14971 [1] requires that the manufacturers ensure that the risks from all identified Hazardous Situations are considered, and all Risk Control activities are completed.

To meet this requirement, it is important that the risk management process is faithfully followed. This would ensure that all the relevant Hazards and Hazardous Situations are identified. Recording all the relevant Hazards and Hazardous Situations in the RACT, and logging their respective Risk Controls, Residual Risks, and relevant Harms would demonstrate compliance with this requirement of ISO 14971 [1]. Verification activities ensure that the claimed Risk Controls are indeed implemented.

CHAPTER 19

Verification of Risk Controls

Abstract

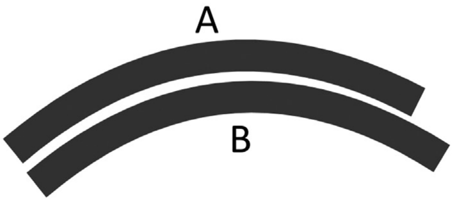
Risk Controls must be verified for both implementation and effectiveness. Objective evidence is required to establish and support claims of verification. In general, testing is the means to provide objective evidence. Test methods must be validated. Several methods of testing are cited. Leveraging conformance to standards as a means of verifying implementation and effectiveness of Risk Controls is discussed.

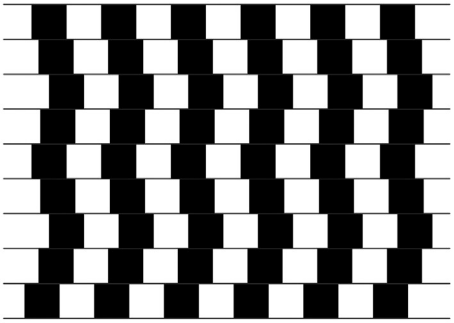
Keywords: Risk Controls; verification; testing; implementation; effectiveness

Risk Controls must be verified for implementation and effectiveness. Objective evidence is required to establish and support claims of verification.

The primary means of verification is testing. But sometimes visual inspections are used to verify the implementation of a Risk Control. For example, if the Risk Control is the installation of a red light, visual inspection for the presence of the red light is the easiest way to verify implementation. Caution should be exercised with respect to reliance on visual inspections. Particularly if the visual inspection is done by one tester over a long period of time. It has been shown that after 2½ hours of continuous visual inspection, the propensity for error increases significantly. Also, visual inspection is subjective. So, a clear description and definition of what constitutes a failure is important.

If you are using visual inspections, be alert to optical illusions. There are many examples of optical illusions such as the images below. In the left image, (A) appears to be smaller than (B), while they are the same length. In the right image the horizontal lines appear to not be parallel, when in fact they are parallel.





Safety Risk Management for Medical Devices
DOI: https://doi.org/10.1016/B978-0-323-85755-0.00019-9

To get the most value from testing, it is important to provide clear and thoughtful objectives and expectations. Testers need to know what is important and needs their attention. Often people are given ambiguous or limited objectives but are expected to focus on many things. In such circumstances, it is easy for a tester to miss the things that they should notice. For example, imagine a device that has a motor that must reach a minimum of 1000 RPM. The test pass-criterion is the RPM measurement, but during testing the motor exhibits unexpected vibrations. Since absence of vibration is not part of the test pass-criteria, the test would be marked as PASS, while the information about the vibration might be very important to the system developers.

Whether attribute or variable testing is chosen, it is best if the selected sample size for testing is based on the safety risks. Sections 20.2—20.4 provide details about risk-based sample size selection.

19.1 VERIFICATION OF IMPLEMENTATION

Verification of implementation means providing objective evidence that the Risk Control is implemented. It can be in the form of test, inspection, demonstration, or analysis. Ensure that the subject of the test represents the final design. Otherwise, you'll have to repeat your test when the final form is available.

Include in your test protocols, any pre-conditioning, configuration, and adaptation if applicable. The protocol must include pass/fail criteria and the test method must be validated. The test report should include:

- The date on which the test was executed
- The names of individuals who performed the test
- The test protocol and methods used
- Identification of any equipment/tooling used in the test including calibration and qualification evidence. If software is used as part of test equipment, refer to evidence of validation of that software
- Collected data, or reference to it
- The test results and pass/fail declarations
- Any additional observations, or deviations from the test protocol

Be sure to retain all test subjects, raw data, and anything else that you would need to defend or replicate your test results, in case of an audit.

Let's take the example of an implantable medical device. A potential Harm from this device is infection; the Hazard would be microbial contamination. The Risk Control would be sterilization. This Risk Control would be found as a safety requirement in the System Requirements Specifications. Through requirements flow-down, and traceability we should be able to find the design outputs, e.g., packaging that serves as a sterile barrier, and process specifications that include a sterilization step. The IFU would also mention that the product is sterilized, by what method, and any special handling requirements.

To verify the implementation of this Risk Control, we would look for design outputs such as a drawing that shows the product is protected by a sterile barrier. This would be by inspection. We would look for test data that shows the sterile barrier meets its requirements. We would also examine the manufacturing process-design and identify the sterilization process step. We would look for evidence of validation of the manufacturing process. Additionally, we would inspect the IFU to find mentions of the fact that the product is sterile, by what method and any special handling requirements. This only verifies that the Risk Control is implemented. To verify whether it is effective see Section 19.2.

19.2 VERIFICATION OF EFFECTIVENESS

Verification of effectiveness means providing objective evidence that the Risk Control is effective at reducing risk. Many methods can be used to establish that a Risk Control is effective in reducing risk. For example:

- **Usability testing** – summative tests with real or surrogate users to show that the Risk Control measure reduces the risk. For example, if in a formative test using an earlier user-interface design, it was found that half of the testers were making a particular mistake, and in the summative test we show that with the final design only 10% of the testers make the same mistake, we can conclude that the Risk Control was effective in reducing risk.

- **Clinical study** – These are formal controlled-studies performed on humans, typically to establish physiological effects. For example, let's say an older version of a pacemaker had a 10% rate of skin erosion in patients, and we have implemented a new design. A clinical study shows that the new design results in less than 5% of the test participants experiencing skin erosion. This would verify the effectiveness of the new design in reducing the risk of skin erosion.

- **Pre-clinical study** – These are formal studies performed on animals, or cadavers. They are used to test properties such as biocompatibility, biostability, toxicity, and efficacy. For example, let's say a new coating material is believed to reduce the rate of infection of an implantable device. In a pre-clinical study two samples of a device, one with the new coating and one without may be implanted in each animal. If under the same conditions, the samples with the new coating show a lower rate of infection, this would verify the effectiveness of the new coating in reducing the risk of infection.

- **Analysis and simulation** – It may possible to verify the effectiveness of a Risk Control by analytical and simulation means. For example, if a new algorithm in implantable defibrillators is promised to be more effective in detection of ventricular fibrillation (VF), we could load the old and new algorithms in two copies of the same defibrillator, and play recordings of a set of ECGs of ventricular fibrillation in both devices. If the device with the new algorithm detects more VF episodes than the old algorithm, this verifies the effectiveness of the new algorithm.
- **Leverage verification** – in some cases the simple functionality of a Risk Control is proof of its effectiveness in controlling risks. For example, if a fuse is used to prevent high current flow, a verification test could show that the fuse is installed, and it functions per the specification to cut the current flow when current flow exceeds a certain limit. The same test also verifies the effectiveness of the Risk Control in reducing the risk of electric shock.

One easy way to establish effectiveness of Risk Controls is by conformance to harmonized standards. For example, IEC 60601-1 [7] gives allowable electrical leakage current values, and even describes how to perform the verification tests. If you can demonstrate conformance to IEC 60601-1 [7] with respect to electrical leakage current, you can presume that your Risk Controls are effective in reducing the risk of electrical shock. Another good source is IEC 60601-1-8 [26]. This Standard provides guidance on alarm systems in medical electrical systems. It provides requirements for alarms of high, medium, and low priorities, and says what color they should be, whether they should be flashing or constantly on, and if flashing, at what frequency and duty cycle. This is very beneficial to the manufacturers because it is very difficult to provide objective evidence that, e.g., a particular frequency of flashing red light is effective in reducing risk. But conforming to IEC 60601-1-8 [26] can be used as evidence of effectiveness of the alarm.

It is important that the test samples, test environment, and testers are representative of real life for the medical device. For example, if a medical device is intended for use by the surgical staff in an operating theatre, then the summative test should create a simulation of the ambiance of an operating theatre and utilize testers who are either members of a surgical team, or a good facsimile thereof. For home-use products, usability testing should use people who are representative of the Intended Users of the product. For example, if the product is intended for home-use by elderly people in France, then the testers should include elderly French people. This is because cultural and language variation from market to market makes a difference on how the users of the product perceive and understand the user-interface and instructions that are provided.

If information for safety is used as a Risk Control, in accordance with IEC 62366-1 [19], that information needs to be tested on representative users to ensure that the information for safety is perceivable and understandable to the user, and it is actually effective in reducing risk. This means for example, if the user profile is elderly people with poor eyesight, the font and contrast of the information should be suitable for the user-profile group.

Risk Controls should be verified for effectiveness not only individually, but also in combination with each other. It is possible that activation of one Risk Control might adversely impact the effectiveness of another Risk Control.

CHAPTER 20

On Testing

Abstract

Testing, in general, is not a Risk Control. Rather, testing can help to identify errors in design or implementation. Testing can also be used to build confidence in the design choices, and verify the implemented Risk Controls. One of the benefits of risk management is to provide a basis for risk-based sample-size determination for testing. This in turn can help steer resources toward the safety-critical aspects of the System.

Keywords: Testing; Risk Control; sample size; confidence; reliability; concept testing; verification testing; validation testing

> *Testing can show the presence of errors, but not their absence.*
>
> ***Edsger Dijkstra, computer scientist (1930–2002).***

Testing, in general, is not a Risk Control. Rather, testing helps to identify errors in design or implementation. Testing can also be used to build confidence in the design choices, and to verify the implemented Risk Controls. An exception to this is when testing is used to eliminate faulty products from reaching the market. For example, quality control testing at the end of the manufacturing process may be able to detect and reject products that have a safety defect. This type of testing does not eliminate the Hazard, but does eliminate exposure to the Hazard, and therefore it influences the P1.

20.1 TYPES OF TESTING

During the course of product development, many types of testing are employed. Below, a few examples that are relevant to Risk Management are cited.

– Concept testing
  This type of testing is done to gain insights into the physics of operation of the medical device. It can demonstrate the feasibility of a concept and give insights into Failure Modes. This type of testing can support assertions of failure Occ ratings. Concept testing is sometimes confused with mitigations, or Risk Controls. It is not the same. Testing does not reduce the rate of occurrence of a failure – it only supports the assertion of Occ rating.

DOI: https://doi.org/10.1016/B978-0-323-85755-0.00020-5

– Verification testing
  In the domain of Risk Management, verification testing is performed to demonstrate that Risk Controls are implemented as intended.
– Validation testing
  In the domain of Risk Management, validation testing is performed to demonstrate that the Risk Controls are effective in reducing risk.
– Quality Control (QC) testing
  This type of testing is relevant to the manufacturing process. It can be used as a Risk Control to prevent defective parts/products from escaping to the field.

20.2 RISK-BASED SAMPLE SIZE SELECTION

It is wise to choose the rigor of testing based on the safety risks related to the subject of the test. Choice of the sample size is an indication of the level of rigor. A higher sample size connotes higher confidence in the test results. This strategy can also have an economic benefit in that for low-risk test subjects, we can reduce the sample size and thereby save on product development costs.

The main question is: how many samples should be used for testing a safety-related requirement? Before we dive into the methodology, it is beneficial to define two important terms: *Confidence* and *Reliability*.

> ***Confidence*** *($1 - \alpha$): Probability that if the test passes, the requirement is met by at least R% of the population. Where R is the* ***Reliability****.*

Safety-requirements can be tested as variable, or attribute. Attribute testing results are discrete, e.g., True/False or Pass/Fail, whereas variable test results are numerical values on a scale. In the following sections a strategy is offered on how to make risk-based decisions on sample sizes.

20.3 ATTRIBUTE TESTING

Requirements that are attribute-tested produce results that are discrete, usually binary. For example, the requirement: "The implantable device shall be able to withstand a 3T MRI environment without damage" would be attribute-tested. Multiple samples would be exposed to a 3T MRI environments, and then tested to see if they suffered any damage.

Using the BXM method, the following steps can be utilized to make a risk-based determination of sample-sizes for attribute-testing. The core idea is to identify the risk-levels associated with the safety requirements and then determine the sample sizes commensurate with their risk levels. Safety requirements are those requirements that realize the Risk Controls.

Using the RACT as a source for risk determination, follow these steps:

Step 1 – Examine the RACT to identify the Risk Controls which link to the safety requirement in question.
Step 2 – Identify the Hazards that are linked to the Risk Controls which were identified in step 1.
Step 3 – For the aggregate of all the Hazards that were identified in step 2, compute the Residual Risk in each Harm Severity-class. Use Boolean algebra's De Morgan's Theorem and Law of Involution.
Step 4 – Within the aggregate, identify the Harm Severity class with the peak risk-value.
Step 5 – Use Table 30 to determine attribute-test sample-size that correlates to the Severity class, which was identified in step 4.

Note – the sample sizes in Table 30 are based on zero failures in all the tested samples.

Table 30 Confidence/Reliability (C/R) and Attribute Sample Sizes

Fatal	Critical	Major	Minor	Negligible
Conf./ Reliability	Conf./ Reliability	Conf./ Reliability	Conf./ Reliability	Conf./ Reliability
95/99	95/95	90/90	80/80	70/70
Attribute Sample Size	Attribute Sample Size	Attribute Sample Size	Attribute Sample Size	Attribute Sample Size
299	59	22	8	4

Note that the Confidence/Reliability numbers in Table 30 are merely suggestions. You should decide the numbers that are appropriate for your QMS. The main point is to have a defensible and documented rationale for your decisions on sample size selection.

Table 31 shows sample sizes for other confidence and reliability combinations, based on the binomial probability distribution. Assumption: zero failures in all the tested samples.

Table 31 Attribute-Test Sample Sizes

Reliability Lower Bound	95% Confidence	90% Confidence
70%	n = 9	n = 7
80%	n = 14	n = 11
85%	n = 19	n = 15
90%	n = 29	n = 22
95%	n = 59	n = 45
96%	n = 74	n = 57
97%	n = 99	n = 76
98%	n = 149	n = 114
99%	n = 299	n = 230

20.4 VARIABLE TESTING

Variable testing of safety requirements produces numerical results along some scale. Example requirement: "Length of the connector shall be 3.00 ± 0.25 mm."

Using the same method that was described in steps 1–4 of Section 20.3, determine the Harm Severity class for the requirement in question. Identify the chosen confidence/reliability values. For variable test data, the statistical distribution of the data matters. Do a normality test on a preliminary dataset, e.g., a confirmation run. If the data distribution is normal, calculate the average and standard deviation of the data. Using a statistical software such as Minitab® iteratively compute the minimum sample size needed to obtain a normal-distribution tolerance-interval that is narrow enough to fit within the specification tolerances. In the example of the connector above, that would be within ±0.25 mm. If the computed sample size comes out to be very small, you can increase it to a larger number, e.g., 10 or 15.

If your data is not normal, you can perform a conversion of the data to make it normal, including the specification limits.

If your data indicates a different distribution, such as Weibull, Lognormal, etc., still find the minimum sample size such that the tolerance interval falls within the specifications. You may need to consult a statistician.

Another method that is used is to correlate the risk level to process capability. For example:

For Fatal risk class – CpK 2.0
For Critical risk class – CpK 1.5
For Major risk class – CpK 1.0
For Minor/Negligible risk class – CpK 0.8

CHAPTER 21

Risk Evaluation

Abstract

ISO 14971 requires the manufacturer to determine if the residual risks posed by the medical device are acceptable using the criteria defined in the risk management plan. Three methods of risk evaluation are presented: qualitative, semi-quantitative, and quantitative. A method for determining state-of-the-art is presented.

Keywords: Risk evaluation; residual risk; qualitative; semi-quantitative; quantitative; state-of-the-art

ISO 14971 [1] requires the manufacturer to determine if the Residual Risks posed by the medical device are acceptable when compared against the criteria defined in the Risk Management Plan. Although preliminary Risk Evaluations can be done before the completion of design, what matters is the final evaluation of the Residual Risks of the medical device, after all the Risk Controls have been implemented.

ISO 14971 [1] requires that the manufacturer evaluate the acceptability of Residual Risk for:

- Individual risks
  - each Hazard
  - each Hazardous Situation
- Overall

The Standard [1] does not prescribe a method for Risk Evaluation and allows the manufacturer to choose an appropriate method. Nor does the Standard specify whether the same or different criteria are to be used for the evaluation of individual Residual Risks and the Overall Residual Risks. The choice is left up to the manufacturer.

Depending on which method of Risk Estimation is chosen: qualitative, semi-quantitative, or quantitative, the evaluation method varies. It should be noted that no matter which method is chosen, the presented data is intended to support the decision on risk acceptability, not replace it.

21.1 APPLICATION OF RISK ACCEPTANCE CRITERIA

For some of the Hazards that a medical device presents, it may be possible to identify an applicable product safety standard, which offers specific requirements for safety that

Safety Risk Management for Medical Devices
DOI: https://doi.org/10.1016/B978-0-323-85755-0.00021-7

address some or all of the risks of a medical device. ISO/TR 24971 [15] advises that when such a standard is found, "the manufacturer can presume that, in the absence of objective evidence to the contrary, meeting the requirements of the relevant standards results in particular risks being reduced to an acceptable level."

In the view of the European community, harmonized standards should be sought first. If no harmonized standard is available, then other national or international recognized standards or publications should be considered.

Comparison of the risk of a medical device with the state-of-the-art is another way to establish acceptable risk. State-of-the-art in the context of ISO 14971 [1] is defined as "Developed stage of technical capability at a given time as regards products, processes and services, based on the relevant consolidated findings of science, technology and experience." Note 1 of the same definition clarifies that: "The state of the art embodies what is currently and generally accepted as good practice in technology and medicine. The state of the art does not necessarily imply the most technologically advanced solution."

If it can be shown that for the same Benefit, the risk of a medical device is less than or equal to the state-of-the-art, then it follows that the risk of the medical device is acceptable. Conversely, if you can show that for the same level of risk, your product delivers more Benefit, you could argue that the risk of the medical device is acceptable.

21.1.1 How to Determine the State-of-the-Art

State-of-the-art in this context refers to the best current treatment of a medical condition for which the subject medical device is indicated. To determine the state-of-the-art, examine:

- Applicable standards
- Current consensus, guidelines, and guidance documents from authoritative organizations
- Information regarding the medical condition's natural course
- Alternative treatments for the medical condition (e.g., pharmaceutical)
- Use of similar devices for the medical condition (benchmark devices)

Review the published scientific literature to find applicable papers related to the medical condition and its treatment. Sound inclusion and exclusion criteria are very important as they may be subjected to scrutiny at a later date.

If the subject medical device is a new iteration of an existing, approved device that is produced by the same manufacturer, evaluation of the relevant field data in the manufacturer's files could be another means of collecting data on state-of-the-art.

It should be noted that 'good practice' in the definition of state-of-the-art does not limit the scope to medical devices. If, for example, a pharmaceutical option is the currently and generally accepted best treatment for a disease, then the risk of that pharmaceutical option sets the bar against which to compare the risk of a medical device that provides a therapeutic alternative for the same disease.

The BXM method uses quantitative methods for Risk Evaluation. As such, the risk acceptability criteria also need to be quantitative. State-of-the-art risk for each Harm Severity-class is defined as the level of risk that the public accepts for the Benefit that is delivered by the state-of-the-art alternative. For example, let's say a comparable medical device, which has been in the market for some time, has a reported history of five cases of permanent, irreversible injury (Critical class) to patients on a base of 10,000 patient-years of use. Since the predicate device is approved and continues to be marketed as a sufficiently safe device, the risk level of 0.05% per patient-year can be construed as an acceptable risk limit for the Severity class of Critical, for that type of device/therapy.

In some cases, such as a when a new and novel device is produced, or when a significant iteration on an existing device is made to deliver novel new therapies, state-of-the-art data may not be available. In such cases, risk acceptance criteria are derived from evaluating clinical evaluation data, and formal Benefit-Risk analyses. See Chapter 23 for more information on how to perform a Benefit-Risk Analysis. It is noteworthy to realize that in such novel situations, the device under analysis could establish the state-of-the-art.

It is possible that what is currently and generally considered good practice in technology and medicine is surpassed by new, more advanced technology and practice that are sufficiently developed and viable for inclusion in the medical device. In that case, the state-of-the-art is the consolidation of what is currently and generally considered good practice, and the new, more advanced technology and practice.

Stakeholder concerns – It is well established that the perception of risk often differs from empirically determined risk estimates. Therefore, the perception of risk from a wide cross section of stakeholders should be taken into account when deciding what risk is acceptable. To meet the expectations of public opinion, it might be necessary to give additional weighting to some risks [17]. For example, people fear flying more than driving a car. As such, a large weighting factor has been put upon flight safety. The FAA sets the acceptable max probability of a catastrophic failure per flight hour for commercial aircraft to 10^{-9}, defined as extremely improbable. To put this in perspective, if an aircraft flies 10 hours per day, every day, it would take 273,973 years to complete 10^9 hours of flying.

As a practical means of measuring the public opinion about the tolerance of risk, it may be acceptable to presume that the concerns of the identified stakeholders reflect the values of society and that these concerns have been taken into account when the manufacturer references a reasonable set of stakeholders.

21.2 RISK EVALUATION FOR QUALITATIVE METHOD

In the qualitative method, risks are stratified into relative rankings from high to low. In the example offered in Section 17.1, three ranks of high (red), medium (yellow), and low (green) were devised.

For Hazards or Hazardous Situations for which applicable harmonized, international or national standards can be found, determine Residual Risk acceptance by evaluation of compliance to those standards. For other Hazards and Hazardous Situations compare the individual Residual Risks, and the Overall Residual Risk to state-of-the-art. A method for establishing the state-of-the-art using risk-profiles was described in Section 13.3.1.

In the absence of applicable standards, or state-of-the-art information, you could leverage the NBRG Consensus Paper [43] and consider risks as acceptable, unless they result in death, or serious deterioration in health. Ultimately, you may need to rely on subjective expert opinion to qualitatively judge the acceptability of risks of your device in consideration of the Benefits that it offers.

21.3 RISK EVALUATION FOR SEMI-QUANTITATIVE METHOD

Similar to the qualitative method, for the semi-quantitative method, strive to use compliance with applicable harmonized, international or national product safety standards as indication of risk acceptance. And, where applicable standards are not available, compare to the state-of-the-art, or refer to Benefit-Risk Analyses.

In the semi-quantitative method, we can numerically compare the probability of occurrence of Harms against the state-of-the-art. However, the Severity is not easily comparable. That is, you could say a particular Harm, e.g., infection, has a Severity of Major and could happen with a probability 10^{-4}. That fills one cell in the risk matrix (see Section 17.2, and Fig. 48). But the state-of-the-art rating of Severity may not match your Severity rating. That is, the manufacturer(s) of the products that inform the state-of-the-art may have different definitions for the Severity classifications than you do.

In the semi-quantitative method, the comparison with the state-of-the-art is easier than in the qualitative method, but still equivocal.

21.4 RISK EVALUATION FOR QUANTITATIVE METHOD

The BXM method uses quantitative methods for Risk Estimation and evaluation. In the quantitative method as in the other methods, where possible, use compliance with applicable harmonized, international or national product safety standards as indications of risk acceptance. Where applicable standards are not available, compare to the state-of-the-art, or refer to Benefit-Risk analyses.

In the quantitative method, comparison with the state-of-the-art is relatively straightforward. Compute the Residual Risk for a Hazard, a Hazardous Situation, or overall in the five Severity classes of Fatal, Critical, Major, Minor, and Negligible. See Section 17.3 for a detailed explanation on how to compute risk in five Severity classes. If the computed Residual Risk for any Severity class is larger than the acceptable risk limits that are spelled out in the RMP, then the risk is not acceptable. Otherwise, the risk is acceptable.

Just because a risk computes to be unacceptable, it doesn't mean the medical device cannot be released to the market. If Benefit-Risk Analysis shows that the Benefits of the device outweigh its risks, it may still be possible to get regulatory approval for the medical device.

CHAPTER 22

Risk Assessment and Control Table

Abstract

Every risk management process typically brings the results of the hazards analyses, risk estimations, and risk evaluation into a table. This is usually a large table and is called by many names. Examples: risk matrix, risk table, risk chart, product risk assessment, and risk analysis chart. The Risk Assessment and Control Table (RACT) tells the story of how each System Hazard manifests itself, what causes it, how exposure to that Hazard happens, and what Harms could ensue. The RACT also captures the Risk Controls and Risk Control option analysis. Additionally, the RACT computes and evaluates the residual risks: both individual risks and overall System risk.

Keywords: Risk Assessment and Control Table; RACT; Risk Control option analysis; risk evaluation; residual risks

Every risk management process typically brings the results of the hazards analyses, Risk Estimations, and Risk Evaluation into a table. This is usually a large table and is called by many names. Examples: risk matrix, risk table, risk chart, product risk assessment, Risk Analysis chart, etc. The BXM method calls this table the Risk Assessment and Control Table (RACT). You can find a template for the RACT in Appendix B – Templates.

