What safety models and principles can be adapted and used in security science?

Reniers, Genserik; Landucci, Gabriele; Khakzad, Nima

DOI
10.1016/j.jlp.2020.104068

Publication date
2020

Document Version
Final published version

Published in
Journal of Loss Prevention in the Process Industries

Journal of Loss Prevention in the Process Industries 64 (2020) 104068

Contents lists available at ScienceDirect

Journal of Loss Prevention in the Process Industries

journal homepage: http://www.elsevier.com/locate/jlp

What safety models and principles can be adapted and used in security science?

Genserik Reniers [a,b,*], Gabriele Landucci [c], Nima Khakzad [d]

[a] Safety and Security Science Group, Faculty of Technology, Policy, and Management, Delft University of Technology, Delft, the Netherlands
[b] Faculty of Economics and Organizational Sciences, Campus Brussels, KULeuven, Brussels, Belgium
[c] Department of Civil and Industrial Engineering, University of Pisa, Pisa, Italy
[d] School of Occupational and Public Health, Ryerson University, Toronto, Canada

ARTICLE INFO

Keywords:
Security models
Security principles
Security management
Learning from safety

ABSTRACT

Engineering risk management is comprised of managing operational safety risks on the one hand and managing physical security risks on the other. Although some basic management principles are obviously the same for both safety and security, some important conceptual and calculation differences exist, as is explained in this paper. For instance, safety risk is usually calculated based on the scenarios' consequences and likelihoods, while security needs to be determined by the assessment of vulnerability, the likelihood of attack and potential consequences. Nonetheless, there are also many similarities. Conceptual models, metaphors and principles that have been elaborated in the safety domain during the past century, many of them based on major accidents and their investigation, can easily be translated to the security domain. In the present study, we will explain how physical security should be seen in relation to safety, and what models and principles, derived from safety science, can be employed to manage the security aspects associated with physical threats.

1. Introduction

Security science is a relatively young field of science, and it can learn a lot from the research that has been carried out in safety science. Over the past decades, a lot of safety theories, concepts, metaphors and management models have been suggested by safety scientists and accident investigators. The models have thus been built after decades of experience and research, within a variety of academic disciplines, and encompassing diverse industrial sectors. Therefore, it is no surprise that the models used to deal with safety risks are very diverse, and that incidents and accidents were a driver and an inspiration for the builders of the models. Hereafter, a number of these theories and models will be discussed for security.

Achieving an adequate security level in an organization starts with adequate security management. It should be noted that many organizations already follow the management plan-do-check-act loop because of their acquired know-how of internationally accepted standards, e.g., ISO 9001, ISO 14001, ISO45001, or/and ISO 31000, continuously improving performance concerning risks. Hence, some degree of basic standardization for operational risk management already exists in many organizations and thorough documented and well-implemented risk management systems are available.

A security risk management system (SRMS), as part of the risk management system, should aim to ensure the various security risks posed by operating the facility are always below predefined and generally accepted company security risk levels. Effective management procedures adopt a systematic and proactive approach to the evaluation and management of the security risks of the plant, including its products and its human resources.

In brief, arrangements need to be made to guarantee that the means provided for a secured operation of the industrial activity are properly designed, set up, tested, operated, inspected and maintained and that persons working on the site (contractors included) are properly instructed on security requirements and features/policies.

Four indispensable features for establishing an organizational SRMS are:

- The parties involved;
- The policy – objectives;
- The list of actions to be taken;
- Implementation of the system.

* Corresponding author. Faculty of Economics and organizational sciences, Campus Brussels, KULeuven, Brussels, Belgium.
E-mail address: G.L.L.M.E.Reniers@tudelft.nl (G. Reniers).

https://doi.org/10.1016/j.jlp.2020.104068
Received 13 September 2019; Received in revised form 1 February 2020; Accepted 1 February 2020
Available online 3 February 2020