The RACT is a tool of risk management that integrates the results of all the analyses performed at lower levels of the System and enables the computation of Residual Risks for the System. The RACT tells the story of how each System Hazard manifests itself, what causes it, how exposure to that Hazard happens, and what Harms could ensue. The RACT also captures the Risk Control option analysis. That is, it shows what Risk Control options were considered and implemented. Additionally, the RACT computes the risks, both individual risks and overall System risk. The RACT can also evaluate the risks by comparing the computed risks against the risk acceptability criteria.

The BXM RACT template that is provided in Appendix B – Templates does not show a pre/post risk. Only the final risks of the medical device are shown. The reasons for this are:

1. The final residual risks of the device are what matter to the patient. Also, it is the final residual risk that is used to evaluate the Benefit-Risk ratio of the device.

DOI: https://doi.org/10.1016/B978-0-323-85755-0.00022-9

2. Manageability of the RACT size. RACTs are typically huge tables and span multiple pages. Page management and reading of a larger RACT is more difficult.

If you desire to track the pre/post risks, the modification of the RACT template is easy. Simply replicate columns P1 through Negl-Risk, and label them 'pre.' Alternatively, as the RACT is a configuration-controlled living document, which continues to evolve, you can reference an earlier version of the RACT as the 'pre-risk,' and use the last version of the RACT as the 'post-risk.'

Tip Besides the Indicated Use, remember to include in your risk analysis, other normal uses of the device, such as repair, maintenance, and disposal.

22.1 RACT WORKFLOW

In the following sections the workflow for RACT is described. The workflow description corresponds to the template that is provided in Appendix B – Templates.

22.1.1 Examine the CHL

Start by citing all the applicable Hazards from the CHL in the Hazard column. Entries in the CHL that are not applicable need to be rationalized and documented. If new Hazards are identified in the underlying analyses, include them in the RACT and initiate an update to the CHL.

22.1.2 Capture End-Effects with Safety Impact

Examine the System DFMEA, the System PFMEA (for integral Systems), and the System UMFMEA. Import the End-Effects that have a Safety Impact of Y. These End-Effects go into the Hazards column of the RACT.

22.1.3 Revisit the PHA

Revisit the PHA. Capture any additional relevant information from the PHA. For instance, you may have identified hazards in the FTA that occur under non-failure conditions.

22.1.4 Populate the Initial Cause and Sequence of Events Columns

For the entries that are collected from the underlying FMEAs, capture the Initial Cause of Hazard, and Sequence of Events from the FMEAs and populate the RACT.

It is possible that you may identify additional initial Causes and Sequences of Events. Add those to the RACT.

For the Hazards that are not the result of any failure, the Sequences of Events are typically found in the FTA.

22.1.5 Populate Hazardous Situations Column

Define the Hazardous Situations. A Hazardous Situation is where persons/property/environment are exposed to Hazards. For example, an implantable defibrillator battery may experience high current discharge and overheating. This would create a Hazardous Situation if the device is implanted in a patient. Another example: a medical device may have a sharp edge. If a user touches the sharp edge, they could experience a cut. This describes a Hazardous Situation.

22.1.6 Populate the P1 Column

P1 is the probability of occurrence of the Hazardous Situation. Occ ratings from the System FMEAs can be inputs to the derivation of P1 values. For example, in the case of implantable devices, exposure is automatic. P(Hazard)=P(Hazardous Situation). But in other cases, where exposure to the Hazard is probable, P1=P(Hazard) × P(exposure). Ideally, P1 numbers are based on actual field experience and are derived from PMS data. Otherwise, you can use your best expert judgement as your starting numbers and update them as field data become available.

22.1.7 Populate the Risk-Controls Columns

The Risk-Controls column is divided into three sub-columns:

- Inherently Safe Design and manufacture (SD)
- Protective Measures in the medical device itself or in the manufacturing process (PM)
- Information for Safety and, where appropriate, training to users (IS)

This is to support Risk Control option analysis as required by ISO 14971 [1] Section 7.1. In the Risk-Controls columns write narratives that describe the strategies to control the risks of the Hazardous Situations. The Risk Controls could apply to the initiating Cause, or somewhere in the sequence of events, or by preventing exposure to Hazards. Capture relevant mitigations from the underlying FMEAs. At the discretion of the analyst, the safety requirement references may be entered in the Risk Control columns.

Note that it is possible that application of a Risk Control for one Hazard may introduce new Hazards, or Hazardous Situations, or exacerbate an existing risk. In this case mark a Y (Yes) in the column "New Risk?" and address the new Hazards/Hazardous Situations or affected risks in the RACT.

The intention is to reduce the Overall Residual Risk of the device. Therefore, it is possible that a viable Risk Control is not implemented in consideration of the Overall Residual Risk of the device. Such decisions should be documented in support of Risk Control option analysis.

22.1.8 Populate the Harm Column

Entries in the Harm column are taken from the HAL. Per the BXM method, all the potential Harms that the product can induce have been accounted for in the HAL. If a Hazardous Situation could precipitate multiple Harms, replicate the Hazardous Situation row and create a new row for each related Harm.

22.1.9 Populate the P2 Columns

P2 numbers are simple lookups from the HAL. They represent the probabilities of different outcomes from the same Harm.

22.1.10 Compute Residual Risks

For each row multiply P1 by the five P2 numbers to compute risk of Harm in five Severity classes. This can be easily automated in a spreadsheet.

22.1.11 Risk Evaluation

In the BXM method Risk Evaluation is simply the comparison of the computed residual risks against the risk acceptance criteria from the RMP. If a computed residual risk is less than, or equal to the acceptable risk limits, it is acceptable. Otherwise, the computed residual risk is unacceptable. This can easily be automated in a spreadsheet, or in a software tool.

If the BXM method is not used, the risk must still be evaluated using the criteria and methods that are stipulated in the RMP.

22.2 INDIVIDUAL AND OVERALL RESIDUAL RISKS

In a quantitative risk management method, such as the BXM method, the individual, and Overall Residual Risks can be computed using Boolean algebra and evaluated automatically.

It is pointed out that the use of Boolean algebra may create a perception of accuracy and precision which is not warranted. In many cases the computed individual risks are based on estimates, or expert judgment. In other cases, real-world data is used, but the confidence intervals are non-uniform. For these reasons, the use of Boolean algebra should be viewed as a convenient and objective way of aggregation of the individual risks, not as a precise final measurement of the Overall Residual Risk.

While the BXM quantitative method conveniently presents the Overall Residual Risk of the device in all five Severity classes, the final decision on Overall Residual Risk acceptability should include expert judgment by specialists who have knowledge and experience with the medical device and the related disease/physical conditions. The experts who evaluate the Overall Residual Risk of the device should have an appropriate level of independence from those who participated in the design and development of the device.

ISO 14971 [1] requires the disclosure of the significant Residual Risks of the device. The RACT could be used as a tool for distinguishing the significant Residual Risks. For example, you might decide to disclose all individual Residual Risks that did not meet the acceptance criteria but were accepted when weighed against the Benefits of the device. Additionally, you might disclose all individual Residual Risks in the top three classes (Fatal, Critical, Major) that are within 5% of the risk acceptance criteria, i.e., close to the edge.

For qualitative or semi-quantitative methods, the manufacturer would need to create internal policies for the determination and evaluation of risks. For example, these could be in the form of using risk matrices such as those shown in Fig. 47, or Fig. 48, and establishing criteria such as: no individual risks in the red zone.

The criteria for evaluation of individual vs. Overall Residual Risks may be the same, or different, depending on the policy of the manufacturer.

22.3 INHERENT RISKS

The use of medical devices inherently involves some degree of unavoidable risk. This is the inherent risk of a medical device. A part of the inherent risk is related to the device itself, which is the Residual Risk of the device. The manufacturer can implement Risk Controls to reduce those risks. Another part of the inherent risk is external to the device. For example, if a patient wants to have an implantable pacemaker, an unavoidable risk is: the risk of surgery. The manufacturer has limited influence and control over the external risks. In the pacemaker example above, the manufacturer cannot control the conduct of the surgical staff, but can provide safety instructions, and make the design of the device such that it is least prone to errors and complications during the surgery.

The part of the inherent risk that is manageable by the manufacturer is included in the RACT and minimized according to the approach, and acceptance criteria chosen by the manufacturer. This is included in the Overall Residual Risk determination. The inherent risk that is external to the device and not controllable by the manufacturer is not included in the Overall Residual Risk of the device.

CHAPTER 23

Benefit-Risk Analysis

Abstract

ISO 14971 requires the manufacturers to establish that the benefits of the medical device outweigh its risks. To determine whether benefits of a medical device outweigh its risks, we must be able to answer two questions: (1) what are the potential benefits? and (2) what are the potential risks? Because the risks and benefits are typically not of the same units, it is often not possible to objectively balance the benefits against the risks. Several factors from FDA guidances for Benefit-Risk evaluation are presented. Benefit-Risk Analysis in clinical studies is discussed.

Keywords: Benefit-risk ratio; benefit-risk analysis; benefit; risk acceptance

After the Residual Risks of the medical device have been reduced to a point that is consistent with the manufacturer's policy, e.g., ALARP, ALARA, AFAP, if the Residual Risks are judged not be acceptable per the criteria in the RMP, the manufacturer is to perform a Benefit-Risk Analysis to determine if the Benefits of the device outweigh its risks. It goes without saying that these are patient safety risks, not business risks.

If the analysis shows that the Benefits of the device do not outweigh its risks, the manufacturer may consider modifying the medical device, or revising the Intended Use (e.g., exclude vulnerable patient groups) in order to be able to show that the Benefits of the device outweigh its risks when used as intended. If after this exercise the risk still remains unacceptable, the medical device development must be abandoned.

For the Overall Residual Risk, a Benefit-Risk Analysis must be done, regardless of whether it meets the manufacturer's risk acceptability criteria.

Benefit-Risk Analysis is generally a subjective judgment by a multi-disciplinary team of experts with medical/clinical backgrounds. Among the factors considered in this judgment, are the magnitude and duration of the Benefit, and whether the Benefits from the device could be achieved through other means, with less risk. Other means include competitive devices, pharmaceuticals, and even diet and exercise. Another factor is whether the risk of unavailability of the device is higher than the risk that it presents when used. Although EU MDR [2] refers to evaluation of "benefit-risk ratio," which implies some kind of quantitative comparison of Benefit to risk, the intention is not to have a quantitative value assigned to Benefits to compute a ratio. The word "ratio" should not be interpreted as arithmetic fraction.

Safety Risk Management for Medical Devices
DOI: https://doi.org/10.1016/B978-0-323-85755-0.00023-0

ISO 14971 [1] suggests that the manufacturer gather and review data and literature to support this subjective decision.

The FDA looks for reasonable assurance of safety and effectiveness by weighing any Benefit to health from the use of the device against any probable risk of injury or illness from such use, among other relevant factors. Final determination in the FDA is based on the judgment of the reviewer, not any numerical ratio.

1. Is there any evidence of clinical Benefit?
2. What is the extent of uncertainty for the Benefits?
3. Are known/probable risks more than minimal?
4. What is the extent of uncertainty for the risks?
5. Do the Benefits outweigh the risks, considering the assessment of Benefit and risk and the extent of uncertainty identified above?
6. Do the Benefits outweigh the risks, when taking into account additional relevant considerations?
7. Can the risks be mitigated, so that Benefits outweigh the risks?
8. Do the Benefits outweigh the risks considering the use of Post-Market actions?
9. Is there any evidence of clinical Benefit for a modified Indications for Use?

Given the subjective nature of the judgment on the Benefit-Risk acceptability, be alert to the cognitive traps that could impel making wrong decisions. When a human perceives risk to be high, the benefit is perceived as low, and vice versa. Paul Slovic identified this as *the affect heuristic* in his 2006 paper [45]. This means, a feeling of good/bad about a risk, without consciousness, conversely affects how we perceive the benefit. For instance, a brain implant is used in therapy for Parkinson's disease. A person who is frightened by the prospect of brain surgery, perceives the benefit of the therapy as low. While a person who is not frightened by brain surgery, perceives the benefit to be higher.

A compelling Benefit-Risk Analysis requires the leadership and participation of medical/clinical staff who are current in the use of the device/therapy. Clinical activities (evaluation) are an integral part of Benefit-Risk Analysis, particularly on the Benefit side of the equation, but also on the risk side.

23.1 WHAT IS A BENEFIT?

Benefit is defined by ISO 14971 [1] as positive impact or desirable outcome of the use of a medical device on the health of an individual, or a positive impact on patient management or public health. There are many types of Benefits. For example:

- improving quality of life
- reducing the probability of death

- aiding improvement/restoration of patient function
- reducing the probability of loss of function
- providing relief from symptoms
- better diagnostics

From a risk management perspective, only Benefits that fit the definition in ISO 14971 [1] are considered in the Benefit-Risk Analysis. Therefore, benefits such as lower cost, or more attractive design would not fit the definition of Benefit.

23.2 BALANCING BENEFITS AGAINST RISKS

Benefit-Risk Analysis (BRA) is a requirement of ISO 14971 [1] for balancing the Benefits of a device against the risks that it presents. To determine whether Benefits of a medical device outweigh its risks, we must be able to answer two questions:

1. What are the potential Benefits?
2. What are the potential risks?

Establishment of Benefits is typically done by Clinical Evaluations, which range from exploratory investigations, such as first-in-man trials, to feasibility and pilot studies, to confirmatory investigations such as pivotal clinical trials.

These are formal, well-planned investigations with defined endpoints to show with statistical validity, the Benefits of a medical device. See Annex XIV of the MDR [2] for further guidance on Clinical Evaluations. Sometimes non-Clinical Evaluations can be used to establish Benefit. Examples: animal and cell-based testing, usability testing, and computer modeling and simulations.

Factors that are considered to evaluate the potential Benefits of a device include:

- **Type of Benefit** – Medical devices provide a variety of Benefits. See Section 23.1 for examples.
- **Magnitude of the Benefit** – The degree to which the patient would experience the Benefit. This is typically measured against a scale according to specific criteria. For example, for Parkinson's disease the patients are asked to walk for 6 minutes. The longer the distance walked, the higher the magnitude of the Benefit.
- **Probability of the Benefit** – Not all patients receive the intended Benefit. Sometimes it is possible to predict which patients are more likely to benefit from a given therapy. For example, a cancer therapy may be more effective if the disease is diagnosed earlier in the course of the disease. It may be that the Benefit is experienced by only a small subset of patients in the target population. Or conversely, the Benefit may be experienced by a large population.

- **Duration of the Benefit** – Some treatments are curatives, while others may be only short-term. The longer the Benefit persists, the more the Benefit would be valued when balancing the Benefit against risk.

It should be noted that clinical Benefits of a device may be indirect, for example, a stent is delivered to its implant site by a number of other devices such as guide wires, catheters, and balloons. All of these supporting devices provide a benefit but are removed after the implant and only the stent remains to deliver the intended clinical Benefit.

The next dimension of Benefit-Risk Analysis is the risk. In the BXM method the risks are quantitatively computed. But Risk Estimation can also be subjective and qualitative. The following factors are considered:

- **Severity, type, likelihood, and duration of Harms** – These are Harms that are caused by the use of the device. Risk management estimates the Severity and likelihood of the Harms. Some Harms last a short while, such as a skin cut. But other Harms may last a long while. For example, brain damage would last a lifetime.
- **Procedure-related Harms** – Some Harms are not caused by the device but are incidental. For example, implanting a medical device requires surgery, and surgery itself always presents risks of Harm.
- **Erroneous Diagnostic results** – A false-positive, or a false-negative diagnosis from a medical device could indirectly lead to harms to patients from unnecessary treatments, or absence of treatment.

For the purpose of Benefit-Risk Analysis, the Overall Residual Risk of the medical device is considered.

Because the risks and Benefits are typically not of the same units, it is often not possible to objectively balance the Benefits against the risks. In other words, it is like comparing apples with oranges. Since it is the patient who bears the risks of the device, for the promise of the potential Benefit, ultimately a subjective decision must be made to answer the question:

> ***Is the patient willing to accept the potential risk of the device for the potential Benefit that it offers?***

One of the complexities of Benefit-Risk balancing is the question of risk tolerance. Personal, societal, economic, and political factors affect the degree of risk tolerance. Therefore, a Benefit-Risk balance which is acceptable in one country/community, may not be acceptable in another.

Benefits of a device are presumed under the condition that the device works reliably, and as intended. Risks and Benefits are not the same for everyone. The same medical device could provide varying degrees of Benefit to different patients, and pose different levels of risks. Many factors are responsible for this, for example variability of the physiology and circumstances of a patient, environmental variability, and variability in manufacturing the medical device itself.

Benefit-Risk Analysis should be done on the overall target population. It may be that the Benefit to risk ratio is acceptable for part of a target population, and not for the entire population. For example, imagine a medical device that provides more Benefit at a lower risk for a younger population, than an older population. As a result, it may be determined that only patients under a cutoff age should be indicated for the use of the medical device.

The FDA has published three guidance documents to help with the determination of Benefit-Risk balance for medical devices:

- Factors to Consider When Making Benefit-Risk Determinations in Medical Device Premarket Approval and De Novo Classifications [44]
- Benefit-Risk Factors to Consider When Determining Substantial Equivalence in Premarket Notifications [510(k)] with Different Technological Characteristics [46]
- Factors to Consider When Making Benefit-Risk Determinations for Medical Device Investigational Device Exemptions (IDEs) [47]

In general, the FDA expects the manufacturer to provide a "reasonable assurance of safety and effectiveness" by "weighing any probable Benefit to health from the use of the device against any probable risk of injury or illness from such use."

The acceptability of Benefit-Risk ratio is based upon clinical data providing sufficient clinical evidence including where applicable, relevant data from Post-Market Surveillance.

Patients are an important source of input on the determination of Benefit-Risk balance. They have an intimate and personal understanding of what it is like to live with a disease and how a device would impact their daily life.

The estimation of Residual Risks of a medical device is the domain of risk management, which is covered in detail in this book. Both clinical and non-clinical methods can be used to confirm estimations of risks, and the effectiveness of implemented Risk Controls.

When judging the risk vs. the Benefits of a device, additional factors that are considered are:

- **Quality of the clinical data** – Poorly designed and executed clinical investigations could render the results of the investigation unreliable and weaken the argument of the dominance of Benefit over risks.
- **The disease characteristics** – Factors considered are whether the disease is degenerative and untreated worsens over time, or, is it stable, or does it get better over time; these make a difference in the judgment of the Benefit risk balance.

- **Availability of alternative therapies** – For some diseases alternative therapies may be available. For example, pharmaceuticals, gene therapy, etc. If a device provides a Benefit, though small, for a disease for which no alternative therapy exists, it may still get approved.
- **Comparable Devices** – Comparison of Benefits and risks of the device with comparable devices that are on the market, and the generally acknowledged state-of-the-art.
- **Patient risk tolerance** – The degree of risk tolerance varies greatly among patients and for different diseases. Patients with very severe diseases where the risk of dying is imminent may tolerate higher risks. For chronic diseases where patients learn to adapt to the presence and management of the disease, risk tolerance may be lower.

Risk tolerance is influenced by many factors including:

- The values of the society
- The population at risk (children, adults, . . .)
- Available alternative therapies
- The nature of the disease (acute, chronic, degenerative, . . .)
- Trust in the manufacturer

There are certain circumstances where demonstration acceptability of Benefit to risk ratio is not difficult. Consider Fig. 53.

In this figure, the State-of-the-Art (SOTA) risks and Benefits are depicted by dotted lines. SOTA represents a medical device that has been approved and in use already. Its Benefits are known, and its risks have been accepted by the market. SOTA may be

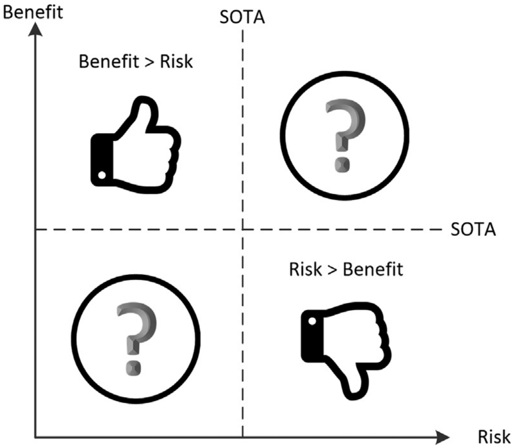


Figure 53 Benefit-Risk Comparison.

your own company's previous device, or a competitor's device. When compared with SOTA, if the new device which is under analysis delivers more Benefit for the same or lower risk, then the Benefit-Risk ratio is improved and dominance of Benefits over risks is surmised. This is represented by the upper left quadrant of Fig. 53. If on the other hand, the new device delivers less Benefit for the same or more risk, then the Benefit-Risk ratio is worsened. This is represented by the lower right quadrant of Fig. 53. These are the clear cases. The upper-right and lower-left quadrants are not so clear and require a deeper analysis.

Sometimes a medical device shows greater risk than a comparable device on the market, but it may be approved to add to the portfolio of available treatments for patients. A higher risk device may also get approved, if it shows greater efficacy for a subpopulation of the patients, or under specific use conditions.

Medical therapies are not static. Even if we do a Benefit-Risk Analysis now and show that the Benefits of a device outweigh its risks, the same conclusion may not hold true later. Because as time goes on, new therapies are developed, culture and habits change, and Benefit and risk perceptions evolve. For example, 60 years ago smoking was not only tolerated, there were even advertisements touting its health benefits. A simple internet search on vintage advertisements on the health benefits of smoking would show several cringe-worthy samples. Slogans such as "More doctors smoke Camels than any other cigarette," or "As your dentist, I would recommend Viceroys" may seem ridiculous today. But 60 years ago, they seemed perfectly reasonable. Even political changes could affect health policy, reimbursements, and therefore alter people's aversion to risk.

23.3 BENEFIT-RISK ANALYSIS IN CLINICAL STUDIES

Clinical studies are special cases in the risk management of medical devices. In a clinical study, the subject medical device may not be approved for commercial release. It may not have any Benefits that the manufacturer could claim. And, the clinical study itself may present safety risks to the study participants. Still the Benefit-Risk profile is expected to be evaluated and shown to be acceptable for the intended study target group.

For clinical studies, according to MEDDEV 2.7/1 [48], it is expected that the risks associated with the performance of the clinical study are minimized and acceptable when weighed against the Benefits to the patient and are compatible with a high level of protection of health and safety.

With respect to the acceptability of Benefit-Risk ratio in Clinical Evaluations MedDev 2.7/1 [48] advises to evaluate the clinical data on Benefits and risks of the device under evaluation when compared with the current state-of-the-art in the corresponding medical field.

Per MedDev 2.7/1 [48] for clinical investigations, typically the following items are considered:

- clinical background
  - information on the clinical condition to be treated, managed, or diagnosed
  - prevalence of the condition
  - natural course of the condition
- other devices, medical alternatives available to the target population, including evidence of clinical performance and safety
  - historical treatments
  - medical options available to the target population
  - existing devices, benchmark devices

When making a decision on the acceptability of risks for the potential Benefits, the deficiencies in current therapies should be identified from a critical and comprehensive review of relevant published literature to ascertain whether the investigative device addresses a significant gap in the currently available healthcare. If there is no significant gap, then the investigative device must show an improved or at least equivalent Benefit-Risk profile compared to existing products or therapies.

CHAPTER 24

Risk Management Review

Abstract

After the completion of the pre-market risk management process, ISO 14971 requires the manufacturer to perform a risk management review to ensure that the planned activities have been faithfully executed; that the overall residual risk is acceptable, and that production and post-production mechanisms are in place to monitor the product performance in the field.

Keywords: Risk management review; production and post-production monitoring; risk management report

The new ISO 14971:2019 [1] requires that after the risk management activities are completed and Risk Control measures have been verified, to perform a *Risk Management Review* to ensure that:

- the RMP has been faithfully executed
- the Overall Residual Risk is acceptable
- appropriate mechanisms are in place to collect, review, and act upon the Production and Post-Production information

The Risk Management Report (RMR) includes the results of the Risk Management Review.

It is possible to have intermediate Risk Management Reviews during the product development process to ensure that the risk management activities are on track with the RMP.

If major changes to the device design happen which necessitate the iteration of the risk management process, a new Risk Management Review is warranted.

The Risk Management Review should not be confused with the periodic review of the risk management process for suitability, which is stipulated in ISO 14971 Section 4.2 [1]. That review is normally done as part of the QMS management review to ensure continued suitability, adequacy, and effectiveness of QMS processes.

Safety Risk Management for Medical Devices
DOI: https://doi.org/10.1016/B978-0-323-85755-0.00024-2

CHAPTER 25

Production and Post-Production Activities

Abstract

ISO 14971 requires that manufacturers collect and evaluate information about the medical device or similar devices, in the Production and Post-Production phases. The US CFR, title 21, part 822 has similar requirements. Patient/user safety is enhanced by active surveillance of production and post-production information about marketed products. The manufacturer also receives significant benefit from the surveillance, namely, the opportunity to quickly identify and rectify product/process defects. This in turn leads to reduced customer complaints, reduced field corrective actions, improved reputation and customer loyalty, which means higher sales. Several Post-Market deliverables such as PMCF, FSCA, SSCP, PSUR, PMSR, MIR, MDR, and CER are also discussed in this chapter.

Keywords: Post-Market risk management; Production and Post-Production monitoring; surveillance; Post-Market Surveillance; PMCF; complaint handling; CAPA; FSCA; SSCP; PSUR; PMSR; MIR; MDR; CER

In pre-market risk management manufacturers estimate the risks of medical devices and predict the performance of the devices when they are put into service. Naturally, predictions and estimations are not the reality. A number of factors can affect the safety and performance of medical devices after they are placed in the market. For example, use-conditions and use-environments could drift, new unforeseen user interactions and product misuses could manifest, and unanticipated product failures could happen. Therefore, manufacturers are required to monitor the performance of their devices during Production and Post-Production phases and make the necessary corrections to ensure their products remains safe for use.

The methods to collect and review Production and Post-Production information about the medical device must be in place before the product is released to the market. These activities do not end for as long as the medical device remains in the market.

Production monitoring aims to detect and prevent the release of non-conforming products whose safety characteristics have been adversely affected. Production monitoring uses techniques such as statistical process controls, control charts, and quality control testing.

Post-Production monitoring is intended to evaluate the performance of the product in the field. A data monitoring plan should be established that stipulates sources of information and frequency of data collection and trending. Trending of data may show

DOI: https://doi.org/10.1016/B978-0-323-85755-0.00025-4

that a particular signal has been increasing and may have exceeded its threshold. Even though no patient Harm may have happened, this may indicate the potential for a future adverse event. Such a signal may necessitate the creation of a CAPA. Examples of data sources for Post-Production monitoring are:

- non-conformance reports
- CAPAs with potential for safety risk to patients
- complaint trending signals
- signals from returned product investigation
- reports of new Hazards in competitor products
- published information
- Post-Market Clinical Follow-ups
- surveillance registries
- reports of injuries and deaths that are attributable to the product

Post-Market-detected issues that have a potential safety impact must be addressed within certain time limits (e.g., 30 days) to limit the exposure of patients.

Post-Market risk management serves many purposes:

- To prevent harm to patients/users from released products
- To ensure Benefit-Risk ratio continues to be acceptable
- To improve future/related products

A range of actions and deliverables are foreseen, which are detailed in the following sections.

Before we proceed with this chapter we should align on terminology. The term "Postmarket" is used by the FDA in the USA. ISO 14971 [1] uses the term "Production and Post-Production." EU MDR [2] uses the term "Post-Market." These terms are roughly equivalent. Fig. 54 shows the contrast between these terms. Essentially, Post-Market begins when the product has left the manufacturer and has gone to the customer.

Production information is collected during the manufacturing process, and Post-Production information is collected on all the phases of the life cycle after the product has been manufactured. The most significant Post-Production life cycle phase is product-use where majority of the feedback is generated.

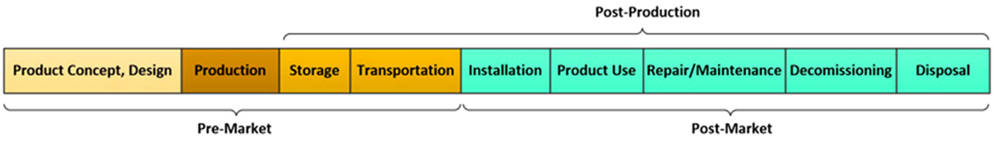


Figure 54 Post-Market vs. Post-Production.

In the remainder of this chapter, we will use the term "Post-Market" interchangeably with "Production and Post-Production" and "Postmarket."

Post-Market Surveillance which is a part of Post-Market risk management can collect information passively, or actively. Examples of passive information gathering: complaint handling, or reaction to a patient injury. Examples of active information gathering: Post-Market Clinical Follow-up (PMCF), surveys, and manufacturer-sponsored registries.

25.1 REGULATORY BASIS

Section 10 of ISO 14971 [1] requires that manufacturers collect and evaluate information about the medical device, or similar devices, in the Production and Post-Production phases. Similarly, under Section 822 of CFR 21 the FDA requires the manufacturers and distributors of medical devices to perform "post-market" tracking and reporting of device malfunctions, serious injuries, or deaths. EU MDR [2] Article 83 also requires that manufacturers plan, establish, document, implement, maintain, and update a Post-Market Surveillance system

25.2 THE PURPOSE OF POST-MARKET ACTIVITIES

In addition to providing opportunities for the manufacturers to learn about the performance of their medical devices, Post-Market risk management enables the manufacturers to verify their predictions on the hazards and harms, and their estimations of the risks of their medical devices.

In the event of discovery of unanticipated hazards or harms, or higher than expected risks, regulatory reporting and information sharing allows more effective control of risks to patients – not only from the subject medical device, but also from other similar devices made by other manufacturers.

25.3 POST-MARKET RISK MANAGEMENT

As stated above, pre-market risk management is a predictive technique, used to forecast potential future Hazards and risks, while Post-Market risk management is a retrospective, and sometimes reactive endeavor that is intended to contain and limit Harm from devices that have been released to the market.

Production and Post-Production monitoring are the means by which to detect whether a released product has harmed patients or has the potential to cause undue

Harm. The result of Post-Market risk management may be to hold manufactured product from being released, or issue corrective actions, including product recalls. In cases of imminent potential Harm to patients, it may be necessary to issue immediate information (Customer Letter) before new Risk Controls are developed and verified.

Post-Market risk management involves understanding of: the Hazard in question, the risk of potential Harm, size and magnitude of the patients' vulnerability, and countermeasures that should be taken until the product itself is addressed for corrective measures.

A common technique that is used in Post-Market risk management is the Health Hazard Assessment (HHA). In the United States, 21 CFR part 7 requires the conduct of an evaluation of the health hazard (actual or potential) presented by a product being recalled or considered for recall. In Europe, MDR [2] Article 89 compels similar action. Elements of an HHA are:

- Identify the Hazard (actual or potential).
- Identify the related Harm(s), both immediate and long-term.
- Identify the population at risk and whether any subpopulation is at greater risk.
- Describe the mechanism of occurrence of the Hazard, and exposure to the Hazard.
- Is the Hazard in question happening when the product is used under labeled conditions?
- Is the Hazard in question previously predicted?
- Is the Hazard in question manifesting under normal or fault conditions?
- Identify conditions that would exacerbate or mitigate the risk.
- Identify the degree to which the Hazard is recognizable by the patient/user and the feasibility of countermeasures.
- What is the likelihood of future additional risks due to the Hazard in question?
- Balance the risk of corrective action vs. the risk of not taking corrective action. Example: an implanted device may pose a greater risk than previously predicted. But the risk of explant surgery could be greater than the risk of leaving the device in.
- Conclusion and recommended actions.

Any decision for action or inaction should be approved by appropriate personnel, e.g., medical safety officer, and the decisions and approvals should be documented.

Post-Market risk management may determine measures to control the discovered risks. These Risk Controls may be in the form of design changes, labeling, or training. Naturally, the new Risk Controls must be verified for effectiveness. The Risk Management File may need to be updated. The manufacturer may also issue advisory/ Field Safety Notices.

For medical devices currently installed and used in the market, the Risk Control measures may be different from those applied to devices that are currently in Production. For example, for products in the field, Risk Control measures may include sending information to doctors or patients, removing product from the field and providing replacement product. For products that are in Production, Risk Control measures may include identification and collection of product, and rework or discard of product.

If a recall, or field product update/revision is decided, speed of action will be material to the effectiveness of risk-reduction activities.

25.4 THE ELEMENTS OF POST-MARKET RISK MANAGEMENT

Post-Market Surveillance is the core part of Post-Market risk management. The purpose of Post-Market Surveillance is to systematically collect, document, analyze, and assess data on the quality, performance, and safety of medical devices. Based on the assessment of the collected data, the manufacturers make decisions on potential actions which could include CAPAs, and FSCAs.

In the following subsections, we will discuss the elements of Post-Market risk management.

25.4.1 Post-Market Surveillance

Section 522 of the Federal Food, Drug and Cosmetic Act gives the FDA the authority to require a manufacturer to conduct Post-Market Surveillance of a class II or class III medical device that meets any of the following criteria:

- its failure would be reasonably likely to have serious adverse health consequences; or
- it is expected to have significant use in pediatric populations; or
- it is intended to be implanted in the body for more than one year; or
- it is intended to be a life-sustaining or life-supporting device used outside a device user facility.

EU MDR Chapter VII, Section 1, article 83 [2] also requires that manufacturers establish a comprehensive Post-Market Surveillance system in a manner that is proportionate to the risk class and appropriate for the type of device. The Post-Market Surveillance system must be an integral part of the manufacturer's QMS.

Post-Market Surveillance is expected to continue for the lifetime of the device. The information gathered via PMS is used to:

- improve the risk management of the device
- update the Benefit-Risk determination
- update the design, manufacturing, or labeling if necessary

- update the Clinical Evaluation
- update the summary of safety and clinical performance
- identify the need for preventive, corrective, or Field Safety Corrective Actions
- detect and report trends in accordance with EU MDR Article 88 [2]

Besides the regulatory requirements for Post-Market Surveillance, it is just good business practice to know how your product is performing and understand the market experience with it.

25.4.1.1 Post-Market Surveillance Plan

Just as with many activities, Post-Market Surveillance (PMS) requires a plan. This is mandated in Article 84 of EU MDR [2], and the requirements for which are set out in Section 1.1 of EU MDR, Annex III [2].

The Post-Market Surveillance Plan lays out a systematic and proactive process to collect, review, analyze, and act upon information regarding approved medical devices in order to monitor the safety, performance, and continued acceptability of their Benefit-Risk ratio. PMS continues for as long as a medical device is in the market.

The PMS plan should include certain elements including:

- Applicability of the PMS plan, e.g., to a single device; a device family; a therapy
- Identification of the sources and means of collecting Production and Post-Production data
- Frequency of data collection and review
- The methods for processing, analysis, and utilization of the collected data, including trending and statistical methods
- Identification of suitable indicators and thresholds to trigger actions
- Identification, or reference to processes for complaint handling, and complaint processing
- Identification, or reference to processes for investigations of market-related experience with product field performance
- Methods and processes for reporting to regulatory bodies (e.g., the FDA or competent authorities), notified bodies, economic operators, and users
- Identification, or reference to processes for the generation and delivery of PMS outputs such as PMSR, PSUR, and SSCP
- Identification or reference to processes for CAPAs and FSCAs including the approval authorities
- Identification or reference to a process for PMCF
- Methods for feedback to pre-market RM and design and manufacturing groups

The PMS plan should be periodically reviewed and updated, if necessary.

25.4.1.2 Post-Market Surveillance System

The purpose of the Post-Market Surveillance system is to actively and systematically collect and analyze data on the device performance, quality, and safety, and motivate appropriate actions.

The Post-Market Surveillance system should be commensurate with safety risks of the medical device, the novelty of the product or technology, and whether the manufacturer has a long history of developing similar device types. A manufacturer who has a long history with a given device, therapy, and the related patient population is likely to better understand the foreseeable risks associated with their product. With a deeper understanding of the risks, the PMS system can be tuned to the right level of rigor. For low-risk devices with a long history, assessing the available information regarding the state-of-the-art market experience with similar devices and a literature search may be adequate. On the other hand, for novel, complex, or high-risk devices manufacturers must have a rigorous PMS system, including PMCF, to ensure early detection of risks that may have not been foreseen during the development of the product.

The information derived from the PMS system is used in many places such as: CAPAs, FSCAs, pre-market risk management, and Clinical Evaluations.

A summary of the results and conclusions of PMS data and resulting actions are reported periodically to Regulatory authorities.

25.4.1.3 Information Collection

One of the most important aspects of Post-Market Surveillance is information collection. Post-Market information can come from a variety of sources. Examples of potential sources of information:

- manufacturing/production
- product service/repair
- returned product investigations
- customer service
- field service/customer visits
- clinical studies, e.g., Post-Market Clinical Follow-ups
- alternative medical devices
- non-medical products that are similar in materials or operating principles
- alternative therapies
- customer complaints
- limited market releases
- product demonstrations
- databases such as MAUDE, or Eudamed

- the legal department
- regulatory agencies, competent authorities (e.g., for Field Safety Notices, Safety Alerts)
- suppliers
- distributors
- published literature on your device or similar, or competitive devices
- social media

Listening systems should be established and tuned in to various sources of information. Define appropriate methods for the collection and processing of data. These could include statistical methods for trend analysis.

The frequency of monitoring and trending of collected information should be established and documented in the PMS plan. It is advisable that the frequency of data monitoring be based on the risk of the device. The higher the risk, the more frequent monitoring. For example, data monitoring may be executed monthly, quarterly or yearly.

25.4.1.4 Information Review

The collected information should be reviewed for relevance to the safety of the medical device. Some of the objectives of the review should be:

- Were any new Hazard, Hazardous Situations, or harms identified that were previously not anticipated?
- Is the device delivering the promised Benefits?
- Are there any misuses/off-label uses that were previously not foreseen?
- Are the predicted P1 and P2 numbers valid?
- Are the Risk Controls proving to be as effective as predicted?
- Is the predicted Overall Residual Risk of the device matching the market experience?
- Are there changes in the state-of-the-art, e.g., introduction of new technologies, materials, practices, or alternative therapies that adversely affect the previous Benefit-Risk Analysis?
- Should the indications, Contraindications, or the intended use of the device be adjusted?

After the review and analysis of the collected information, decisions are made on the consequent actions.

25.4.1.5 Consequent Actions

The results of the review of Post-Market information may necessitate certain actions by the manufacturer. Examples:

- Assess newly identified risks
- Revise the Benefit-Risk Analysis

- Update FMEAs
- Update the CHL
- Update the HAL
- Update Residual Risk calculations
- Implement additional Risk Controls
- Issue Field Safety Notices
- Initiate CAPAs
- Issue product recalls

A well-organized PMS system and quality information help with making good decisions on the consequent actions; decisions that could be explained and defended.

25.4.2 Post-Market Clinical Follow-up

Prior to release of a medical device, Clinical Evaluations are performed to establish the clinical Benefits, and confirm the estimated risks of the device. After a device is approved and released to the market, many things can change that could impact the Benefit-Risk ratio of the device. For example, new devices may come to existence whose interaction with the subject medical device could interfere with the function of the subject device; new therapies may become available; or the environment in which the device is used may change.

Pre-market clinical studies have limitations, such as the duration of the study, number of subjects, heterogeneity of the subjects, number of investigators, and the controlled setting of the study vs. the natural and full range of patients and clinical conditions that happen in real life. These limitations make it unlikely that pre-market clinical studies detect rare complications that can be encountered during widespread and long-term use of the device. To compensate for this shortcoming, Post-Market Clinical Follow-ups are necessary throughout the lifetime of the medical device to ensure the continued safety and performance of the medical device while the device is on the market. PMCFs by design are performed over a much larger and varied population in real life.

Prior to release of a device, sometimes there are unclarities about the long-term clinical performance of a device. PMCF studies are intended to complement the pre-release clinical studies of the device, and to confirm the safety and clinical performance of the device throughout its expected lifetime. In addition to confirming the clinical Benefits of the device, PMCF can also detect emerging risks and ensure the continued acceptability of the Benefit-Risk ratio of the device based on factual evidence.

Another benefit of PMCF is the identification of possible systematic misuse/off-label use of the device, and verification that the Intended Use of the device is correct.

Post-Market Clinical Follow-up is a continuous process using CE-marked devices that are used for their Intended Purpose, according to their instructions for use. PMCF can identify previously unknown side-effects, and monitor known side-effects over the long term. PMCF continues for the duration of the expected lifetime of medical devices. That is, until the end of the expected lifetime of the last copy of the product which is released. For example, if a device's expected lifetime is 2 years, and Production ends 10 years after the first product is released, the PMCF should continue for at least $10 + 2 = 12$ years. PMCF studies have to be approved by Ethics Committees. If the PMCF deviates from normal clinical practice and involves additional procedures that are invasive or burdensome, e.g., additional X-rays images, or if off-label use is planned by the study, then approval by Competent Authority in the EU member State is required. Annex XIV, Part B of EU MDR [2] provides details of the expectations for PMCF studies.

It is possible that the PMCF activities may reveal the need for Corrective And Preventive Actions (CAPA). In such cases follow the appropriate internal CAPA processes.

The results of PMCF activities are documented in the PMCF report which according to EU MDR [2] shall be part of the CER and the technical documentation.

It is required that PMCF be performed according to a plan. In the following sections the PMCF plan and report are discussed.

25.4.2.1 PMCF Plan

PMCF studies are required to have a plan that includes study hypotheses, objectives, endpoints, statistical evaluation strategy, sample size, inclusion/exclusion criteria, ethical considerations, etc. The study should be performed with adequate controls to ensure conformance to the PMCF plan. The PMCF plan must be addressed in the PMS plan. The final report should draw conclusions related to the study objectives and hypotheses. MDCG 2020-7 [49] provides a template to guide manufacturers in complying with the requirements of EU MDR [2].

According to MDCG 2020-7 [49] the aim of the PMCF plan is:

- confirming the safety and performance, including the clinical Benefit if applicable, of the device throughout its expected lifetime
- identifying previously unknown side-effects and monitor the identified side-effects and contraindications
- identifying and analyzing emergent risks on the basis of factual evidence
- ensuring the continued acceptability of the Benefit-Risk ratio of the device
- identifying possible widespread misuse or off-label use of the device, with a view to verifying that the Intended Purpose is correct

At a minimum the PMCF plan must include:

1. General actions to be performed, such as gathering clinical experience, collecting user feedback, and literature searches
2. Specific actions such as use of registries and PMCF studies
3. Rationale for why the methods defined in steps (1) and (2) are appropriate
4. References to CERs and the risk management results
5. The specific objectives of PMCF
6. Evaluation of clinical data related to equivalent of similar devices, if any
7. References to any relevant harmonized standards, or clinical studies that are used
8. A detailed time schedule for the performance of PMCF and reporting of the results

25.4.2.2 PMCF Report

The purpose of the PMCF report is to capture the results of the PMCF activities, and the analysis of PMCF findings. The PMCF report should include the following information:

- Description of the device(s) in scope, including the Intended Purpose
- The PMCF plan objectives that were addressed
- How the PMCF has progressed according to the timelines in the PMCF plan
- Summary of the analysis of the results
- Identification of new issues, if any
- Identification of any pervasive misuse/off-label use of the device
- Conclusions, particularly whether the Indications/Contraindications are still appropriate, and whether the Benefit-Risk ratio remains acceptable

The PMCF report is supposed to be included in the CER and is part of the technical documentation of the device. The PMCF report is the evidence that PMCF activities followed the PMCF plan. The conclusions of the PMCF report are used to update the Clinical Evaluation, and risk management artifacts. It may be also necessary to update the PMS and the SSCP as a result of the PMCF conclusions.

MDCG 2020-8 [50] provides a template to guide manufacturers in complying with the requirements of EU MDR [2].

25.4.3 Complaint Handling and Monitoring

One of the most important sources of customer feedback is complaints. Monitoring of this source of information is critical to the proper tracking and management of product performance in the field. In addition to providing insights to potential safety risks, complaint monitoring could provide valuable information on customer experience and product performance. This information could benefit product design teams to improve product design for: better performance, safety, and customer satisfaction.

What is a complaint? According to 21 CFR part 820.3 a complaint is "Any written, electronic, or oral communication that alleges deficiencies related to the identity, quality, durability, reliability, safety, effectiveness, or performance of a product after it is released for distribution or has been placed on the market." Note that a complaint may be also about the product's labeling, packaging, or instructional materials.

Complaint handling is considered to be a passive form of information collection. Looking at the sources of information that were presented in Section 25.4.1.3 above it can be seen that some require proactive effort by the manufacturer, e.g., literature searches, or MAUDE database review. Complaint information is passively received by the manufacturer who then reacts to the information.

To receive real value from the complaints, thoughtful planning must be done to properly process, analyze, and code the complaint data. Good complaint-handling makes complaint-monitoring easier and more beneficial. Complaint handlers should be trained to collect as much relevant information as they can from the complaint source. Below is a list of useful information to collect:

- Name and contact information of the caller (source of complaint)
- Patient name and condition; contact information
- Event date: the date on which the incident took place
- Event description/reason for removal, patient symptoms, contributing factors any Intervention/troubleshooting of Patient and or Device/Event Status/ Outcome/Event-Cause
- Doctor's first and last name; contact information
- Suspect-device model and serial/lot numbers/software version number
- Notify date: the date the first employee of the manufacturer learned of the reported event (complains may come to any employee at any time)
- Patient weight (FDA Requirement)

Complaint monitoring requires the criteria for assessing the collected data. For example, you may trend the monitored data using established statistical methods and set up trigger criteria when trended data exceed predetermined thresholds.

The details of complaint handling and monitoring are out of scope of this book, but the contribution of complaint information to risk management is within scope. Complaint data can be used to update: the CHL, the HAL, P1 and P2. This serves to ensure that Risk Analysis of the device is always most complete and accurate.

25.4.4 Post-Market Risk Management Actions

Post-Market risk management is about ensuring that the product remains safe and effective and that its Benefits continue to outweigh its risks. Post-Market Surveillance may present opportunities to improve product safety. In many cases such actions involve design or manufacturing process improvement. Sometimes opportunities involve certain actions such as CAPAs and FSCAs which are briefly described in the following sections. There are many resources available on both topics that go into depth on the methods and mechanics of CAPAs and FSCAs.

25.4.4.1 Corrective and Preventive Actions

The US code of federal regulation title 21 part 820.100 requires that manufacturers establish and maintain procedures for implementing Corrective And Preventive Action (CAPA).

EU MDR [2] Article 10, clause 9 (l) requires manufacturers to establish a quality system that addresses corrective and preventive actions.

Also, ISO 13485 Sections 8.5.2 and 8.5.3 require that organizations take corrective and preventive actions to prevent non-conformities from recurring.

A CAPA is a formal, systematic method for correcting existing non-conformity, or safety issues, and preventing them from recurring. It involves root-cause analysis, defining corrective and preventive actions, and verification of the effectiveness of said actions.

CAPAs are not regulatory punishments. They are just good business practices for continuous improvements to company products and practices.

Refer to additional resources such as *Handbook of Investigation and Effective CAPA Systems* [51] or other similar resources for in-depth discussions on CAPAs.

25.4.4.2 Field Safety Corrective Actions

According to MEDDEV 2.12-1 [52] a Field Safety Corrective Action (FSCA) is an action taken by a manufacturer to reduce a risk of death or serious deterioration in the state of health associated with the use of a medical device, which is already placed on the market. FSCAs may include a range of actions, for example:

- Return of the Medical device to the supplier
- Exchange of medical device
- Modification of medical device design, or manufacturing
- Destruction of the medical device
- Patient follow-up
- Field Safety Notices

A device modification could be, e.g., a change in the labeling, a software update, or a change in the clinical management of the patients.

Field Safety Notices could provide information regarding changes in the way the device is used, changes to storage/handling conditions, a recall, etc. Section 5.4.4.2 of MEDDEV 2.12-1 [52] provides guidance on the content of Field Safety Notices.

If a released medical device can fail in a way that might lead to death or serious deterioration of the health of patients/users, the manufacturer must initiate an FSCA.

The decision on the type and extent of FSCA hinges upon several factors, including:

- The hazards that could arise from a shortcoming of the medical device
- The probability of Harm to patients/users from the device
- The balance of the risk due to the FSCA itself vs. the risk from the medical device

Article 92 of EU MDR [2] requires that Field Safety Corrective Actions, and Field Safety Notices be entered in Eudamed.

25.5 DELIVERABLES OF POST-MARKET RISK MANAGEMENT

The Post-Market risk management system is intended to create certain deliverables. In the subsections below five deliverables are briefly described.

25.5.1 Summary of Safety and Clinical Performance

Article 32 of the EU MDR [2] requires the manufacturers of class III and class IIb implantable devices to produce a Summary of Safety and Clinical Performance (SSCP) of their device on an annual basis, or when the risk profile of the device is changed. The SSCP reports on the performance of the device in the context of diagnostics or therapy when compared to alternatives and use-conditions. The SSCP is not required for custom-made or investigational devices.

The SSCP is a public source of information which will be stored in Eudamed. It is intended to create more transparency and access to information. However, it does not replace the IFU or the patient card, nor is it intended to offer advice on diagnostics/treatment of patients. The SSCP must be objective and adequately summarize both favorable and unfavorable data about the device.

The SSCP is produced by the manufacturer and validated by Notified Bodies prior to uploading to Eudamed. Validation entails inspection of the SSCP to ensure all the required elements are included, and that the SSCP is in alignment with other technical documentation related to the device. The SSCP may be submitted to Notified Bodies in the local language. The Notified Bodies would then validate the SSCP in the original language, also known as the master language. However, if the original language is not English, an English translation must be uploaded to Eudamed within 90 days of the upload of the master SSCP to Eudamed. The SSCP must state in which language it was validated. The SSCP has a technical section, intended for the clinicians, and a Lay section if patients interact with the device. The Lay section must be translated in the local language of all the localities where the device is marketed.

Under certain circumstances it may be allowed not to update the SSCP, for instance, if there is no increase in Residual Risks, no signal change in PMS documents, and no change to the verification reports.

Refer to MDCG 2019-9 [53] for additional guidance on the creation of the SSCP, and a template for the SSCP.

Write the SSCP in a way that is understandable by its intended audience. You may add additional content beyond the template, as long as it doesn't affect the readability of the SSCP and excludes materials of promotional nature.

MDCG 2019-9 [53] states that in the lay section of the SSCP, the Residual Risks and side-effects should be explained and quantified. The BXM method conveniently provides quantitative estimations of Residual Risks of a device for inclusion in the SSCP.

Include in the IFU that the SSCP is available in Eudamed and link it to its Basic UDI-DI.

The following are two resources to help with writing the lay section of the SSCP.

1. Summaries of Clinical Trials Results for Laypersons
   https://ec.europa.eu/health/sites/health/files/files/eudralex/vol-10/2017_01_26_summaries_of_ct_results_for_laypersons.pdf
2. Common European Framework of Reference for Languages: Learning, teaching, assessment (CEFR)
   https://rm.coe.int/1680459f97

25.5.2 Periodic Safety Update Report

Article 86 of the EU MDR [2] requires the manufacturers of class IIa, class IIb, and class III devices to periodically prepare a report to summarize the results and conclusions of the analyses of the Post-Market Surveillance data, including the rationale and description of any preventive and corrective actions taken. This report is called the Periodic Safety Update Report (PSUR). PSURs must be prepared for each device, or where appropriate, for each category or group of devices.

The purpose of the PSUR is to present a comprehensive analysis of the Post-Market data to facilitate the identification of changes to the Benefit-Risk ratio of medical devices. The scope of the analyzed data includes PMCFs, Vigilance reports, Clinical Evaluations, complaint monitoring, trending, and the PMS data. The intention is to focus on any new safety-related information that has emerged since the previous PSUR, or since the approval of the device. The PSUR is a public document that is to be electronically shared in Eudamed, as required by article 92 of the EU MDR [2].

The PSUR is part of the technical documentation of the medical device and is linked to the RMP, PMS, CE, PMCF, and CAPA. PSURs are reviewed by NBs to determine whether the Benefit-Risk ratios are/remain valid in lieu of the gathered Post-Market information.

The PSUR should have certain content, including:

General information

- Executive summary
- Description of the devices covered by the PSUR and their Intended Uses
- Justification of the grouping of devices if applicable

Post-Market context

- Estimated: volume of sales
- Target population and their characteristics
- Where practicable, usage frequency of device

Presentation of data

- PMCF studies plus evaluations
- Possible change in the-state-of-art
- Vigilance data including trending/signals and related evaluation
- PMS data (safety and performance) and related evaluation
- Corrective and preventive actions for safety reasons and related evaluation
- Other data sources and related evaluation

Summary of the findings

- A more detailed compilation of findings than what was presented in the executive summary

Assessment of the Benefit-Risk profile

- Baseline safety and performance information
- Update on characterization of risks, if any
- Any new risk reduction actions and their effectiveness
- Update of characterization of Benefits, if any
- Update to Benefit-Risk profile, if any

Conclusions of the PSUR report

- Result and conclusion of analysis of PMS data

- Information on any serious incidents
- Information on non-serious incidents and undesirable side-effects
- Information from trend reporting
- Feedback information, e.g., from complaint handling,
- Citations of relevant literature, registers, databases on the current or similar devices
- Benefit-Risk determination
- Main findings of PMCF
- Prediction of the number of devices in the field, patient population size, and characteristics

The date and cadence of PSUR submissions depend on many factors such as:

- Is the device certified under MDD [3]/AIMDD [4]?
- Is the device certified under EU MDR [2] before the Date of Application (May 26, 2021)?
- Is the device certified under EU MDR [2] after the Date of Application (May 26, 2021)?
- The classification of the device

Consult your Regulatory expert to determine your requirements for the date and cadence of PSUR submissions.

A guidance document is available, which is endorsed by the Medical Device Coordination Group (MDCG) established by Article 103 of EU MDR [2]. See https://ec.europa.eu/health/md_sector/new_regulations/guidance_en

Where applicable, PSURs are required for the recertification of devices.

Table 32 summarizes the applicability and frequencies of PSURs as expected by EU MDR [2] articles 85 and 86.

25.5.3 Post-Market Surveillance Report

Article 85 of the EU MDR [2] requires the manufacturers of class I devices to collect, analyze, evaluate, and summarize the Post-Market Surveillance data on the devices, including any preventive and corrective actions taken, and prepare a report to make available to Competent Authority upon request. This report is called the Post-Market Surveillance Report (PMSR), and must be updated when necessary, e.g., when the PMS data shows that the risk profile of the device is worse than expected.

Table 32 summarizes the applicability and frequencies of PMSRs as expected by EU MDR [2] articles 85 and 86.

Table 32 Types and Frequencies of Post-Market Reports

Device Class/Type	Report Type	Update Frequency	Notified Body Reporting	Competent Authority Reporting
Class I	PMSR	When necessary	Upon request	Upon request
Class IIa devices	PSUR	At least every 2 years	Make available	Upon request
Class IIa implants	PSUR	At least every 2 years	Electronic (Eudamed)	
Class IIb devices	PSUR	At least annually	Make available	Upon request
Class IIb implants	PSUR	At least annually	Electronic (Eudamed)	
Class III devices	PSUR	At least annually	Electronic (Eudamed)	
Class III implants	PSUR	At least annually	Electronic (Eudamed)	

25.5.4 Manufacturer Incident Report

Article 87 of the EU MDR [2] requires the reporting of serious incidents and Field Safety Corrective Actions to the relevant Competent Authorities. This is known as Vigilance. Vigilance reporting is a system of cooperation and information-sharing among users, manufacturers, Notified Bodies, and Competent Authorities to facilitate more rapid detection and mitigation of risks to patient/user health.

The tool used for this purpose is the Manufacturer Incident Report (MIR). The MIR form can be used for Vigilance reporting of Incidents under the EU directives, and Serious Incidents under EU Regulations.

Use of the MIR form is mandatory. The latest revision of the form requires the citation of IMDRF codes to improve stakeholders' ability to conduct detection, analysis, and communication of information related to risks and failures, associated with medical devices and in vitro diagnostic medical devices.

The MIR form has five sections:

Section 1 – identifies the Competent Authority, the manufacturer, date, type and classification of the incident, Submitter information, and references other related MIRs or FSCAs.

Section 2 – identifies the subject medical device using UDI, category of device, risk class, commercial name, model number, and other specific subject-device identifications, any required accessories, geographies of distribution, and the Notified Body.

Section 3 – is about the incident. It includes the details related to the incident, patient information, reporter information, and the IMDRF codes for: device problem, and health effects.

Section 4 – contains the manufacturer’s analysis. It includes root cause analysis, risk assessment, and IMDRF codes for: cause and involved components, any remedial, preventive, corrective, or Field Safety Corrective Actions. If similar incidents have happened, then details related to the similar incidents are cited in this section.

Section 5 – is for general comments about anything else that is not covered in Sections 1–4.

You may download the latest MIR form from the website of the European Commission at https://ec.europa.eu/growth/sectors/medical-devices/current-directives/guidance_en

25.5.5 Medical Device Reporting

Code of Federal Regulation Title 21, part 803 is the US law that requires the reporting of deaths or serious injuries that have been, or may have been caused by a medical device. The mechanism used is called Medical Device Reporting (MDR). This is similar to the European Vigilance system and is a Post-Market Surveillance tool that informs the FDA and the public of detected device-related issues that could have contributed to a death or serious injury.

Reporting is mandatory by manufacturers, importers, and device user-facilities. Reporting is voluntary by Healthcare Professionals, patients, caregivers, and consumers.

MDR submissions depend on the device safety class, and Severity of the event.

Reporting is done on form 3500A which is intended for use by the manufacturers, importers, and device user facilities, and can be downloaded at https://www.fda.gov/media/69876/download. This form is also known as the MedWatch form. General instructions for filling out form 3500A can be found at https://www.fda.gov/media/82655/download.

Form 3500 is intended for voluntary reporting by Healthcare Professionals, patients, caregivers, and consumers. The form can be downloaded at https://www.fda.gov/media/76299/download

25.6 CLINICAL EVALUATION

EU MDR [2] defines Clinical Evaluation as a systematic and planned process to continuously generate, collect, analyze, and assess the clinical data pertaining to a device in order to verify the safety and performance, including clinical Benefits, of the device when used as intended by the manufacturer.

Clinical Evaluations can be initially performed to support the original CE marking of a medical device, or they can be periodic activities (e.g., annual) that continue to examine and evaluate all the available information to confirm the performance, risks, and Benefits of a medical device.

Although Clinical Evaluation is not within the domain of ISO 14971, it is of value to discuss the topic, because there is interplay between risk management and Clinical Evaluation. Below, Clinical Evaluation is described at a high level to create awareness of the subject and understanding of the connection with risk management.

Clinical Evaluations are done in three steps:

Step 1: Identify and collect clinical data about the device under evaluation.

Potential sources:

- pre-market or Post-Market clinical studies
- pre-clinical testing
- Post-Market Clinical Follow-ups
- comprehensive literature reviews
- examination of clinical experience data
- complaint monitoring
- Post-Market Surveillance
    - product surveillance registries
    - Vigilance reports
    - Field Safety Corrective Actions

Step 2: Screen the collected data

Apply inclusion/exclusion criteria and appraise the data for applicability, relevance, quality, adequacy, significance, etc.

Step 3: Analyze the collected data

Analyze the collected data and draw conclusions on whether there is sufficient clinical evidence to meet the GSPR in Annex I of EU MDR [2]. The Clinical Evaluation may conclude that further clinical investigation is necessary.

A hallmark of Clinical Evaluations is literature search. A variety of data sources could be used for searches. Examples:

- Embase® by Elsevier – goes back to 1947; contains over 29 million records from more than 8500 journals from at least 90 countries. Includes all of MEDLINE® plus over 2000 extra titles (including more EU journals) and 260,000 conference abstracts. Contains Cochrane Reviews.
- PubMed® – has been available since 1996. It has more than 30 million references.

- MEDLINE® – the US National Library of Medicine. Started in the 1960s, it now provides more than 26 million references to biomedical and life sciences journal articles back to 1946. MEDLINE is a subset of PubMed®.
- Cochrane Reviews – a database of systematic reviews and meta-analyses provided by Wiley and Sons.

A successful search of databases requires the thoughtful choice of key terms, and time frames. The literature search should include all relevant published scientific literature, both favorable and unfavorable.

An important element of Clinical Evaluation is examination of the State-of-the-Art (SOTA) to ensure the medical device remains a viable alternative in the context of the SOTA. Examination of the SOTA involves identifying the latest practice guidelines and recommendations, consensus statements, and systematic reviews related to the specific indications and populations covered. Knowledge of the SOTA is pivotal in the determination of Benefit-Risk ratio, which is a key requirement of ISO 14971 [1].

Another activity that provides input for Clinical Evaluations comes from the review of the relevant internal RMRs and RMFs to ensure the list of hazards and harms are up-to-date.

Clinical Evaluations should be thorough and objective, and be commensurate in depth and extent, with the risks of the device and the claims of Benefits of the device.

The Clinical Evaluation may identify gaps in clinical evidence to demonstrate conformity with the general safety and performance requirements for the device and recommend actions to close the gaps.

The results of a Clinical Evaluation are documented in a Clinical Evaluation Report (CER). Writing a CER is a cross functional activity involving many disciplines, such as: Clinical Affairs, Regulatory, Vigilance, and Medical Affairs. See Section 25.6.2 below for more details about CERs.

EU MDR [2] Annex XIV, Part A requires that manufacturers plan, continuously conduct, and document a Clinical Evaluation process for medical devices to demonstrate conformity with the general safety and performance requirements defined in EU MDR [2] Annex I. See Section 25.6.1 for additional details on the Clinical Evaluation Plan.

Historically, under MDD [3]/AIMDD [4], Clinical Evaluations were used to demonstrate conformity to the essential requirements listed in MDD [3]/AIMDD [4] Annex I.

25.6.1 Clinical Evaluation Plan

As in other risk management activities, Clinical Evaluation must follow a plan. Briefly, the minimum requirements for a Clinical Evaluation Plan as specified in EU MDR [2] Annex XIV, Part A are:

- Identify the general safety and performance requirements of the device under evaluation, that require support from relevant clinical data.
- Specify the Intended Purpose of the device.
- Provide a clear specification of intended patient target groups with clear Indications and Contraindications.
- Provide a detailed description of the intended clinical Benefits with relevant and specified clinical outcome parameters.
- Specify methods to be used for examination of qualitative and quantitative aspects of clinical safety with clear reference to the determination of Residual Risks and side-effects.
- Provide a list of parameters to be used to determine the acceptability of the Benefit-Risk ratio.
- Provide a plan for necessary clinical studies to support the Clinical Evaluation — from exploratory investigations, such as first-in-man studies, feasibility and pilot studies, to confirmatory investigations, such as pivotal clinical investigations, and a PMCF. Include milestones and potential acceptance criteria.

The Clinical Evaluation Plan becomes part of the technical documentation of the device.

25.6.2 Clinical Evaluation Report

The Clinical Evaluation Report (CER) is a crucial part of the technical file for CE marking a device and is required for all device classifications. The CER is a living document that is updated periodically — more frequently for higher risk devices, and less frequently for low-risk devices. As time goes on, and more data becomes available, the CER provides better and more accurate assessment the device safety and performance.

Although there is no mandatory format for a CER, there are some resources that can be used as references. For example, MDCG 2020-13 [54] or MEDDEV 2.7/1 [48], Annex A9. Below, a high-level description of key elements of the CER is presented.

25.6.2.1 CER Template Structure

Below, a suggested CER structure is provided. Not every element in the structure will be present in every CER.

Executive summary

Identification of the device, and summary of the determination of the Benefit-Risk Analysis of the device and the acceptability of risk profile based on the state-of-the-art.

Purpose and Scope of the Clinical Evaluation

- Purpose: verification of performance and safety of the medical device
- Scope: whether the CE encompasses one device, a family of devices, or a class of devices
- Device identifier information

Overview

- Details of identification of the device/device family, e.g., model numbers, etc.
- Description of the device, including any accessories
  - Physical, chemical, functional description
  - Product characteristics, e.g., sterility, stability, radioactivity, etc.
  - Materials used in particular biocompatibility
  - Any relevant pre-clinical information
  - Any changes in materials/design/labeling since the previous CER
- Principles of operation
- Intended Purpose, Indications, Contraindications
- Intended target population
- Intended Use, e.g., single/multi use, part of the body, etc.
- Specific claims of Benefit
- Potential risks associated with the use of the device
- Relevant Warnings and Precautions
- Compliance with any Common Specifications, or Standards
- Expected lifetime of the device

Device Equivalence (if applicable)

If data from an equivalent is used to support safety and performance of the device, provide supporting information to demonstrate equivalence. The types of information used to demonstrate equivalence include:

- Technical: similarity in specification, design, properties, principles of operation, and use-conditions.
- Biological/chemical: use of the same materials that come into contact with human tissue, similar duration and type of tissue contact, similar leachables, and degradation properties.
- Clinical: same purpose, disease, part of the body, same target population, and type of user

There should be no significant clinical difference with the predicate device's safety and performance.

State-of-the-art

Establish the state-of-the-art for the treatment of the condition that is addressed by the subject medical device. Consider: benchmark devices, alternative therapies, the natural course of the disease, current best practices in the treatment of the disease, and applicable standards/guidances.

Benefit-Risk Assessment

Provide a detailed Benefit-Risk assessment of the device in the context of the state-of-the-art. Include any new knowledge gained since the previous CER, with respect to risks and device performance. Ensure consistency with the RMF. Benefit-Risk assessment should consider the nature, magnitude, and duration of the Benefit and the extent to which the Benefit is valued by the target population. Make a clear statement whether the Benefits outweigh the risks in the context of the state-of-the-art.

Post Market Clinical Follow-up

Describe any current or planned PMCF activities, or whether there is a need for PMCF for any unanswered questions.

Conclusions

The conclusion section should include statements on the safety and performance of the device; any safety concerns; the Benefit-Risk balance; confirmation of the claimed clinical Benefits, and predicted risks, or reporting of any deviations thereof.

Data

- Sources of literature review
- Literature search protocols; usage and exclusion criteria
- Data generated and held by the manufacturer
- Preclinical data
- Non-clinical data
- PMS data
- PMCF data

The identified clinical data should be appraised for:

- Quality of the work, including methods, results, and conclusions
- Scientific validity of content
- Relevance to the Clinical Evaluation

Cadence of CER updates

The CER must be updated when new information is identified from Post-Market Surveillance, or on a regular schedule based on the risk of the medical device. For Class III medical devices, update annually. For devices of lower risk, update every 2—5 years.

25.7 FREQUENCY OF RISK MANAGEMENT FILE REVIEW

As Post-Market Surveillance continues to bring in new information about the product performance in the field, the Risk Management File should be periodically reviewed to determine need for update. The frequency of Risk Management File review depends on:

- the risks of the device
- the novelty of the device
- the duration of time that the device has been in the market

For a new, novel and high-risk device do more frequent reviews; perhaps as often as monthly or bimonthly. As the length of time that the device has been on the market increases, and more is learned about it, the review frequency can be reduced, e.g., every year, or every other year. For low-risk, old-technology devices, the review frequency could be even lower, e.g., every 4—5 years.

Whatever frequency the manufacturer chooses should be recorded in the RMP. Document the rationales for your decision on review frequency.

25.8 FEEDBACK TO PRE-MARKET RISK MANAGEMENT

There is a connection between the Post-Market and Pre-Market risk management. Knowledge gained from product performance after it is manufactured and released must be fed back to Pre-Market risk management in a drive to add veracity to the Pre-Market predictions and estimations of the risks of a medical device. The types of information that Post-Market risk management can provide to Pre-Market risk management are:

- Is there evidence of new Hazards that were previously not foreseen?
- Are the P1 and P2 estimations still valid?
- If qualitative methods are used, are the estimates of risks still valid?
- Are there reports of misuse which were not foreseen in the original risk management process?

- Are the Risk Controls proving to be effective in reducing/maintaining risk levels?
- Is there any evidence that the actual market experience of risk acceptability for the received Benefit has changed?

One of the key benefits of Production and Post-Production monitoring is the derivation of P1 and P2 numbers from field data. P1 and P2 estimates that are based on actual field data are far more credible than expert opinion. However, the key to successful mining of field data is thoughtful, well-planned, and well-executed collection, coding, and cataloguing of the field data.

P1 is the probability of occurrence of a Hazardous Situation. P1 is prevalence. P1 has units. The units of P1 are dependent on the application and are determined by the manufacturer. For example, for an insulin pump a sensible unit could be patient-hours of operation. For a sphygmomanometer (blood pressure monitor) a sensible unit could be number of uses. To measure P1, a certain time interval needs to be selected.

A hypothetical example: 50,000 units of insulin pump model X have been in operation between January 1, 2020 and June 30, 2021. During this period, the average length of service for model X has been 4000 hours. In the same time period, there have been 250 reported and confirmed cases of over-infusion.

$$P1 = 250/(50,000 \times 4000) = 1.25 \times 10^{-6} \; per \; patient - hour$$

This information should be fed back to Pre-Market risk management so that if the prediction of P1 for over-infusion was different from 1.25×10^{-6} it can be updated.

P2 is the probability of sustaining Harm, given that the Hazardous Situation has already occurred. In the BXM method, risk is computed in five Severity classes, as defined in Table 33.

P2 is outcome-based. To derive P2 from field data we need to know after the Hazardous Situation happened, what was the outcome for the patient. For example, in the insulin pump example above, we would ask, after the over-infusion event what was the Harm and what was the outcome to the patient? A potential Harm of insulin over-infusion is hypoglycemia. Potential answers to the above question could be:

- Patient died (fatal)
- Patient became unconscious and suffered brain damage (critical)
- Patient fainted and was taken to the emergency room, but has recovered now (major)
- Patient felt a little lightheaded but ate a piece of candy and was fine (minor)
- Patient reported feeling a little strange, but it passed (negligible)

Each of the above answers would be counted as one instance in each of the five Severity classes. Let's imagine that in a dataset of 97 hypoglycemia events we have the following counts:

- Fatal: 0
- Critical: 2
- Major: 20
- Minor: 25
- Negligible: 50

P2 is agnostic of the Hazardous Situation. That means we want to know, for all reported cases of hypoglycemia regardless of the Hazardous Situation that caused it, what were the outcomes. So, if two different Hazardous Situations could cause hypoglycemia, we aggregate all the hypoglycemia cases together. In the hypoglycemia example, over infusion of insulin can lead to hypoglycemia. Also, excessive consumption of alcohol can cause hypoglycemia. Regardless of what caused the hypoglycemia, we are interested on the impact on the patient.

Continuing with our example, the total cases of hypoglycemia were: 97. Therefore, for the Harm of hypoglycemia P2 numbers are:

- P2(Fatal): 0/97 = 0%
- P2(Critical): 2/97 = 2.1%
- P2(Major): 20/97 = 20.6%
- P2(Minor): 25/97 = 25.8%
- P2(Negligible): 50/97 = 51.5%

To ensure effective feedback loops from Post-Market to Pre-Market risk management, it is advisable that the responsibility for maintaining the Risk Management File be defined and assigned to specific staff.

25.9 BENEFITS OF POST-MARKET SURVEILLANCE

Clearly patient/user safety is enhanced by active surveillance of Production and Post-Production information about market-released products. But the manufacturer also receives significant benefit from the surveillance. Namely, the opportunity to quickly identify and rectify product/process defects. This in turn leads into reduced customer complaints, reduced field corrective actions, improved reputation and customer loyalty, which means higher sales. And if that's not enough motivation, failure to perform product surveillance could result in substantial fines, criminal prosecutions, seizure of product, and closure of the business.

Another benefit of Post-Market Surveillance is about the clinical Hazards list (CHL) (see Section 13.5). The CHL is an invaluable tool of risk management. The CHL is claimed to be complete, at any given time. The basis of that claim is that the CHL is a living document, containing the best available knowledge at any given time. And, if any new Hazards are discovered, they are added to the CHL. Without Post-Market Surveillance data, we cannot make the claim of completeness.

CHAPTER 26

Traceability

Abstract

ISO 14971 requires manufacturers to provide traceability for each Hazard to its risk analysis, risk evaluation, Risk Controls, residual risk evaluation, verification of implementation, and effectiveness of Risk Controls. This chapter examines methods and strategies for capturing and documenting traceability for medical devices.

Keywords: Traceability; traceability map; software traceability; Risk Management Report

ISO 14971 Section 4.5 [1] requires manufacturers to provide traceability for each Hazard to its Risk Analysis, Risk Evaluation, Risk Controls, Residual Risk evaluation, verification of implementation and effectiveness of Risk Controls. For medical devices that include software, IEC 62304 Section 5.1.1 [10] requires that traceability between System requirements, software requirements, software system tests, and Risk Control measures implemented in software must be made.

Traceability is an invaluable tool to ensure completeness in risk management. Without traceability, it is possible to miss Hazards, fail to control their risks, or fail to verify their Risk Controls. Fig. 55 depicts a model for traceability for risk management.

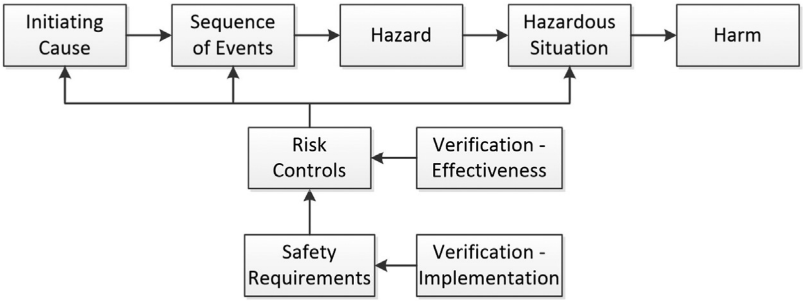


Figure 55 Traceability Model.

You can capture your traceability in any form that is convenient. Examples include spreadsheets, databases, or requirements management systems.

DOI: https://doi.org/10.1016/B978-0-323-85755-0.00026-6

Traceability between Hazards and Risk Analysis can be captured in the RACT. That is, the description of initiating event and the subsequent sequence of events that lead into the Hazard are captured in the RACT. Similarly, the traceability between each Hazard and the evaluation of the risks associated with that Hazard can be captured in the RACT.

The assessment of acceptability of the Residual Risks must also be documented. In the BXM method this traceability is captured in the RACT.

As design, implementation, testing, and risk management activities continue, it is crucial that the integrity of traceability links be maintained. Without this diligence, it is easy for the links to become inaccurate. The use of automation tools can help with this endeavor. Many requirements management tools enable the creation of entities, e.g., requirements, Risk Controls, or test cases, and to link such entities within the tool. This is very convenient for up-to-the-minute viewing and reporting of link maps. Moreover, the tools can flag links as suspicious, if one or the other end of the link is modified. For example, if the link between a requirement and a verification test is established, and then the requirement is modified, the validity of the associated verification test goes under question. The requirements management tool can automatically flag the link between the requirement and its verification test for review. The engineers can then review the contents of both ends of a suspicious link and verify whether the link is still valid.

For devices of even moderate complexity the traceability analysis report would be a large document. For this reason, it is not recommended that the traceability analysis report be included in the Risk Management Report (RMR), as it could make the RMR too large and unwieldy. Instead, it is better to include a summary of the traceability analysis report in the RMR, and make a reference to the traceability analysis report, as one of the elements of the Risk Management File (RMF).

CHAPTER 27

Lifetime of a Medical Device

Abstract

Medical devices, like any other system, have a limited life. Knowledge of the expected lifetime of a medical device is necessary for the fulfillment of the European Medical Device Regulation, and the US FDA. Besides meeting regulatory requirements, the manufacturer benefits from knowledge of the expected device lifetime for business reasons, such as warranty period determination. Several factors are presented to aid the manufacturer in determining the expected device lifetime.

Keywords: Device lifetime; expected service life; useful life

Medical devices, like any other system, age and decay over time. This is of importance for multiple reasons. From a business perspective, the manufacturer wants to know how long to warranty the device; what the maintenance costs of the device are; and when the product should be replaced. From the risk management perspective, we are interested to know how long the device can be used for its Intended Purpose without causing unacceptable safety risks to patients/users.

EU MDR, Annex I, par. 6 [2] states that "The characteristics and performance of a device shall not be adversely affected to such a degree that the health or safety of the patient or the user and, where applicable, of other persons are compromised during the lifetime of the device."

EU MDR [2] Article 18 requires the specification of device lifetime in the Implant Card.

Article 83 [2] requires performance of Post-Market Surveillance for the entire lifetime of the device.

Article 86 Section 1 [2] requires that Periodic Safety Update Reports be prepared throughout the lifetime of the device.

IEC 60601-1 [7] requires that the manufacturer state the Expected Service Life of the medical device.

Additionally, the US CFR 21 part 821 authorizes the FDA to require manufacturers to track certain types of medical devices for their useful life. The FDA Medical Device Tracking Guidance [55] describes the types of devices that must be tracked.

Safety Risk Management for Medical Devices
DOI: https://doi.org/10.1016/B978-0-323-85755-0.00027-8

There are many factors that can be the basis of the defined lifetime of a device, for example: technical, safety, legal, commercial, or other factors.

According to ISO/TR 14969 [56] Section 7.1.3, factors that affect the device lifetime are:

- **a.** shelf life of the medical device
- **b.** expiry date for medical devices or components which are subject to degradation over time
- **c.** number of cycles or periods of use of the medical device, based on life testing of the medical device
- **d.** anticipated material degradation
- **e.** stability of packaging material
- **f.** for implantable devices, the Residual Risk that results from the entire period of residence of the device inside the patient's body
- **g.** for sterile medical devices, the ability to maintain sterility
- **h.** organization's ability/willingness or contractual or regulatory obligation to support service
- **i.** spare parts cost and availability
- **j.** legal considerations including liability

ISO/TR 14969 [56] has been withdrawn, but the guidance that it offers is still beneficial.

At a minimum, the expected lifetime of a medical device is the duration over which the medical device can be used for its Intended Purpose, according to instructions for use, and deliver its expected safety and performance requirements while maintaining an acceptable Benefit-Risk ratio. For business reasons, e.g., cost of maintenance, a shorter life may be stipulated. From a practical perspective, considering all factors, the shortest number governs.

The device lifetime could be expressed in clock time, or in the number of uses, or number of activations, etc. The manufacturer should be able to state the rationale for the choice of device lifetime, which could be based on the factors mentioned above.

CHAPTER 28

Safety Versus Reliability

Abstract

There is a general misperception that reliability and safety are the same, and that a reliable device is a safe device. While this is sometimes true, it is not a universal truth. Unreliable devices can be safe, and reliable devices can be unsafe.

Keywords: Safety; reliability

There is a general misperception that reliability and safety are the same, and that a reliable device is a safe device. While this is sometimes true, it is not a universal truth.

Reliability is defined as the ability of a system or component to function as intended, for a specified length of time, under stated conditions. Safety is defined as freedom from unacceptable risk. These are different concepts.

A simple example is a scalpel. A reliable scalpel will cut tissue every time. But if the design of a scalpel makes it conducive to cut the surgeon's hand, there is a safety issue. A converse example – imagine a medical device that has so many safety mechanisms that it frequently shuts down to avoid causing injury. The device may be very safe, but also very unreliable. Typically, when safety mechanisms have high sensitivity but low specificity, we encounter safe but unreliable Systems.

The role that reliability plays in safety is when both attributes are aligned. Take the example of a stent. An unreliable stent that dislodges or fractures would be also an unsafe stent. When safety and reliability are aligned, improved reliability also improves safety.

Safety Risk Management for Medical Devices
DOI: https://doi.org/10.1016/B978-0-323-85755-0.00028-X

CHAPTER 29

Risk Management for System of Systems

Abstract

A System of Systems (SoS) is an assembly of two or more interoperable systems together with any Accessories that delivers a clinical function. Modern complex medical systems can be comprised of a number of interoperable individual medical devices. While each individual device has its own Risk Management File, it is the SoS that delivers the clinical benefit. Risk Management Reports of individual medical devices should consider the risk to the patient in the context of the SoS.

Keywords: System of Systems; SoS; direct harm; indirect harm

Medical devices vary in complexity. Some are as simple as a surgical glove, and some are highly complex Systems of Systems (SoS). In modern hybrid operating rooms, such as the example in Fig. 56, a multitude of interconnected and communicating medical devices are working together to support the clinicians to deliver a clinical Benefit to the patient.

Figure 56 Hybrid Operating Room.

Each element within the SoS would be an approved, e.g., CE-marked, medical device with its own Risk Management File. To be a part of the SoS, a device must be interoperable within the SoS. Otherwise, that device is not part of the SoS.

One of the challenges with medical device risk management in systems of systems is that as technology advances, various parts of the system of systems get updated in an asynchronous manner. Ensuring the continued safety of one system in the SOS requires continuous vigilance and monitoring of the SoS.

DOI: https://doi.org/10.1016/B978-0-323-85755-0.00029-1

In this chapter we discuss how to manage the risks of systems of systems.

29.1 DEFINITION OF SYSTEM OF SYSTEMS

An SoS is an assembly of two or more interoperable systems together with any Accessories that delivers a clinical function.

The SoS may include Medical Devices and humans who function as part of the SoS. Fig. 57 depicts a schematic of how an SoS interacts with the patient. Some Medical Devices can present direct hazards to the patient, and some can present indirect hazards to the patient. The clinician, who is part of the system, may also inflict Harm to the patient via one of the Medical Devices.

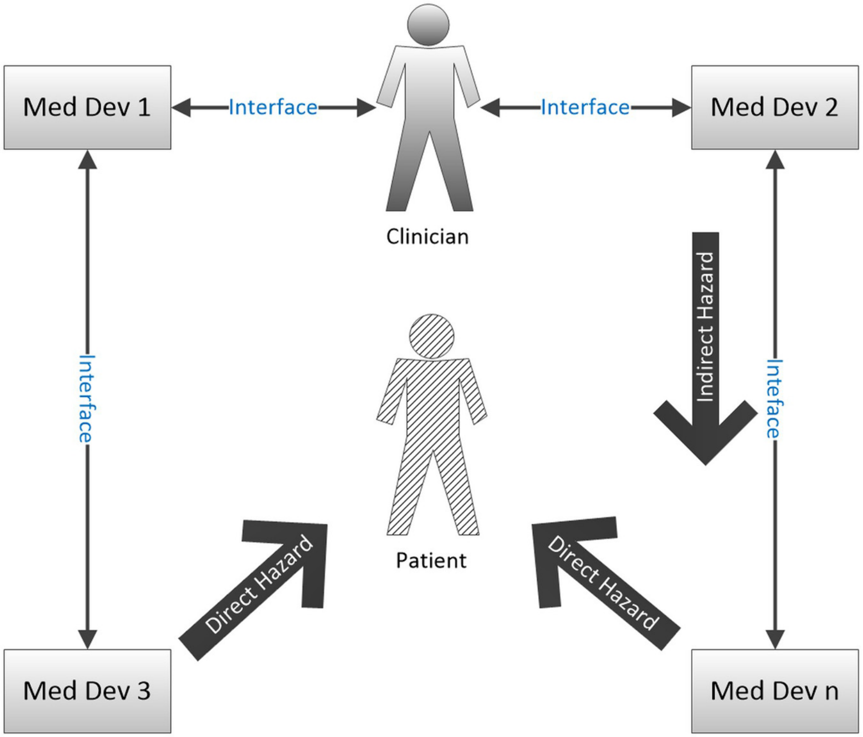


Figure 57 System of Systems.

Should the human be included as part of the SoS? The answer is: it depends. A human who has no control over the system is not part of the system, but is a subject of the system. For example, a patient with implanted spinal fusion hardware is not part of the system. But a physician who receives diagnostic data from an SoS and reacts to that data, programming the SoS accordingly, is part of the system. In the latter example, the human has direct control and influence on the SoS performance – similar to other elements of the SoS.

29.2 DIRECT AND INDIRECT HARMS

Medical Devices have the potential to cause two types of Harm:

- Type 1 – Direct Harm
- Type 2 – Indirect Harm

Both types of Harm can be under fault and non-fault conditions.

Direct Harm occurs when a Medical Device presents a Hazard, exposure to which could potentially Harm the patient/user. Example: a surgical tool that is supposed to be smooth, has a sharp edge on it.

Indirect Harm means exposure to the Medical Device itself does not cause Harm. But the interoperation of the Medical Device with other systems in the SoS does create Hazardous Situations, from which harms can arise.

In Fig. 58, the Failure Mode of Med Dev 1 would cause Med Dev 2 to present a Hazard to the patient. Exposure to the Failure Mode itself, does not cause Harm.

Example: A pulse oximeter incorrectly measures the patient's blood oxygen level, leading to the nurse reducing the oxygen flow to the patient, leading to hypoxia. Exposure to the data coming out of the pulse oximeter doesn't cause Harm. But exposure to low oxygen levels does.

Each Medical Device in an SoS should have a RACT to estimate and evaluate the risks of direct harms that it can cause. For indirect harms, the RACT usage would need to be

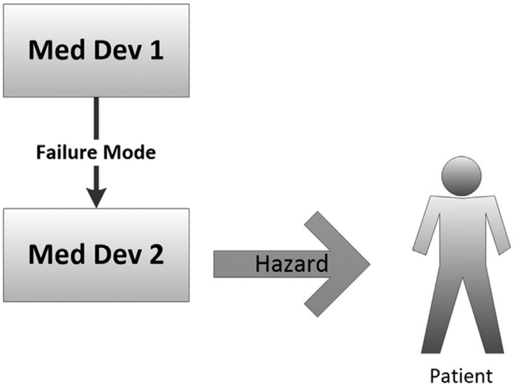


Figure 58 Direct and Indirect Harms.

modified in that since the device itself does not present any direct hazards, the hazards at the SoS level can be cited and P1 at the system level can be estimated in the device's RACT. In the example of the pulse oximeter, the device could pinch or scratch the finger (direct harms). The risks of direct harms are estimated and evaluated in the RACT as normal. But the pulse oximeter could also indirectly cause hypoxia (indirect Harm). For the indirect harms, the Hazard and Harm at the SoS-level are cited in the pulse oximeter RACT, and P1 is conservatively set to P(patient not receiving sufficient oxygen).

29.3 ASSESSMENT OF THE RISKS OF AN SOS

Let's consider the SoS in Fig. 59. This SoS is comprised of four medical devices that together deliver the clinical Benefit to the patient. The patient directly interfaces with System 4, through which he receives the clinical Benefit. Also, the patient can receive direct Harm from System 4, and indirect harms from Systems 1, 2, and 3.

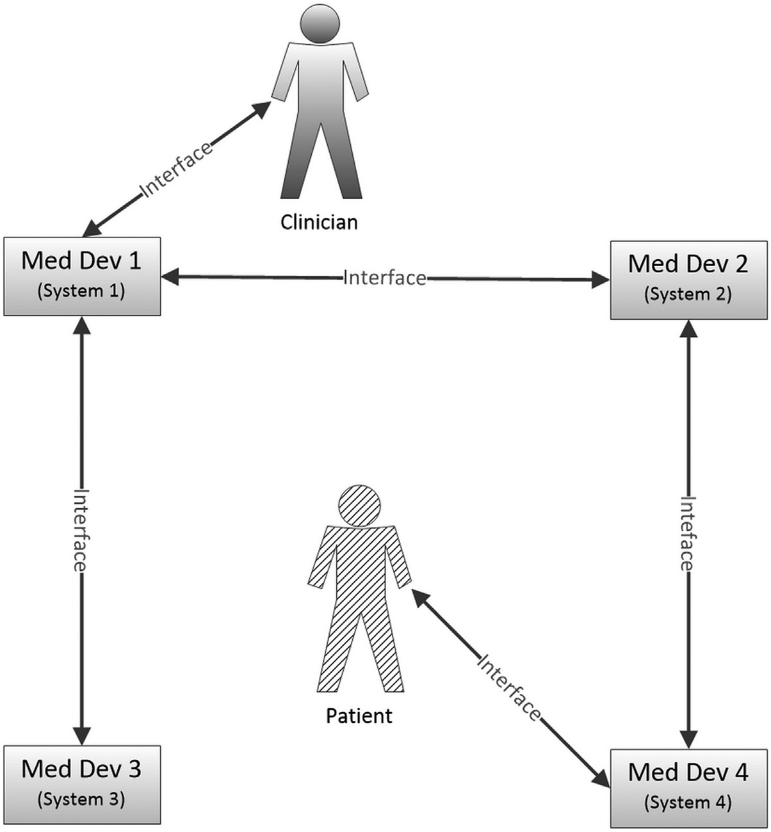


Figure 59 Risk Estimation with a System of Systems.

Most medical device manufacturers of an SoS like the one in Fig. 59 submit each element of the SoS separately for Regulatory approval. That is because each element is packaged and sold as a device, by itself. The submission for each medical device has its own dossier and Risk Management Report, within which the Overall Residual Risk (ORR) of the medical device is evaluated. Since none of the elements of the depicted SoS can alone deliver the clinical Benefit, and the patient interfaces with the entire SoS, how can we determine the ORR of each element of the SoS? Below, a method is presented to address this question.

1. Determine the ORR for the entire SoS. This would be captured within the RACT of the SoS.
2. For each element in the SoS (each interoperable medical device), isolate the rows of the SoS RACT that represent the contributions of that element to the hazards of the SoS.
3. For each element of the SoS, aggregate the risks of all the rows that were isolated in step 2 – these are the relevant risks of each element of the SoS. This action would produce the ORR for each element of the SoS, within the context of the SoS.

CHAPTER 30

Risk Management for Clinical Investigations

Abstract

Clinical investigations are governed by ISO 14155, which addresses good clinical practice for the design, conduct, recording, and reporting of clinical investigations carried out on human subjects. ISO 14155 requires that prior to the execution of clinical trials, the risks associated with clinical trials be estimated in accordance with ISO 14971. In this chapter the risk management requirements of ISO 14155 are discussed and the interaction between ISO 14155 and ISO 14971 are described. Special terminology of Clinical Investigations is presented and mapped to the terminology of ISO 14971.

Keywords: Clinical investigations; risk management; clinical study

In this chapter, we will examine the requirements for risk management in clinical investigations. Clinical investigations are governed by ISO 14155 [18], which addresses good clinical practice for the design, conduct, recording, and reporting of clinical investigations carried out on human subjects (also called participants). With respect to risk management, ISO 14155 [18] has a broader view than just health safety. That is because a clinical investigation is a project. Section 6.2.3 of the standard [18] addresses risks to planning and conduct of clinical investigations, risks to the reliability of clinical data, and risks to the safety of the subjects. As the focus of this book is management of risks to the safety of humans, we will not address the project risks of clinical investigations.

ISO 14155 [18] defines Clinical Investigation as a "systematic investigation in one or more human subjects, undertaken to assess the safety or performance of a medical device."

Note: according to ISO 14155 [18] Section 3.8, the terms "clinical trial" or "clinical study" are synonymous with "clinical investigation."

Clinical studies are conducted to increase medical knowledge as to how a medical device performs in humans. Some examples of the reasons for conducting clinical studies:

- Evaluate the clinical Benefits of a medical device in treatment of diseases, syndromes, or conditions in the target patient populations.
- Evaluate the risks associated with the use of a medical device both due to the medical device itself, and how it would be used in clinical settings.

Safety Risk Management for Medical Devices
DOI: https://doi.org/10.1016/B978-0-323-85755-0.00030-8

- Confirm the predicted risks and identify any new Hazards associated with the use of the medical device.
- Gain insight into uncertainties about the performance of the medical device in vivo.
- Identify rare complications.
- Examine the performance of the medical device under long-term and widespread use.
- Investigate particular features regarding clinical utility.
- Assess cost/Benefit or health outcomes in support of reimbursements.

30.1 TERMINOLOGY

In the remainder of this chapter references are made to the following terms. It is important to understand the language of clinical investigations and be able to distinguish the terms.

Adverse Device Effect (ADE): "Adverse event related to the use of an investigational medical device" ([18] 3.1).

Adverse Event (AE): "untoward medical occurrence, unintended disease or injury, or untoward clinical signs (including abnormal laboratory findings) in subjects, users or other persons, whether or not related to the investigational medical device and whether anticipated or unanticipated" ([18] 3.2).

Anticipated Serious Adverse Device Effect (ASADE): "effect which by its nature, incidence, severity or outcome has been identified in the risk assessment" ([18] 3.51, Note 1).

Clinical Evaluation: "a systematic and planned process to continuously generate, collect, analyze and assess the clinical data pertaining to a device in order to verify the safety and performance, including clinical Benefits, of the device when used as intended by the manufacturer" [2] Article 2 (44).

Clinical Investigation: "systematic investigation in one or more human subjects, undertaken to assess the clinical performance, effectiveness or safety of a medical device" ([18] 3.8).

Clinical Investigation Plan (CIP): "document that states the rationale, objectives, design and pre-specified analysis, methodology, organization, monitoring, conduct and record-keeping of the clinical investigation" ([18] 3.9).

Investigator's Brochure (IB): "compilation of the current clinical and non-clinical information on the investigational medical device(s), relevant to the clinical investigation" ([18] 3.31).

Serious Adverse Device Effect (SADE): "adverse device effect that has resulted in any of the consequences characteristic of a serious adverse event" ([18] 3.44).

Serious Adverse Event (SAE): "adverse event that led to any of the following

a) death,
b) serious deterioration in the health of the subject, users, or other persons as defined by one or more of the following:
  1) a life-threatening illness or injury, or
  2) a permanent impairment of a body structure or a body function including chronic diseases, or
  3) in-patient or prolonged hospitalization, or
  4) medical or surgical intervention to prevent life-threatening illness or injury or permanent impairment to a body structure or a body function,
c) foetal distress, foetal death or a congenital abnormality or birth defect including physical or mental impairment" ([18] 3.45).

Unanticipated Serious Adverse Device Effect (USADE): "serious adverse device effect which by its nature, incidence, severity or outcome has not been identified in the current risk assessment" ([18] 3.51).

Some noteworthy input from Ref. [18]:

- In general, "observational" clinical trials are "non-interventional"
- "Post-Market clinical investigation" can be a part of "Post-Market Clinical Follow-up"

  The terms "Clinical trial" or "clinical study" are synonymous with "clinical investigation."

30.2 CLINICAL STUDIES

Before we discuss the requirements of risk management for clinical studies, it is important to understand the different types of clinical studies.

There are many factors that determine the type of clinical study:

– Pre-market, Post-Market
– Exploratory, confirmatory, or observational
– Interventional, non-interventional

In the earliest stages of medical device development, it may be necessary to evaluate the merits and limitations of a new device, prove a concept, or test a new Indication for an existing device. These are pre-market, exploratory, or feasibility studies performed on a small number of participants and require risk management.

If the exploratory studies produce good results, a confirmatory pivotal clinical investigation can be performed to collect data on the safety and efficacy of the device on a larger group of participants. Pivotal clinical investigations also require risk management.

After the device is approved for market release, Post-Market confirmatory clinical investigations can be performed on the device in order to collect data on the clinical performance, safety, and efficacy of the device. Risk management may be necessary depending on the objectives of the clinical investigation plan.

Another type of clinical investigation is the observational Post-Market study, where the device is used within its labeled Indication. This type of study collects data on large groups of patients to evaluate specified outcomes on patient populations, and serves scientific, clinical, reimbursement, or policy purposes. Often these are registry studies where the decision to use the medical device is clearly separated from the decision to include the subject in the clinical study. Observational Post-Market studies do not introduce any additional risk on the study participants and risk management is not required prior to the start of the study.

30.3 MAPPING OF RISK MANAGEMENT TERMINOLOGIES

ISO 14155 [18] defines Serious Adverse Event as an event that led to: "

a) death,

b) serious deterioration in the health of the subject, users, or other persons as defined by one or more of the following:

  1) a life-threatening illness or injury, or

  2) a permanent impairment of a body structure or a body function including chronic diseases, or

  3) in-patient or prolonged hospitalization, or

  4) medical or surgical intervention to prevent life-threatening illness or injury or permanent impairment to a body structure or a body function,

c) foetal distress, foetal death or a congenital abnormality or birth defect including physical or mental impairment"

A commonly used set of definitions for Harm severities, based on ISO/TR 24971 [15] Table 4 is presented in Table 33.

ISO 14155 [18] requires that the risks associated with the clinical investigations be estimated in accordance with ISO 14971 [1]. This necessitates the mapping of terminologies among the two standards. It could be surmised that "Serious Adverse Event"

Table 33 Definitions of Severity Based on ISO/TR 24971 Table 4

Severity Class	Definition
Fatal	Death
Critical	Permanent impairment or irreversible injury
Major	Injury or impairment requiring medical or surgical intervention
Minor	Temporary injury or impairment not requiring medical or surgical intervention
Negligible	Inconvenience or temporary discomfort

maps to Fatal, Critical, and Major severities of Harm, and therefore, Minor and Negligible classes of Harm Severity would NOT be Serious Adverse Events.

As it is intended that Clinical Investigations provide feedback to risk management regarding the risks of the medical device, a higher resolution classification of Serious Adverse Events is needed to facilitate proper feedback to Risk Management. The CIP would be a good place to capture the higher resolution classification of Adverse Events and Serious Adverse Events during the Clinical Investigations.

30.4 RISK MANAGEMENT REQUIREMENTS

ISO 14155 Section 6.2.2 [18] requires that prior to the execution of clinical trials, the risks associated with the use of the investigational device be estimated in accordance with ISO 14971 [1].

The participants in a clinical investigation are faced with two types of risk:

- Risks associated with the medical device
- Risks associated with the design and conduct of the clinical study, including any follow-ups

The risks associated with the medical device are the main subject of this book and are covered extensively. The risks associated with the conduct of the clinical study could involve the clinical study design, methods of data collection, data processing, clinical setting, personnel performance, etc.

Risk management must estimate and balance the combined risks against the potential Benefits of the clinical study. The same principles that are applied to the management of the device risks, are applied to the design and conduct of the clinical investigation. The clinical study risks must be analyzed, estimated, controlled, and evaluated.

When analyzing risks, consider the risks not only to the participants, but also to the clinicians, investigators, and other persons.

Benefit-Risk Analysis for clinical studies is different from the Benefit-Risk Analysis of commercially released devices in that the point of the study is to demonstrate the Benefit. As such, risk management considers the expected and potential Benefits of the device in the Benefit-Risk Analysis.

As part of the risk management of the clinical study, it is expected that a thorough review of published and available unpublished literature be done to uncover any known risks that could be relevant to the clinical study.

For a clinical investigation, risks are controlled over two horizons: before an Adverse Event, and after the Adverse Event. Before the Adverse Event, Risk Controls aim to prevent the Hazardous Situations from happening. After the Adverse Event Risk Controls aim to limit the Harm. Actions such as patient monitoring, Adverse Event reporting, or termination of the clinical investigation are designed to limit the Harm to study participants. The study sponsor should design and implement appropriate training for the clinical investigators to ensure that proper data collection, processing, Hazard recognition, and escalation activities are performed. The extent and scope of this training should be based on the Severity of the risks, as communicated from risk management.

Risk Controls could include instructions and training to the investigators. In exceptional cases where an instruction for use is not required, the collection, appraisal, and analysis are conducted taking into account generally recognized modalities of use [48].

Sometimes clinical studies that intend to investigate a new Indication for an existing device, use an approved device off-label. The additional device-risk which is introduced from the off-label use, is counterbalanced by the close clinical monitoring and safety protocols of the clinical investigation.

Clinical investigations are themselves a component of the risk management process in that they provide evidence of the Benefits, which is used in the Benefit-Risk Analysis.

At the end of the clinical investigation the risk data collected should be reviewed and fed back into the risk management process for confirmation or revision of the estimated risks. Also, if any new Hazards were identified during the study, they should be added to the Risk Analysis. The Benefit-Risk Analysis should be revisited as well for confirmation or revision.

Any knowledge gained about the potential Hazards and risks of the medical device should be captured and communicated to the risk management process for use in future analyses of the risks of the subject device. Also, knowledge gained from the performance of the clinical investigation and risks that were manifested to the participants, users, or other persons should be captured and used in future clinical studies.

30.5 ADVERSE EVENT CATEGORIZATION

When an adverse event happens, it must be classified. In addition to the clinical investigations perspective, from a medical device risk-management perspective, we are interested to know whether the adverse event was caused by the medical device. The classification of adverse events helps with the investigation and determination of potential impact of the adverse events on the risk management file of the device. Fig. 60 depicts a thought process for classifying adverse events in alignment with ISO 14155 [18].

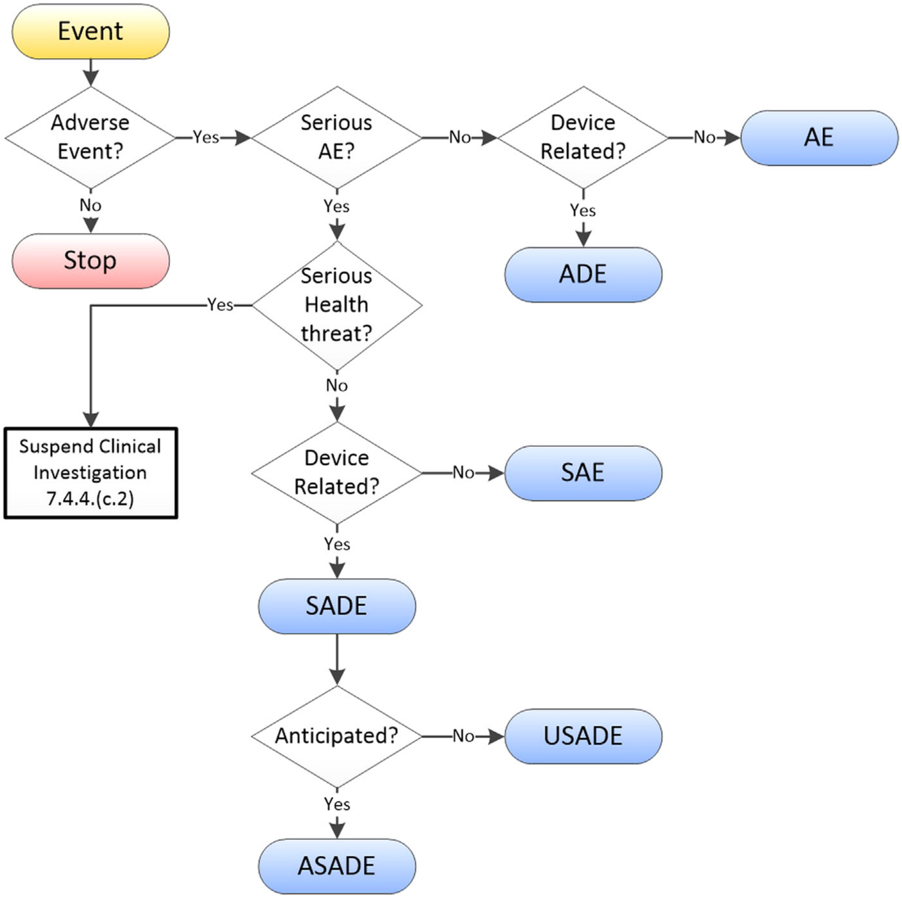


Figure 60 Adverse Event Categorization.

30.6 RISK DOCUMENTATION REQUIREMENTS

Risk management makes contributions to the required documents of clinical investigations. Table 34 outlines the contribution of risk management to elements of the clinical investigation documentation.

30.7 INFORMATION FLOW BETWEEN ISO 14971 AND ISO 14155

Clinical investigations are indeed a part of the risk management process. There is communication between the risk management process per ISO 14971 [1] and the clinical investigation process per ISO 14155 [18]. Certain information from risk management supports clinical studies, and reciprocally, certain information from clinical studies supports risk management. Below, the information flow between the two processes are described:

From risk management to clinical studies:

- Identification of hazards and risks
- Affirmation that risks are adequately addressed

Table 34 Risk Management Input to Clinical Documentation

Clinical Investigation Document	Risk Management Contribution
Clinical Investigation Plan (CIP)	Summary of Risk Analysis
	Anticipated adverse device effects
	Identification of Residual Risks
	Risk Controls
	Benefit-Risk Analysis summary
Investigator's Brochure (IB)	Summary of Risk Analysis
	Anticipated adverse device effects
	Identification of Residual Risks
	Anticipated risks, Contraindications, Warnings, etc.
	Benefit-Risk Analysis summary
	Results of risk assessment
Clinical Investigation Report (CIR)	Benefit-Risk Analysis summary
	Adverse events
	Adverse device effects
Informed Consent Form (ICF)	Anticipated adverse device effects

- Information for safety, Warnings, Cautions
- Acceptability of Benefit-Risk profile
- Special risk areas to focus/study
- Risk Management Report

From clinical studies to risk management:

- Confirmation of Benefits
- Confirmation of risk estimates
- Verification of effectiveness of Risk Controls
- Feedback on the user interface and IFU
- Support for Residual Risk acceptability
- Confirmation of hazards/harms, or discovery of new hazards/harms

CHAPTER 31

Risk Management for Legacy Devices

Abstract

For established manufacturers, it is likely that they have products that have been in the market for a long time. Perhaps even before the existence of ISO 14971. These products are termed Legacy Devices; defined as medical devices which were legally placed on the market and are still marketed today, but for which there is insufficient objective evidence that they are in compliance with the current version of the Standard. This chapter provides guidance on how to manage the risks of Legacy Devices.

Keywords: Risk management; legacy device

For established manufacturers, it is likely that they have products that have been in the market for a long time. Perhaps even before the existence of ISO 14971. These products are termed Legacy Devices; defined as medical devices which were legally placed on the market and are still marketed today, but for which there is insufficient objective evidence that they are in compliance with the current version of the Standard [1].

Since ISO 14971 [1] is intended to be applied throughout the entire life cycle, especially during the design phase, a retrospective application of the standard to an existing legacy device is not particularly valuable. However, an abbreviated application of the Standard [1] would be of value, particularly for Post-Production risk management and maintenance of the Risk Management File.

The following steps may be performed as an alternative to performing clauses 5 through 7 of the Standard [1].

1. Ensure there is a risk management process in place that is compliant with clause 4.1 of the Standard [1].
2. Prepare a Risk Management Plan for the legacy device in accordance with clause 4.4 of the Standard [1].

   The scope of the Risk Management Plan can be limited to: the creation of the Risk Management File, performance of Production and Post-Production risk management, and maintenance of the Risk Management File. The plan should define the actions and responsibility for field data collection and processing. If future versions of the device will be developed, the plan should lay out the appropriate activities for the risk management of the new device.

Safety Risk Management for Medical Devices
DOI: https://doi.org/10.1016/B978-0-323-85755-0.00031-X

3. Establish and maintain a Risk Management File per clause 4.5 of the Standard [1].
4. Identify the following for the Legacy Device:
   a. Intended Use, and clinical Indication
   b. Intended patient population
   c. Intended user profile
   d. Intended use-condition and environment
   e. Operating principle
   f. Characteristics related to safety
5. Considering item #4 above, identify the Hazards, Hazardous Situations, and potential Harms from the legacy device.
6. Identify the Risk Control measures that are already in place in the Legacy Device and classify them as: Safe by design or manufacture, Protective measures, or Information for safety/training.
7. Create a traceability report among the Hazards, Hazardous Situations, Harms, Risk Controls, and verification tests.
8. Create a Risk Management Report to document the above activities.
9. If advances in technology and practices enable the manufacturer to feasibly further reduce the device risks, then in the future releases of the legacy device additional Risk Controls should be implemented and the Risk Management File updated, including a new Benefit-Risk Analysis.

CHAPTER 32

Risk Management for Combination Medical Devices

Abstract

A combination medical device is a product composed of two or more different types of medical products, i.e., a combination of a drug, device, and/or biological product with one another. When managing the risks of combination medical devices, the total risk from the medical device has contributions from the device, the drug/biologic, and the interaction thereof.

Keywords: Combination medical device; interaction; drug; biologic; primary mode of action

Before embarking on the risk management of combination medical devices, we should first elucidate what they are. Title 21 CFR part 3 says a combination product is a product composed of two or more different types of medical products (i.e., a combination of a drug, device, and/or biological product with one another). For example, drug eluting stents, inhalers, or prefilled syringes are combination products. The Venn diagram in Fig. 61 depicts the universe of combination devices.

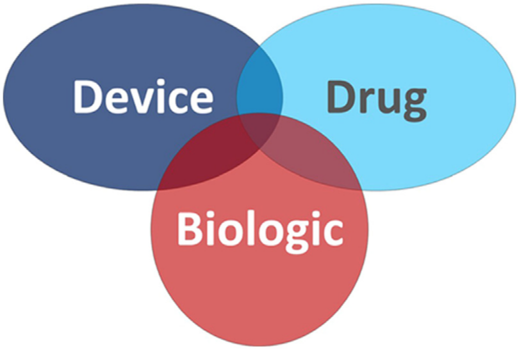


Figure 61 The Universe of Combination Devices.

What is not a combination medical device? A mere drug container or enclosure, such as Fig. 62, is not a combination medical device.

Safety Risk Management for Medical Devices
DOI: https://doi.org/10.1016/B978-0-323-85755-0.00032-1

Figure 62 A Simple Drug Container.

Combination devices can be sold as a single entity, such as the prefilled syringe in Fig. 63. See 21 CFR 3.2 (e)(1).

Figure 63 A Pre-Filled Syringe.

Or co-packaged (co-pack) where the device and the container are sold together in one package and the user assembles/combines them. See 21 CFR 3.2 (e)(2). A first aid kit is an example of a co-packaged combination device. Or, as a cross-label "set" where the products are separately packaged but are intended specifically to be used with each other to achieve the Intended Purpose. See 21 CFR 3.2 (e)(3), and (e)(4). An example of cross-labeled combination products is: photosensitive dental composite resin, and dental LED curing lights.

Because this book is concerned with risk management for *medical devices*, we will not address risk management for drug/biologic combinations. We will consider risk management for device/drug, and device/biologic combinations.

Combination devices can be evaluated as a device, drug, or biologic depending on their Primary Mode of Action (PMOA). The PMOA is the channel through which a device delivers its main Benefit. The PMOA of a drug eluting stent is device because its main purpose is to open the lumen of vessel in the body. On the other hand, the

PMOA of an auto-injector is drug because the main Benefit is derived from the drug, not the injector. Sometimes it is difficult to discern the PMOA of a combination device. For example, Vanilla SilQ™, a barium sulfate suspension used as a contrast agent which is ingested before X-ray or CT scans, is a liquid and appears to be a drug, but it has no chemical or metabolic reaction with the body. Therefore, it meets the definition of a device. Manufacturers can submit a Request for Designation (RFD) to the US FDA for help in designating the PMOA of their product.

Since drugs and biologics are both pharmaceuticals, for simplification of language, in the balance of this chapter the word drug is used to represent either drug or biologic.

Risk management is governed by ISO 14971 [1] for medical devices, and by ICH Q9 [57] for pharmaceuticals. ICH Q9 [57] is informed by ISO 14971 and as such there are similarities between ICH Q9 [57] and ISO 14971. Both documents focus on the health and safety, and expect risk identification, risk reduction, and risk assessment.

As stated before, safety is a property of the entire medical device and should be addressed at the system level. As this book is about management of the risk of medical devices, the focus of this chapter is on combination devices whose PMOA is device. For combination devices whose PMOA is drug, the pharmaceutical risk management takes the lead.

In many cases combination medical devices are a joint effort by a drug manufacturer and a device manufacturer. In such cases, the manufacturer of the drug and the device must do risk analyses of their components. The manufacturer who represents the PMOA (device or drug) would take on the responsibility for integrating the device and drug risk assessments to generate the Risk Management Report for the combination device.

When considering the risks of a combination device, we can classify the risks in three groups:

1. Risks as related to the drug alone. For example: formulation (strength, purity, potency, viscosity, etc.), Indication (disease, target patient), and sterility.
2. Risks as related to the device alone. For example: sterility, mechanical aspects (sharps; pinch points), and dose completion indication.
3. Risks due to interaction of device/drug. For example: dose accuracy, under/over dosing, and failed delivery (wrong target)

For combination medical devices that combine device, drug, or biologics, a good strategy is to first do analysis of risks for each aspect of the combination device, i.e., device part, drug part, and biologic part, and then analyze for the risks due to the interaction of the parts, such as drug with device. Then bring it all together in the RACT and determine the Overall Residual Risk.

Example hazards for combination devices: wear debris; particles; hazards due to device-drug interactions, e.g., chemical change of the drug, or malfunction of the device due to the drug.

CHAPTER 33

Basic Safety and Essential Performance

Abstract

Basic Safety and Essential Performance are key concepts in risk management of medical electrical devices. This chapter gives guidance on how to identify Basic Safety and Essential Performance, and how to distinguish them from each other.

Keywords: Basic Safety; Essential Performance; IEC 60601-1

IEC 60601-1 [7] is the Standard for non-implantable medical electrical equipment (ME). Ref. [7] defines two special terms:

- Basic Safety: "freedom from unacceptable risk directly caused by physical hazards when ME equipment is used under normal condition and single fault condition" [7] 3.10.
- Essential Performance: "performance of a clinical function, other than that related to Basic Safety, where loss or degradation beyond the limits specified by the manufacturer results in an unacceptable risk.

  NOTE Essential Performance is most easily understood by considering whether its absence or degradation would result in an unacceptable risk" [7] 3.27.

Understanding, and the ability to identify the Basic Safety and Essential Performance of your medical device is essential to your ability to demonstrate compliance to IEC 60601-1 [7].

33.1 HOW TO IDENTIFY BASIC SAFETY

Consider your medical device while it is not performing its clinical function. Analyze for all the relevant requirements of IEC 60601-1 [7] and determine if the device under normal, and single fault conditions could pose a Hazard. This is the basis of identification of Basic Safety of your device.

33.2 HOW TO IDENTIFY ESSENTIAL PERFORMANCE

Essential performance is about clinical functions of the device. Follow these steps:

a) Make a list of all your clinical functions.

b) Identify those functions whose failure or degradation could lead into a Harm. These are candidates for Essential Performance.

Safety Risk Management for Medical Devices
DOI: https://doi.org/10.1016/B978-0-323-85755-0.00033-3

c) Use the RACT to determine the risk levels for each candidate function from step (b). If the Residual Risk for a clinical function is unacceptable, then that clinical function is part of the Essential Performance of the device.

If in step (c) an Essential Performance is identified which is vulnerable to degradation, you should specify a degradation limit before which the risk is acceptable, and beyond which the risk becomes unacceptable.

Note that it is possible to have a medical device with no Essential Performance. What that means is that the device risks are controlled in such a way that the loss or degradation of any of its clinical functions do not result in unacceptable risk.

CHAPTER 34

Relationship between ISO 14971 and other Standards

Abstract

ISO 14971, the central Standard for medical device risk management, works in concert with many other related Standards. In this chapter we examine the relationships between ISO 14971 and IEC 60601-1, ISO 10993-1, IEC 62366, and ISO 14155. Each of these specialized Standards makes a normative reference to ISO 14971. As such, conformance to any of these specialized Standards requires conformance to ISO 14971.

Keywords: IEC 60601-1; ISO 10993-1; IEC 62366; ISO 14155

As mentioned in Chapter 6, a number of safety-related Standards rely on ISO 14971 [1] for determination of safety risks. In the following subsections, the relationships between ISO 14971 [1] and IEC 60601-1 [7], ISO 10993-1 [20], IEC 62366 [19], and ISO 14155 [18] are described.

34.1 INTERACTION WITH IEC 60601-1

IEC 60601-1 [7] is related to general requirements for basic safety and essential performance of Medical Electrical (ME) equipment, and is intended for the non-implantable MEs.

IEC 60601-1 [7] makes a normative reference to ISO 14971 [1] and expects the performance of risk management per ISO 14971 [1]. This means conformance to IEC 60601-1 [7] is not possible without conformance to ISO 14971 [1].

IEC 60601-1 [7] specifies certain requirements and acceptance criteria that facilitate the risk management process. For example, there are detailed requirements in IEC 60601-1 [7] for protection against electric shock. Test equipment, measurement methods, and pass criteria are provided in the Standard [7]. Therefore, if a medical device is compliant with IEC 60601-1 [7], it can claim that for instance, that the risk of electric shock from the device is acceptable.

In other cases, e.g., with respect to the safety of emitted ultrasound energy from a medical device, IEC 60601-1 [7] does not offer any means of testing for safety, or acceptance criteria. Instead, it defers to the risk management process per to ISO 14971 [1].

Safety Risk Management for Medical Devices
DOI: https://doi.org/10.1016/B978-0-323-85755-0.00034-5

In some cases, the determination of whether certain aspects of the medical device design are subject to IEC 60601-1 [7] is left up to the risk management process. For example, 'applied part' has a special meaning in [7]. It is the part of the device that comes into contact with the patient for the purpose of performing its clinical function. In some cases, a medical device may come into contact with the patient/user but not for the purpose of performing the device's clinical function. Such contact may be a source of Hazards. IEC 60601-1 [7] defers to ISO 14971 [17], the determination of how to treat the non-applied parts of the device that come into contact with the patient/user.

The concept of Essential Performance was defined in Section 4.1 and elaborated in Chapter 33. IEC 60601-1 [7] expects the manufacturer to identify the Essential Performance of the medical device. There are many specialized test houses who perform IEC 60601-1 [7] compliance-testing for manufacturers. As input to the test house, besides samples of the medical device, the test house expects the manufacturer to identify the Essential Performance of the device.

A point to keep in mind about using compliance with IEC 60601-1 [7] as the foundation of claim of risk acceptance, is that IEC 60601-1 [7] itself is not a Risk Control. The design features that enable passing the IEC 60601-1 [7] tests are the Risk Controls. Therefore, the 60601-1 [7] passing test results are the objective evidence that the Risk Controls are effective.

34.2 INTERACTION WITH ISO 10993-1

ISO 10993 is a series of Standards numbered ISO 10993-1 to ISO 10993-20. ISO 10993-1 [20] is about biological evaluation and testing of medical devices within a risk management process. ISO 10993-2 to ISO 10993-20 are each dedicated to a special aspect of biocompatibility. The aim of this series of Standards is the protection of humans from biological risks due to the use of medical devices.

The range of biological responses that are considered as adverse, i.e., Hazards, is quite broad and complex, and varies from person to person. They include: cytotoxicity, sensitization, irritation, hemocompatibility, pyrogenicity, carcinogenicity, and genotoxicity.

ISO 10993-1 [20] does not intend to provide a rigid battery of tests, including Pass/Fail criteria that can be used by a manufacturer to demonstrate biocompatibility. Instead, the standard offers guidance on ways of determining what testing is needed with the aim of achieving an acceptable level of risk for the Benefits that the medical device offers.

ISO 10993-1 [20] considers biological risk management as part of the overall process of management of safety risks to humans in accordance with ISO 14971 [1]. Conduct of biological evaluations serve to meet the requirements of both ISO 14971 [1], and ISO 10993-1 [20].

Execution of biological evaluations requires planning. The biological evaluation plan is a part of the overall Risk Management Plan. It is possible to combine the two plans under one cover. The biological evaluation plan must include arrangements for the identification, estimation, and evaluation of biological risks of the medical device. Additionally, the plan must include activities for the identification, review, and approval of: biological Risk Controls, residual biological risk, and disclosure of the residual biological risks.

One of the activities of biological Risk Analysis is the identification of biological hazards. This involves the consideration of the level of toxicity of utilized materials, and their route and duration of exposure. Sometimes the physical properties of materials play a role in the level of toxicity of the material. This includes factors such surface roughness, or porosity of the material. Chemical properties of materials can also introduce biological hazards. For example, dissimilar metals may create a galvanic, and corrosive process, which creates a biological Hazard.

As part of Hazard identification, potential contributors such as the choice of materials, additives, processing-aids, catalysts, etc. should be considered. Also, downstream processes, e.g., welding, sterilization, degradation materials, and packaging can introduce Hazards.

Characterization of the biological hazards of a device include identification of the type and duration of exposure to materials. For example, exposure to intact skin is very different from exposure to internal tissues such as blood or brain.

Risk Estimation requires knowledge of the probability of exposure to the toxicant and the potential Harm that could ensue. Probability of exposure can be derived from the availability of the toxicant and the Intended Use of the device. Severity is related to the biological dose-response in the exposed tissue and can be estimated based on published literature, or animal studies.

Risk Controls aim to reduce the potential risks. Some examples of Risk Controls are:

- Design changes to eliminate toxic materials from the design or manufacturing process
- Changes to physical/geometric properties
- Reduction of exposure time
- Avoidance of the more hazardous exposure routes

Biocompatibility can also guide the device risk management by contraindication of patients who could be more vulnerable. For example, a product may be adequately safe for adults, but not safe for infants.

Evaluation of the biological risks of a medical device is part of the Overall Residual Risk evaluation. Risk Evaluation requires knowledge of risk acceptance criteria. The criteria for risk acceptability are established in the Risk Management Plan, at the start of the design process.

Risk Controls must be verified for implementation and effectiveness. Verification of implementation can typically be achieved via the normal design verification testing. Biological evaluation could serve as verification of biological Risk-Control effectiveness.

A great service from biological evaluation to risk management is providing data, which allows for more accurate Risk Estimation, instead of simply assuming the worst-case outcomes. For example, biocompatibility could state that 2% of the patient population would potentially show an allergic reaction to the device materials. This number helps with P1 derivation.

Biocompatibility testing can be lengthy and expensive. A sound biocompatibility strategy can provide the justification to waive certain tests. This strategy could, for example, be based on toxicology information, or relevant prior use of materials. This is not only efficient, but also ethical. In some cases, it may be possible to reduce/eliminate animal testing by substituting chemical and in-vitro testing.

34.3 INTERACTION WITH IEC 62366

IEC 62366 [19] is the Usability Engineering Standard for medical devices. It is intended to minimize Use Errors with the primary focus of safety. It is understood that proper usability engineering of medical devices can control some, but not all Use Errors. The relationship between the usability engineering process and risk management process is illustrated in Ref. [19] Fig. A.5. Both processes are interested in characteristics of the medical device that are relevant to safety. Specifically, IEC 62366 [19] is focused on the user interface characteristics that are related to safety. Usability engineering evaluates the safety impact of Use Errors by evaluating the potential of the Use Errors for inducing Hazardous Situations.

There are two types of formal testing that are envisioned in IEC 62366 [19]: Formative, and Summative testing. Formative tests are performed iteratively during the design and development phase, with the intention to explore the effectiveness of the user-interface design and to identify potential Use Errors, or misuses. Formative tests typically do not have formal acceptance criteria. Their goal is to guide the design of the user interface and achieve a level of quality that ensures the summative tests will be successful. From the risk management perspective, the focus of formative testing is on reducing the likelihood of Use Errors that have the potential for creating Hazardous Situations.

Summative tests are performed at the end of user-interface development, after formative tests are completed. The objective of summative tests is to produce objective evidence that the user-interface contribution to safety risks is acceptable. For Use Errors that have the potential to cause serious Harm, e.g., Fatal, or Critical Harm, it is expected that all Summative test subjects complete the related tasks without Use Error, or sufficient justification be provided that all practical mitigations have been exercised to prevent Use Errors. For Use Errors that do not have the potential to cause serious Harm, quantitative acceptance criteria may be exercised, e.g., 95% of the test subjects complete the task within 5 minutes with no Use Errors. Summative tests can be utilized as a means of verification of effectiveness of Risk Controls.

Risk Management can inform Usability Engineering vis-à-vis decisions on the performance of summative tests. One such contribution is on the identification of user-interfaces that have, or do not have, an impact on safety. For safety-related user-interfaces, summative tests need to be performed. The choice of the number of participants in a summative test can be informed by Risk Management.

IEC TR 62366-2 [24] offers equation K.1 as:

$$R = 1 - (1 - P)^n$$

where

R is the cumulative probability of observing or detecting a usability problem,

P is the probability of a single test participant having a usability problem,

n is the number of test participants.

Given the risk acceptance criteria, and P2 numbers, the maximum probability of the Hazard, and thereby probability of use-failure, P, can be derived. Additionally, there can be a 'Company' policy that R, the probability of detecting a use-failure in a summative test must be, e.g., ≥90%. With these two pieces of information, the number of participants can be derived. For example: let's say that the max tolerable P is 10%, and R, per 'Company' policy is 90%. The number of participants, n computes to 22. You can also use table K.1 in Ref. [24] for the same purpose.

Another input from Risk Management to Usability Engineering is the indication of areas of the UI that are not safety-related, thereby enabling Usability Engineering to use expert reviews, rather than conduct new summative tests, for minor changes to those areas.

The contribution of Usability Engineering to Risk Management is both in the identification of Use Errors which could result in Hazards, and in the performance of summative studies which can serve as verification of effectiveness of Risk Controls.

34.4 INTERACTION WITH ISO 14155

ISO 14155 [18] is about clinical investigation of medical devices in human subjects. ISO 14155 [18] makes a normative reference to ISO 14971 [1] and requires that prior to the conduct of clinical investigations, the risks associated with the use of medical devices in clinical investigations be estimated according to ISO 14971 [1].

ISO 14155 [18] states that the terms: clinical investigation, clinical trial, and clinical study are synonymous. As such, these terms are used interchangeably herein.

In a clinical investigation, risks can be viewed over two horizons: pre-study, and post-study. Before the study, risk management per ISO 14971 [1] serves to identify the Hazards to the study participants, estimate the risks, control the risks, and do Benefit-Risk Analysis. In this capacity, risk management behaves as a predictive engineering technique. After the study has begun, risk management is reactive to Adverse Events and attempts to minimize any Harms to the study participants.

There is a bidirectional flow of information between risk management and clinical investigations. In fact, clinical investigations are a part of the risk management process.

See Section 30.7 for a description of information flow between risk management and clinical investigations.

CHAPTER 35

Risk Management Process Metrics

Abstract

Process metrics are interesting to many businesses, and the risk management process is no exception. But how does one measure the performance of a risk management process? Typically, evaluation of a process is done after the process has been in use for a while. In the case of risk management, it would be better to have advance knowledge of the goodness of the process to prevent potential injuries to patients. In this chapter three methods are offered for evaluation of the risk management process.

Keywords: Process metrics; risk management process

Process metrics are interesting to many businesses, and the risk management process is no exception. But how does one measure the performance of a risk management process?

If a project was successful, met its objectives, had no questions/findings from the Regulatory bodies, and the product is performing safely in the market, is that a sign that the risk management process was successful? Or was it just good luck? When everything goes smoothly people tend to believe they have a good risk management process and may not feel motivated to actually measure the goodness of the risk management process.

How do we go about measuring the effectiveness and success of a risk management process? What do we measure? How do we measure it? And, if we were able to measure 'it,' what is considered good, and what is bad? What are the criteria for goodness?

There is currently no consensus on how to measure the goodness of a risk management process. But in the subsections below, we offer three options for consideration.

35.1 COMPARISON WITH HISTORICAL PROJECTS

If a company has produced and commercialized a significant number of medical products, and has collected data about each product on how smoothly the product was approved, and whether it was the subject of any Field Safety Corrective Actions, then the company could potentially create a benchmark from a composite of the

DOI: https://doi.org/10.1016/B978-0-323-85755-0.00035-7

performance of the previous products. With this benchmark, the risk management process on a new product could be measured.

The problem with this method is that it is a lagging indicator. It can only indicate whether the risk management for a project met expectations, perhaps years after all is said and done.

35.2 ISSUE DETECTION HISTORY

Similar to the method in Section 35.1, this method relies on historical performance and collection of data. But this method can provide a leading indicator on the performance of a risk management process.

During the course of risk management processes, issues with potentially adverse safety-impacts are identified and mitigated. These are usually design-related issues which had gone unnoticed by the product development team. Assuming constant maturity and performance by the design team, one can presume and expect a certain rate of detection of safety issues. If the rate of issue detection on a new project is significantly lower than the historical levels, one could construe that the current risk management process is not working as well as the past projects.

The problem with this method is that team performance is not constant, project complexities are not the same, and safety issue identification can be subjective. So, the conclusions derived are just conjectures.

35.3 SUBJECTIVE EVALUATION

In this method people who are involved in the project and experienced with risk management evaluate the project on several vectors. For example:

- the productivity of the working sessions and how well they are run
- the sense of confidence in the ability to identify Hazards and estimate risks
- the contribution of the risk management process to a sense of communication among the participating functional groups
- how well risk management identifies safety-impact of proposed design changes

This method is also not precise but can provide real-time feedback to management. And even though it is subjective, it is not less valuable than the other two methods that are offered in this chapter.

CHAPTER 36

Risk Management and Product Development Process

Abstract

As technology advances, more sophisticated and more complex devices are produced to handle difficult medical conditions. Many of these devices employ hazardous and potentially lethal sources of energy such as gamma radiation and lasers, or dispense life supporting medicines into the patients. The rise in complexity of these medical devices brings about both increased benefits and increased safety risks. What safety strategies should a manufacturer adopt? How can risk management be a value-added activity to product development? Can risk management help identify Essential Design Outputs? This chapter explores answers to these questions.

Keywords: Safety strategy; essential design outputs; life cycle; product development; value-add

As technology advances, more sophisticated and more complex devices are produced to handle difficult medical conditions. Many of these devices employ hazardous and potentially lethal sources of energy such as gamma radiation and lasers, or dispense life supporting medicines into the patients. The rise in complexity of these medical devices brings about both increased Benefits, and increased safety risks.

The requirements of ISO 14971 [1] with respect to risk management apply to the entire life cycle of a medical device. This includes the product development part of the life cycle.

Considering product risks during the product development process, the safety features of the System can be developed as an integral part of the product development process and effectively integrated in the System architecture. This reduces the product development costs and can accelerate the product development schedule as well.

Activities such as safety characterization, and investigation of historic information about past performance of similar products give insights into the potential risks of the new device. With this knowledge, the system can be strategically architected for optimum safety and performance.

With advance consideration to safety, several characteristics should be considered in the design. For example:

- The safety aspects of the System should be as simple as possible, with clearly understandable design and operation.

Safety Risk Management for Medical Devices
DOI: https://doi.org/10.1016/B978-0-323-85755-0.00036-9

- Functionality of safety-critical parts of the System should be kept independent of the rest of the System, if possible.
- Interfaces to safety-critical parts of the System should be well-defined.

Most medical Systems today are complex. It is likely that some latent design flaws with the potential for unintended behaviors would remain in the design. It is advisable to create functional and design boundaries between the safety-critical parts of the System and the rest of the System and create firewalls to limit the impact of the latent design defects.

In the course of regulatory review of the medical device submissions, the device design, particularly the safety aspects of the design, becomes scrutinized. A well-architected System with clear and simple safety-subsystems would be more easily reviewed, with fewer questions, and gets approved more quickly.

36.1 IDENTIFICATION OF ESSENTIAL DESIGN OUTPUTS

CFR Title 20, Part 820.30 [58] states that "Design output procedures shall contain or make reference to acceptance criteria and shall ensure that those design outputs that are essential for the proper functioning of the device are identified."

It can be stated that Essential Design Outputs (EDO) are those design outputs, which are essential to the safety and efficacy of the medical device.

The term 'design output,' which is referenced in 21 CFR 820.30(d), can have different meanings. A design output is the result of design efforts at each phase, and also at the end of the total design effort. Therefore, there can be intermediate and final design outputs.

The FDA defines finished design output as the basis for the Device Master Record; and defines the total finished design output of the device, as the device itself plus its packaging, labeling, and the Device Master Record (DMR).

So, what are Essential Design Outputs? Why do they matter? And, once we identify them, what are we supposed to do about them? Let's answer each question in turn.

1. EDOs are element of the actual finished design output whose loss or degradation would have an adverse impact on the safety or proper functioning of the device. For example, a particular dimension on a part, or a component itself could be essential design outputs.
2. EDOs matter because they are essential for the 'proper functioning' of the device, meaning safe and effective functioning of the device.
3. Once EDOs are identified, certain policies should be exercised to provide higher confidence in the implementation and performance of those outputs. This could be in the form of increased process capability requirements, tighter QC inspections, etc.

So, what role does risk management play for EDOs? As stated above, EDOs are critical for the safe and effective functioning of the device. Risk management is concerned with safety and can assist the product design process in the identification of EDOs. Fig. 64 presents a strategy for the identification of EDOs from a safety perspective. This strategy is designed around the BXM method but can be adapted for other methods as well.

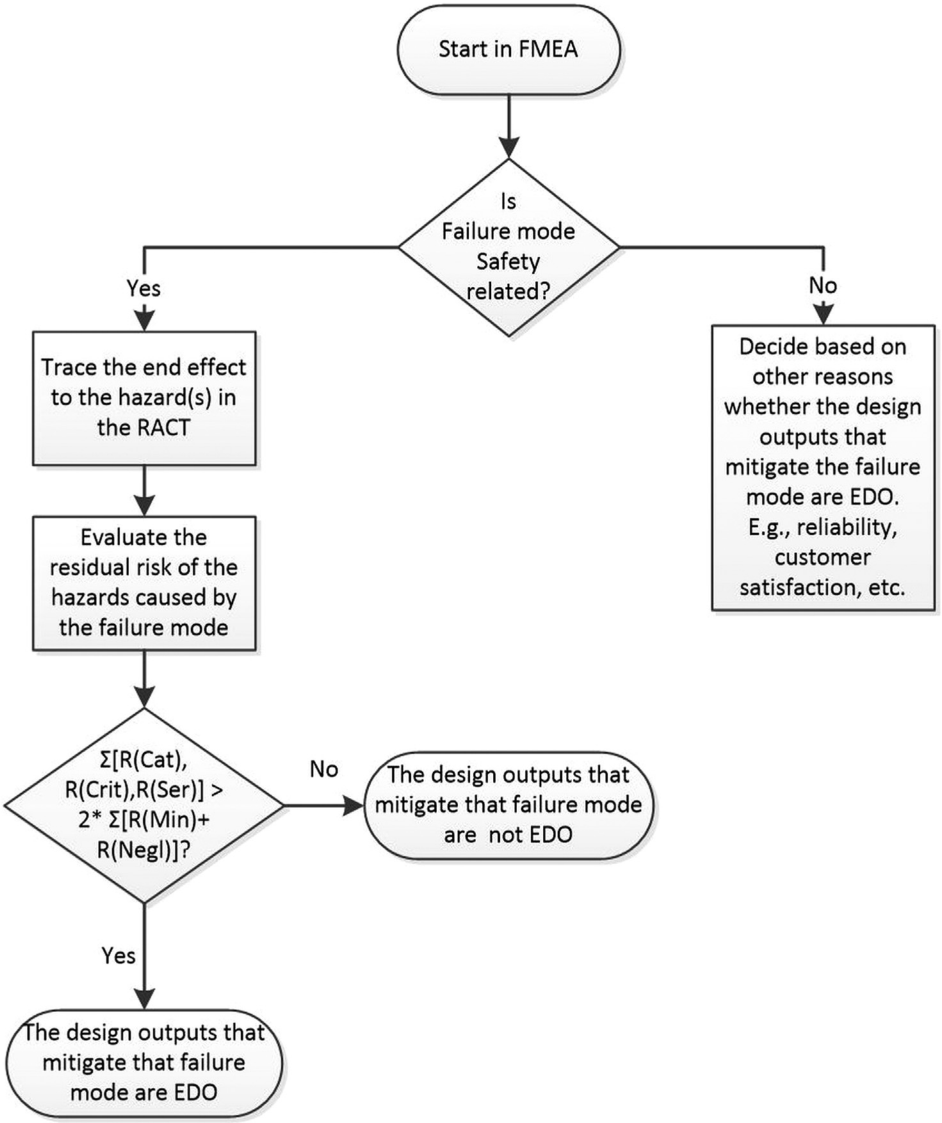

Start in FMEA
Is Failure mode Safety related?
Yes
No
Trace the end effect to the hazard(s) in the RACT
Decide based on other reasons whether the design outputs that mitigate the failure mode are EDO. E.g., reliability, customer satisfaction, etc.
Evaluate the residual risk of the hazards caused by the failure mode
Σ[R(Cat), R(Crit),R(Ser)] > 2* Σ[R(Min)+ R(Negl)]?
No
The design outputs that mitigate that failure mode are not EDO
Yes
The design outputs that mitigate that failure mode are EDO

Figure 64 Identification of Essential Design Outputs.

The core concept is the use of FMEAs to help with the identification of EDOs. Not every Failure Mode has a safety impact. For non-safety related Failure Modes, other reasons could drive the decision as to whether a design output is EDO. For instance, reliability or customer satisfaction could cause the manufacturer to declare a design output as EDO. If the Failure Mode does have a safety impact, then we need to know the amount of risk it could present to the patient/user. A safety-related Failure Mode is necessarily connected to one or more Hazards of the System. Use the RACT to determine the Residual Risk of the Hazard(s) that are the result of that Failure Mode. You should end up with five numbers, one for each Severity class of Harm. Sum the Residual Risk for the top three classes of Fatal, Critical, and Major. Also sum the Residual Risk for the bottom two Severity classes of Minor and Negligible. If the risks of the top three classes are more than twice the risks of the bottom two classes, then declare the design output as EDO. Of course, this is a suggested strategy, and you can adapt it to suit your QMS. The main point is to have a rationale and documented strategy.

Design outputs that achieve the Essential Performance of a medical device, as defined in IEC 60601-1 [7], can be considered to be part of the EDOs of a device.

36.2 LIFE CYCLE RELEVANCE OF RISK MANAGEMENT

Risk management is an activity that adds value to the product development life cycle. Companies who view risk management as a necessary evil, and a box that needs to be checked in order to get their product approved, miss out on the value that they could derive from risk management.

Fig. 65 displays a typical product life cycle. The blue triangles depict the risk management deliverable and their relative timing to the product life cycle. In the beginning,

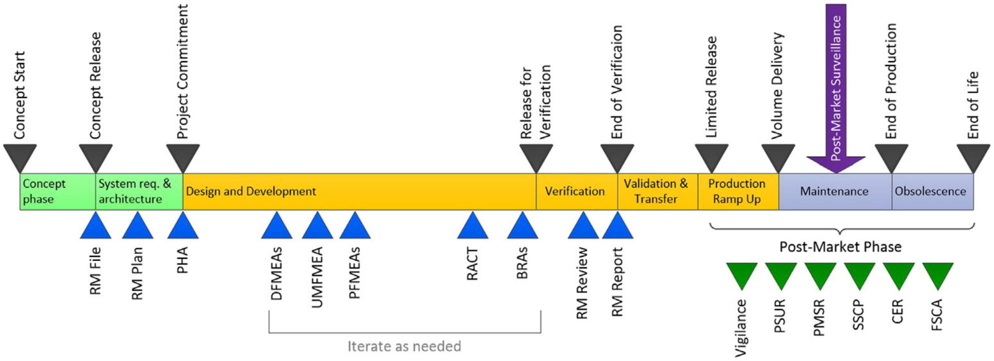


Figure 65 Risk Management and Product Life Cycle.

after the voice of customer is captured and the concept is released, the Risk Management File is formed, and a Risk Management Plan is written. In the meantime, product development produces the System requirements specification, and architecture. Based on these early work products, a preliminary Hazard analysis (PHA) is performed. The PHA provides valuable input to the product development:

1. It can serve as advisory to management on whether to commit to the project. If the PHA indicates that the risk of the product will outweigh its Benefits, management can stop the project before committing large amounts of resources to a project that would have to be canceled later.
2. If the product risks are estimated to be manageable, the PHA can identify the safety-critical aspects of the design so the product development team can enter the design phase with knowledge of where to focus their resources. This serves to reduce waste and optimize resource usage in product development.

After the approval of the project and commitment of resources, design and development begins in earnest. As designs of the product, the process, and the user interfaces become available, Failure Modes and effects analyses begin. The FMEAs provide feedback to the design team to improve the design. Another benefit that the risk management process offers to the product development team is the estimation of risk, which not only enables the teams to make risk-based sample size determination for verification testing, but also alerts the design team to potential problem areas. The sooner the design team knows about the problem areas, the less costly it is to fix them.

After risk assessment is completed, Benefit-Risk analyses are performed to provide evidence that the Benefits of the device outweigh its risks. This is a critical part of the regulatory submission, without which you cannot get approval for commercialization of your product.

After the release of the product, risk management continues to monitor the product in the Production and Post-Production phases. New knowledge gained about the product performance is fed back to the risk management process and evaluated for potential updates and/or improvements to the pre-launch risk estimates.

CHAPTER 37

Risk Management for Suppliers

Abstract

Most medical device manufacturers purchase parts and subassemblies from suppliers to build their products. Suppliers have an important contribution to medical device safety. This chapter discusses how to incorporate the supplier's risk management into the manufacturer's risk management of finished medical devices. Also certain advice is given for more successful interactions between manufacturers and suppliers.

Keywords: Supplier; supplier risk management; quality agreement

Most medical device manufacturers purchase parts and subassemblies from suppliers to build their products. The topic of risk management affects both the manufacturer of the finished medical device, and the suppliers to the manufacturers. From a regulatory perspective, it is the manufacturer of the finished medical device who makes the submission for approval and must demonstrate the safety and performance of the device. However, suppliers to the manufacturer also play a role in the safety of the medical device. In this chapter we address the topic of risk management from both perspectives of the supplier and the manufacturer with respect to product safety.

37.1 MANUFACTURER PERSPECTIVE

Supplied parts have a contribution to product safety. For instance, supplied parts could fail to perform as specified, or be off nominal-specs. The supplier might change materials or their manufacturing process without notifying the manufacturer. These all could impact the safety of the medical device. There are a number of actions that the manufacturer can take to safeguard the safety of the medical device with respect to supplied parts.

- **Supplier change-control** – the manufacturer should be apprised of changes to the design or manufacturing of the supplied parts. This includes changes to the raw ingredients that go into the supplied parts.
- **Quality inspections** – the supplied parts may be inspected at receiving inspection, or by mutual agreement via quality inspection at the supplier.
- **Quality agreement** – the manufacturer needs access to certain documents, such as the FMEAs of the supplied parts. Stipulation of such access in advance would prevent surprises during the interactions with the supplier.

DOI: https://doi.org/10.1016/B978-0-323-85755-0.00037-0

37.1.1 How to Incorporate Supplier Risk

In order to incorporate the safety risks due to supplied parts, the manufacturer needs to know the Failure Modes of the supplied parts, and any deviations from specifications of the supplied part. The Failure Modes of the supplied parts are the End Effects in the FMEAs of the supplied parts. Knowledge of deviations from specifications comes from the internal change-requests at the supplier. This knowledge is incorporated in the FMEAs of the finished medical device. For example, a sourced plastic casing may exhibit the Failure Mode of cracking at a particular spot. This knowledge from the supplier helps the manufacturer assess the safety impact of such failure. Or, the supplier may start using a new manufacturing process-aid that is toxic. Knowledge of this process-change would help the manufacturer assess the safety risk impact on the finished medical device. All of this knowledge from the supplier should be incorporated in the RACT for the finished medical device.

37.2 SUPPLIER PERSPECTIVE

Suppliers do not make submissions for the approval of the finished medical device. But they do have a contribution and a responsibility to the safety of the medical devices that incorporate their supplied parts. Since safety risk management is done at the system level, i.e., the level at which the patient/user interacts with the device, the suppliers of components cannot assess the medical device safety risks. That is the responsibility of the manufacturer of the finished medical device. An exception is when the supplier produces the finished medical device. In that case the supplier is able to assess the safety risks of the medical device.

The suppliers should perform FMEAs of their supplied parts to learn of the ways in which their supplied parts could fail to meet their requirements and specifications; what could cause such failures; and at what rate such failures could happen. This knowledge should be shared with the customer of the supplied parts.

The supplier might know how/where their supplied part would get used, or they might not know, e.g., in the case of generic parts, such as a screw. The supplier FMEAs estimate a criticality rating for their Failure Modes. One of the ingredients in the criticality estimation is Severity of the End Effect of the Failure Mode. The manufacturer of the finished medical device should inform the supplier of the Severity of the Failure Modes of the supplied parts, based on the role that the supplied part plays in the finished medical device. This knowledge would help the supplier properly rank the criticality of the Failure Modes of the supplied parts. The higher the criticality, the more efforts and resources should be used to mitigate a Failure Mode, e.g., by additional quality inspections, increased process capability, or testing. If a supplied part is used in many different contexts, the highest Severity ranking should be used in the supplier FMEAs. For instance, a supplied valve may be used in many applications. The Severity of the failure of the valve depends on the medical device in which it is used.

CHAPTER 38

Axioms

Abstract

Axioms are self-evident truths upon which we build our knowledge and analysis. In this chapter 10 axioms of risk management are offered. Reference to these axioms can help create clarity for the practitioner of risk management.

Keywords: Axioms; system safety; safety vs. reliability; risk controls

Below are 10 axioms of medical device risk management that would be useful to keep in mind:

1. Safety is not the mission, but a constraint
   Customers acquire medical devices for clinical Benefits, and expect safety
2. Hazardous Situations can arise even when there are no faults, i.e., under normal operational conditions
3. Safety is an emergent property of the System
   Knowledge of the safety of System components does not assure safety of the System
4. A Hazard cannot result in Harm until a sequence of events leads to a Hazardous Situation
5. Safety and reliability are not the same thing
   See Chapter 28 for more details
6. Severity is a qualifier for Harm…
   … not Cause, Hazard, nor Hazardous Situation
7. Death is not a Harm (in the jargon of risk management)
8. Risk Controls are targeted at risk reduction (severity | likelihood)
9. Software is never a Hazard; but can contribute to a Hazard
10. Highly reliable software is not necessarily safe

DOI: https://doi.org/10.1016/B978-0-323-85755-0.00038-2

CHAPTER 39

Special Topics

Abstract

In this chapter some special topics are covered that are not, per se, part of the risk management process, but are of interest to practitioners of medical risk management. Topics of personal liability, Cassandras, and creating a safety culture are discussed.

Keywords: Personal liability; complacency; Cassandras; creating a safety culture

In this chapter some special topics are covered that are not, per se, part of the risk management process, but are of interest to practitioners of medical device risk management.

39.1 THE CONUNDRUM

Human psychology tends to lead people to become myopic and lose sight of potential dangers, if there are no perceptible signs of danger. This is why most governments tend to react to disasters at a much higher cost, than prevent disasters at a lower cost.

Likewise, when risk management predicts high-risk of an adverse event, if there have not been any reported occurrences of the adverse event, people tend to think 'it hasn't happened before, therefore likely it will not happen in the future.' This kind of thinking diminishes the level of attention that high-risk events deserve.

Successful risk management can avert adverse events, and injuries – creating a sense of 'risklessness.' This may lead to a lack of appreciation by the outsiders, including management. A sense of complacency could set in, and attention and investment in risk management can diminish.

Sometimes even political motivations and aspiration can get involved. Careers tend to get advanced when a person steps up in a crisis and saves the day. It is thought that Winston Churchill said: "Never waste a good crisis." Heeding the advice of risk management to avert an unprecedented crisis could appear as a waste of money and resources on something that has not happened before. And if nothing happens, the precautionary actions are not given credit. On the other hand, ignoring the warnings from risk management and taking a chance could result in a crisis, which could create the opportunity for a 'hero' to step up and fight the fires. It doesn't matter whether the hero succeeds or not. Heroism will be rewarded.

Safety Risk Management for Medical Devices
DOI: https://doi.org/10.1016/B978-0-323-85755-0.00039-4

39.2 CASSANDRAS

Cassandra was a character in Greek mythology who could foresee future disasters but was cursed by the gods so that when she would warn people, no one would believe her. This is a term used to refer to people who warn of future disasters but are not believed.

Richard Clarke, the former counterterrorism adviser to US presidents Bill Clinton and George W. Bush, has written a book: "Warnings: Finding Cassandras to Stop Catastrophes" [59]. In this book, he talks about how Cassandras can/should be recognized, and how to benefit from their foresight while not being buffeted by too much fear.

In medical device risk management, we are required to analyze risks from both known and foreseeable Hazards. Cassandras tend to better see the foreseeable Hazards. The problem is that if something foreseen has never happened before, it may be difficult to persuade your organization to devote resources to it.

Clarke suggests not to be dismissive. Instead, take a surveillance and hedging strategy. What this means is to spend a small amount of resources and monitor the foreseen Hazard. Perhaps do some experimentation – investigate, research, and gather data. If the data supports the forecast, then devote more resources to mitigate the Hazard. Otherwise, you may be able to disprove the hypothesis. You don't have to make a final decision all at once. It can be taken in steps.

39.3 PERSONAL LIABILITY

Hiding safety-related defects or falsifying test results is illegal and carries serious legal consequences, including personal liability on the part of the perpetrators. For example, the Wall Street Journal published a story on August 9, 1996 that reported the conviction of three C.R. Bard executives for knowingly conspiring to hide potentially deadly flaws in a catheter model and selling devices that had not been approved by the FDA. They were sentenced to prison-time. In another example, The Telegraph published a story on December 10, 2013 about Jean-Claude Mas, the founder of PIP® breast implants, who was sentenced to 4 years in prison for the deliberate use of unapproved silicone gel in breast implants.

It should be noted that this does not mean that if a medical device causes injury, it is automatically concluded that people who were involved in the design and production of that device are criminally liable. It is understood that even if manufacturers follow sound practices for risk management and do all that they can to prevent injuries to people, some injuries are inevitable.

39.4 CREATING A SAFETY CULTURE

Culture is the lifeblood of a company. It is expressed in our mission, the ways we see ourselves, the values we hold, the ways we communicate and tell our stories, and our vision for the future. Culture helps us define who we are and to see ourselves in the context of the industry and the communities in which we work.

The culture of a company is important because it underpins the business decisions made. It establishes the implicit expectations that we have of ourselves, without the need to explain or defend the directions that we choose, when they are aligned with the company culture. For example, a company whose culture values creativity would be more receptive to radical ideas, than a company with a conservative culture.

A company who cares about producing safer medical devices, would be well-served to embrace and promote safety as part of its culture. As ISO 14971 [1] recognizes, top management plays an important role in creating a safety culture. Cultures are set by the top echelons of the company, who can imbue the culture with attitudes, beliefs, and values that extol safety.

What does a safety culture look like? What are the traits of a safety culture?

- Top management attitude is that patient/user safety is paramount in the business of the company.
- There is a sense of safety for the people in the organization that they will not be punished for identifying safety-risks of the products that the company produces.
- People have no doubt that patient/user safety is first, and everyone wants to help their team to mitigate safety risks.
- There is trust and confidence in the risk management process, perhaps underpinned by publicized metrics, such as the familiar "N accident-free days" signs in factories.
- Everyone has at least a basic understanding of risk management and how their individual work can affect product safety.
- There is cross-functional collaboration in the work of risk management.
- People operate based on knowledge of risk, and not based on fear and panic.

While declarations of the importance of safety by top management, and creation of safety policies are important, actions can breathe life into the words and policies. Some of the actions that management can take are:

- Offer training and resources to individuals.
- Praise the safety record of products.
- Hold people accountable, if it becomes clear that the negligence of individual (s) was the root cause of a safety issue.
- Lay out the cost of releasing unsafe products in terms re-work, recall, liability, consent decree. Management can create a sense of scale. For example, one recall means $X millions of lost revenue and goodwill, which translates to loss of bonuses/raises, and loss of Y number of jobs.

Top management can also create the opposite of safety culture. If leaders threaten to punish individuals for placing "too much" focus on safety, safety attitudes will be squashed. There are many examples of the power of top management on the culture of companies. Example: in 2015 the Japanese company Toshiba, nearly collapsed when it was found that Toshiba had been falsifying their financial records and overstating their operating profits by 151.8 billion yen ($1.23B) from 2008 to 2014. The reason for this was that top management set unrealistic financial objectives. Middle management didn't dare to object, and anxious not to disappoint the upper management pressured workers to falsify financial records. Another example was the Volkswagen diesel scandal, where the CEO Martin Winterkorn had set unrealistic sales goals that were not achievable. The pressure permeated layers of management until the engineers found that by a technical trick, they could cheat emission tests of diesel engines and make them appear to be cleaner-burning than they really were. With this trick they were able to sell more cars.

These stories sound egregious, and you may not even imagine it happening in your workplace. But these events did not happen overnight. There is a slow descent into the abyss. The American psychologist Diane Vaughan coined the term *Normalization of Deviance* to describe a process through which deviance from the correct behavior becomes normalized in a corporate culture. This shift happens slowly. Humans judge a circumstance by the measure of its variation from the previous state. A small variation, particularly if it doesn't result in an unacceptable outcome, becomes the new normal – after some incubation period. Imagine an unscrupulous employee who steals a small coin from the till, and nothing happens. In the first time or two, it feels uncomfortable. After a while, the small theft feels normal and comfortable. Then a slightly larger theft is tried. If nothing happens, that becomes the new normal, and so one. This may go on and the person may not get caught for a long time. By that time the person may be comfortably embezzling large amounts of money. When the news breaks and people hear of it for the first time, they would think this person is abnormal and such a behavior is unfathomable.

A positive ascent to a safety culture can follow the same gradual process. Step-by-step, with nurturing by management, the culture of a company could shift towards an established pattern of practices and attitudes toward safety.

39.5 PREDICTING THE FUTURE

While risk assessment may provide sufficient substantiation that a medical device is acceptably safe at the time of release, the safety status may not persist over time. The assumptions made may slowly drift and invalidate the bases of assertions of dominance of benefits over risks. Some examples:

- Risk controls degrade over time and their effectiveness diminishes.
- User interactions change over time, e.g., new clinical methods are conceived.
- Use-conditions change, e.g., infusion pumps made for use in clinics are sent home with patients.

39.5.1 How to Better Predict the Future

Risk management intends to predict the future in order to prevent/reduce safety risks. Below, some methods are suggested to help with better prediction of rises in risk.

Pay close attention to changes related to the device – changes to design, manufacturing process, maintenance, and use. Some changes are deliberate and planned, e.g., product design changes. But some changes are unplanned (by the manufacturer), e.g., a new, third party medical device is introduced to the market, which has an adverse interaction with the subject device.

Use PMS to confirm assumptions. Safety risks could rise if assumptions are incorrect initially, or become incorrect over time. Examples of assumptions to be monitored and confirmed:

- Failure rates of hardware.
- Users will receive, understand, and remember training.
- Handoffs will be done correctly, e.g., the maintenance person will leave the system in a safe state.
- UI risk controls will remain effective over time. Humans become desensitized to stimuli over time. A warning sign may evoke caution the first few times that it is seen. But after weeks and months, the user may not even notice its presence!

Explicitly document assumptions. This makes it easier to know what to monitor in PMS.

It is likely that the assumptions that underpin the design and manufacture of a medical device will be violated. Two strategies that would be wise to implement are:

1. Using PMS, detect and prevent changes that would violate the assumptions.
2. Build resilience in the system design such that if an assumption is violated and goes undetected, the system remains acceptably safe.

CHAPTER 40

Critical Thinking and Risk Management

Abstract

Critical thinking is an intellectually-disciplined process of receiving information and analyzing it accurately and objectively, free from bias. In this chapter several cognitive traps that can impact decision-making on system risks are discussed.

Keywords: Critical thinking; risk management; thinking errors; cognitive traps

Critical thinking is an intellectually-disciplined process of receiving information and analyzing it accurately and objectively, free from bias. It is easier said than done.

We all think. But without the discipline of critical thinking, much of our thinking is biased, distorted, and inaccurate. In our daily lives we make decisions, sometimes with dire consequences, based on mindless thinking. This book is not about critical thinking – that is a much larger subject. But in this chapter a few examples of critical thinking issues are provided just to make the reader aware of the potential impact of thinking errors on risk management.

Below some contributors to thinking errors are highlighted.

Incredulity – We often miss things if they don't fit our mental models and beliefs. Can you imagine a color that you have never seen before? It is not possible, because you need to first have a mental model of the color, before you can imagine it. If a phenomenon that you believe cannot happen happens, you would do everything possible to persuade yourself that it didn't happen. From doubting the data, to doubting your perception and analysis.

Super-focus – Consider a tester whose job it is to test a specific requirement. While observing the system for that one requirement, other events or things may manifest. If the tester is super-focused on the task, he/she could easily miss even major extraneous observations. An interesting experiment called the monkey business illustrates this. You can see a video by Daniel J. Simons on YouTube at this web address: https://youtu.be/IGQmdoK_ZfY. There is also a related book with the title "The Invisible Gorilla" [60].

Confirmation bias – if we believe something to be true, or perhaps want it to be true, we tend to seek/welcome information that confirms our belief and dismiss the information that refutes our belief. This is a regular occurrence in human existence.

Safety Risk Management for Medical Devices
DOI: https://doi.org/10.1016/B978-0-323-85755-0.00040-0

For example, you may have heard the saying 'love is blind,' which describes a person who is in love and can see no faults or flaws in their beloved. This is a manifestation of confirmation bias, where only the information that supports the goodness of the beloved is accepted, and the information to the contrary is rejected.

Confirmation bias appears in science and engineering as well. The paper "False-Positive Psychology" by Simmons et al. [61] talks about biased selection and processing of test results to support hypotheses. Simmons says, "flexibility in data collection, analysis, and reporting dramatically increases actual false-positive rates." This is what is also referred to as 'cherry picking.' Some researchers have, in the past, selectively presented only the data that supported their claims and discarded the data that refuted their claims. This is what gave rise to the replication crisis in the early 2010s, as many scientific studies were difficult or impossible to reproduce in subsequent investigations.

Confirmation bias is also a reason why when an outlier happens in test results, sometimes the tendency is to try to find a reason why the outlier should be discarded, instead of trying to find the root cause.

Anchoring bias – You may have experienced that sometimes if you are not previously very confident in your thought or opinion, hearing someone else's thoughts sways you to their side. This is called anchoring bias. It is when another thought or piece of information anchors your thoughts and biases you towards the anchor. Imagine if you were going to guess the number of jellybeans in a jar to be 300. But before you could say anything, a respected, smarter person says there are at least 1000 jellybeans in that jar. Could you see yourself changing your estimate to a higher number?

In working meetings, typically a few people tend to dominate and anchor the thoughts of the other team members. Usually, people with more authority or seniority have that power. Also, people with the loudest voices or those who are more self-assured or impassioned can anchor other people's thoughts.

Availability bias – When a thought or concept is more recent, or easier to remember, it is seen as more true, more probable, or more relevant. This is called the availability bias. For example, when a serious adverse event happens in the field, e.g., if a patient is seriously injured by a medical device, the whole engineering team and the management see that event as the highest risk that must be addressed. At the same time, it is possible that an even worse risk which has not happened yet, is lurking in the background.

Description-experience gap – When a person is faced with a decision about a new situation, their perception of risk based on the description of the situation is higher than after they have gained experience with the situation. Take for example, skydiving. A person who has never skydived feels a high degree of risk before the first jump. After several successful jumps the same person will feel that skydiving is not so risky.

Comparison with the past –

1. We tend to judge a new situation by simile to the past, even when the past event is not a good simile. For example, having been bitten by a vicious dog, might make a person afraid of all dogs.
2. When we rely on the most similar past experience, we often have a small sample to compare with. For instance, one significant loss in a stock transaction may sour you on stock trading altogether.

The above examples of cognitive traps are some of the many ways that our minds can be led to make poor decisions. With respect to risk management, we need to be vigilant so that we do not miss Hazards, make good estimates of the risks, and make the best design decisions to reduce the risks of medical devices. In your daily work, be mindful of cognitive biases that we all have, and try to be objective in considering and evaluating your own thoughts as well as the thoughts of others.

CHAPTER 41

Advice and Wisdom

Abstract

Mastery of the engineering and mathematics of risk management is not sufficient for success. Certain additional knowledge and experience helps propel the practitioner to success. In the closing chapter, advice and wisdom from 28+ years of experience in doing risk management in the medical device industry are presented as a complement to the knowledge that is presented in the rest of the chapters.

Keywords: Advice; wisdom

In closing, here is some advice and wisdom gathered over 28 years of medical device industry experience:

- System safety should never be looked at as a cost or a liability, but as a means for reducing program cost, schedule-risk, legal liability, and increased customer satisfaction.
- Team dynamics — how well the team members communicate, and whether there is a prevailing safety culture have an impact on the design and safety of the product.
- Product developers' minds are focused on how to make a product work. Reliability engineers and risk managers' minds are focused on how a product could fail.
- Discovery of a design flaw that could lead to a Hazard, could create an emotional reaction in the design engineers as a personal offense. Be sensitive and mindful of this possibility and couch your discoveries as opportunities for design improvement towards the shared goal of preserving patient/user safety.
- Team continuity throughout the product life cycle has an impact on product safety. It is possible that the original design team implemented certain safety features that were not well-documented. Then during the maintenance part of the life cycle, the continuation-engineering team may remove a safety feature due to lack of understanding of the rationale for the existence of that feature.
- Make the Risk Management File available to all team members. Access to this information helps the product development team make better decisions during the design and development phase.

DOI: https://doi.org/10.1016/B978-0-323-85755-0.00041-2

- Write well! An easy to read and understand RMR will go a long way to build confidence and trust in a regulatory reviewer. Your colleagues will also appreciate well-written documents that are easy to understand and review.
- While conformance to ISO 14971 [1] offers a reasonable assurance of safety of the device, it does not mean the device will not cause Harm.
- Risk management is a living and an ongoing process for as long as the medical device is in the field.
- Include in the RMP that a person with relevant medical knowledge will review and approve documents that evaluate Harms or risks of Harms, e.g., HAL, RACT, BRA.
- Good traceability is an invaluable tool for both change-impact analysis, and determination of whether a detected field issue has a safety impact or not.
- When doing UMFMEA, include people in the team who have clinical knowledge, such as doctors, nurses, or field clinical engineers who spend time in the clinics/operating rooms and know how the product actually gets used.
- Near misses or close calls should not be dismissed. They are gifts – a warning without any harm. Learn from them as if they were real events.
- It is important to maintain consistency among the risk management artifacts and the design. As designs iterate, a robust change-control and configuration-management system helps ensure that the risk management documents remain consistent with the actual design of the medical device.
- Risk management produces large documents that are not easy to review. When asking people to review risk management documents, make it easier for them by limiting the scope of their review – make specific requests of them, e.g., ask the medical/clinical person to review the document from the medical safety perspective, while the mechanical engineer would evaluate the mechanical aspects in the document.
- Risk management is a collaborative endeavor. In addition to engaging the normal functions of R&D, manufacturing, Clinical, etc., engaging the Intended User can provide a unique perspective and may identify risks that relate to their expected use of the product in their actual environments.
- Even though the BXM method deploys a numerical method which lends itself to mathematical computations, one should not be lulled into thinking that the output of the analysis is the absolute truth. Remember that the input to the math is still an estimation. But it is better to make many small estimates and mathematically aggregate them, than to just make one big overall estimate. This

is similar to estimating the annual budget of a company. The CFO doesn't just pull a number out of thin air. He/she asks people at all levels to make estimates for their budgets. Then these small estimates are gradually aggregated until the entire company budget is determined.

- Observe patterns and derive predictive analytics. Example: the town of East Orange, New Jersey police dept. used CCTV cameras and learned that the prevailing pattern prior to a car theft was gathering of 5+ people around 8 p.m. in the streets. Solution: when they saw this pattern on CCTV cameras, they would send a police car to drive by. Car thefts dropped significantly! What can you learn? What patterns have been present before field-safety events? Can you think of preemptive actions to avoid field-safety events?
- It is important to cultivate and encourage humility in self and others. The absence of humility can lead to unjustified certitude or hubris. This is when the spirit of inquiry stops and can lead to errors in risk management.
- Cultivate and encourage imagination.

Contents

Academic Press is an imprint of Elsevier
125 London Wall, London EC2Y 5AS, United Kingdom
525 B Street, Suite 1650, San Diego, CA 92101, United States
50 Hampshire Street, 5th Floor, Cambridge, MA 02139, United States
The Boulevard, Langford Lane, Kidlington, Oxford OX5 1GB, United Kingdom

Notices
Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods, professional practices, or medical treatment may become necessary.

Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information, methods, compounds, or experiments described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data
A catalog record for this book is available from the Library of Congress

ISBN: 978-0-323-85755-0

For Information on all Academic Press publications
visit our website at https://www.elsevier.com/books-and-journals

Publisher: Mara Conner
Acquisitions Editor: Carrie Bolger
Editorial Project Manager: Gabriela Capille
Production Project Manager: Poulouse Joseph
Cover Designer: Matthew Limbert

Typeset by MPS Limited, Chennai, India

Dedication

This book is dedicated to all the people of this planet who suffer from illness and who look to medical technology with hope and trust.

EXPERIMENTAL CHARACTERISATION OF SELF-HEALING IN RECONSTITUTED BOOM CLAY

TOPIC 04: Hydro-mechanical properties

B. Chandan Malagar [1], P. Vardon [1], A.C. Dieudonné [1].
[1]*Delft University Of Technology - Delft (Netherlands)*

Abstract

Disposal of radioactive waste in deep and stable geological formations is considered a feasible approach to isolate these wastes from anthropogenic activities and the environment over a long time period. Argillaceous formations are proposed as one of the suitable host rocks for such infrastructure thanks to their low permeability, high sorption capacity and propensity to plastic rather than brittle deformation. As a result of tunnel excavation, the host rock will experience significant stress redistribution, leading to local failure of the material, the creation of excavation damage zone and a local increase of the host rock permeability. Nevertheless, laboratory and field experiments have shown that these fractures disappear or seal naturally with time (Meier et al., 2000, Bastiaens et al., 2007, Zhang, 2013). This specific behaviour has been attributed to the high plasticity and swelling of clay minerals (hydraulic) and increase in mean stress (mechanical) after the closure of facilities. Studies focusing on sealing of fractures have generally quantified these characteristics in terms of decrease in hydraulic conductivity and increase in fracture volume when it interacts with water. (De La Vaissière et al., 2014, Auvray et al., 2015). However, limited quantitative information is available on mechanical properties of self-healed fractures in preferred host rocks. Therefore, this work focuses on evaluating the recovery of strength along a discontinuity in reconstituted Boom Clay samples under different normal stresses. Normal stress is a crucial parameter affecting shear strength within continuums and the effective contact area between two surfaces of a discontinuity. This work investigates the amount of self-healing in reconstituted Boom Clay under variable normal stresses and testing conditions (direct shear and rotary shear conditions). Further, it aims at supporting the development of models for the post-closure strength recovery of host rock for radioactive waste repositories.

References

Auvray, C., Morlot, C., Fourreau, E., & Talandier, J. (2015). X-RAY TOMOGRAPHY APPLIED TO SELF-HEALING EXPERIMENTS ON ARGILLITES. 13th International Congress of Rock Mechanics, May, 1–12.

Bastiaens, W., Bernier, F., & Li, X. L. (2007). SELFRAC: Experiments and conclusions on fracturing, self-healing and self-sealing processes in clays. Physics and Chemistry of the Earth, 32(8–14), 600–615.

https://doi.org/10.1016/j.pce.2006.04.026

De La Vaissière, R., Armand, G., & Talandier, J. (2014). Excavation damaged zone under imbibition: Evidence of self-sealing into claystone. Unsaturated Soils: Research and Applications - Proceedings of the 6th International Conference on Unsaturated Soils, UNSAT 2014, 2(May 2019), 1481–1487. https://doi.org/10.1201/b17034-216

Meier, P. M., Trick, T., Blümling, P., Vockaert, G., Parc, A., Croix, D., & Monnet, J. (2000). SELF-HEALING OF FRACTURES WITHIN THE EDZ AT THE MT . TERRI ROCK LABORATORY : RESULTS AFTER ONE YEAR OF EXPERIMENTAL WORK. Proceedings of International Workshop on Geomechanics, Hydromechanical and Thermohydro-Mechanical Behaviour of Deep Argillaceous Rocks: Theory and Experiment, 1, 267–274.

Zhang, C. L. (2013). Sealing of fractures in claystone. Journal of Rock Mechanics and Geotechnical Engineering, 5(3), 214–220. https://doi.org/10.1016/j.jrmge.2013.04.001

Index

List of figures

List of tables

Preface

A painting is never finished – it simply stops in interesting places.

Paul Gardner, artist

This book is written to serve both the professionals in the Medical Technology (MedTech) industry as well as the students in universities. The book delivers not only the theory but also offers practical guidance on how to apply the theory in your day-to-day work. The objective of this book is to demystify risk management and provide clarity of thought and confidence to the practitioners of risk management as they do their work.

I offer here the result of more than 30 years of experience in risk management, beginning with my work in aerospace, on the Space Shuttle at NASA and continuing in the medical device industry. What is presented in this book is the best available knowledge today. But as in any scientific or technical endeavor, the methods and techniques in risk management will continue to evolve, mature, and improve.

Disclaimer – The opinions and materials presented in this book are mine and do not necessarily represent the views of Medtronic.

Bijan Elahi

References

[1] ISO 14971:2019, Medical devices—Application of risk management to medical devices.

[2] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC.

[3] Council Directive 93/42/EEC—Medical Device Directive (MDD).

[4] Council Directive 90/385/EEC—Active Implantable Medical Device Directive (AIMDD).

[5] Official Journal of the European Union.

[6] MDCG2021-5, Medical Device Coordination Group document, April 2021.

[7] IEC 60601-1 Edition 3.1, Medical electrical equipment—Part 1: General requirements for basic safety and essential performance.

[8] ISO/IEC Guide 63, *Guide to the development and inclusion of aspects of safety in international standards for medical devices*, third ed., 2019.

[9] Guide 51, Safety aspects—Guidelines for their inclusion in standards, third ed., 2014.

[10] IEC 62304:2015, Medical device software—Software life-cycle processes.

[11] MDCG 2020-6, *Regulation (EU) 2017/745: Clinical evidence needed for medical devices previously CE marked under Directives 93/42/EEC or 90/385/EEC*, April 2020.

[12] P.L. Bernstein, Against the Gods: The Remarkable Story of Risk, Wiley, 1998.

[13] A. Willet, The Economic Theory of Risk and Insurance, University of Pennsylvania Press, Philadelphia, PA, 1901.

[14] N.G. Leveson, Engineering a Safer World, MIT Press, 2012.

[15] ISO/TR 24971:2020, Medical devices—Guidance on the application of ISO 1491.

[16] M. Lewis, The Undoing Project, Norton, 2017.

[17] ISO 14971:2007, Medical devices—Application of risk management to medical devices.

[18] ISO 14155, Clinical investigation of medical devices for human subjects—Good clinical practice, third ed., 2020.

[19] IEC 62366-1:2020 Edition 1.1, Medical devices, Part 1: Application of usability engineering to medical devices.

[20] ISO 10993-1:2018, Biological evaluation of medical devices—Part 1: Evaluation and testing within a risk management process.

[21] EN ISO 14971:2012, Medical devices—Application of risk management to medical devices.

[22] REGULATION (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU.

[23] EN ISO 13485:2016, Medical devices—Quality management systems—Requirements for regulatory purposes.

[24] IEC TR 62366-2:2016, Medical devices—Part 2: Guidance on the application of usability engineering to medical devices.

[25] FDA, Guidance on applying human factors and usability engineering to medical devices, February 3, 2016.

[26] IEC 60601-1-8:2006, Medical electrical equipment—Part 1–8: General requirements for basic safety and essential performance—Collateral Standard: General requirements, tests and guidance for alarm systems in medical electrical equipment and medical electrical systems.

[27] ANSI/AAMI HE 75:2009/ (R) 2013, Human factors engineering—Design of medical devices.

[28] FDA, Guidance on postmarket management of cybersecurity in medical devices, December 28, 2016.

[29] M. Bordwin, Factoring the Law into Medical Device Design, MDDI, March 2005.

[30] FDA, MAUDE database, Manufacturer and user facility device experience. www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfMAUDE/search.CFM

[31] Eudamed, European database on medical devices.
[32] J. Surowiecki, *The Wisdom of Crowds*, Anchor, 2005.
[33] NASA, Fault Tree Handbook with Aerospace Applications; Ver 1.1, August 2002.
[34] NUREG-0492, *Fault Tree Handbook*, 1981.
[35] AIAG & VDA FMEA Handbook, first ed., 2019.
[36] C. Carlson, *Effective FMEAs*, Wiley, 2012.
[37] IEC 62366:2007, Medical devices—Application of usability engineering to medical devices.
[38] IMDRF SaMD WG N10.
[39] IEC TR 80002-1, Technical Report, Medical device software—Part 1: Guidance on the application of ISO 14971 to medical device software, Edition 1.0 2009-09.
[40] FDA, Guidance for the content of premarket submissions for software contained in medical devices, 2005.
[41] G.J. Holzmann, The Power of Ten—Rules for Developing Safety Critical Code, NASA/JPL Laboratory for Reliable Software, Pasadena, CA, 2006.
[42] FDA, Guidance on medical device patient labeling, April 19, 2001.
[43] Notified Bodies Recommendation Group, Consensus Paper for the Interpretation and Application of Annexes Z in EN ISO 14971:2012; Version 1.1, October 13, 2014.
[44] FDA, Factors to consider when making benefit-risk determinations in medical device premarket approval and de novo classifications, August 30, 2019.
[45] P. Slovic, E. Peters, *Risk perception and affect*, Current Directions in Psychological Science 15 (6) (2006).
[46] FDA, Benefit-risk factors to consider when determining substantial equivalence in premarket notifications [510(k)] with different technological characteristics, September 25, 2018.
[47] FDA, Factors to consider when making benefit-risk determinations for medical device investigational device exemptions (IDEs), January 13, 2017.
[48] MEDDEV 2.7/1, Clinical evaluation: A guide for manufacturers and notified bodies under directives 93/42/EEC and 90/385/EEC. Revision 4, 2016.
[49] MDCG 2020-7, *Post-market clinical follow-up (PMCF) Plan Template. A guide for manufacturers and notified bodies.*
[50] MDCG 2020-8, *Post-market clinical follow-up (PMCF) Evaluation Report Template. A guide for manufacturers and notified bodies.*
[51] J. Rodriguez-Perez, *Handbook of Investigation and Effective CAPA Systems*, second ed., ASQ Quality Press, 2016.
[52] MEDDEV 2.12-1, rev 8, *Guidelines on a medical devices vigilance system*, January 2013.
[53] MDCG 2019-9, *Summary of safety and clinical performance. A guide for manufacturers and notified bodies*, August 2019.
[54] MDCG 2020-13, *Clinical evaluation assessment report template*, July 2020.
[55] FDA Guidance, Medical device tracking, March 27, 2014.
[56] ISO/TR 14969, First edition: 2004-10-15, Medical devices—Quality management systems—Guidance on the application of ISO 13485:2003.
[57] ICH Q9, International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use, Quality Risk Management Q9, 2005.
[58] Code of Federal Regulations, Title 21, Part 820.30.
[59] R.A. Clark, R.P. Eddy, Warnings: Finding Cassandras to Stop Catastrophes, 2017.
[60] C. Chabris, D. Simons, The Invisible Gorilla, Broadway Paperback, 2009.
[61] J.P. Simmons, L.D. Nelson, U. Simonsohn, False-Positive Psychology, *Psychological Science*, 22 (11):1359−66, 2011.

Safety Risk Management for Medical Devices

Safety Risk Management for Medical Devices

Second Edition

BIJAN ELAHI

ELSEVIER

ACADEMIC PRESS
An imprint of Elsevier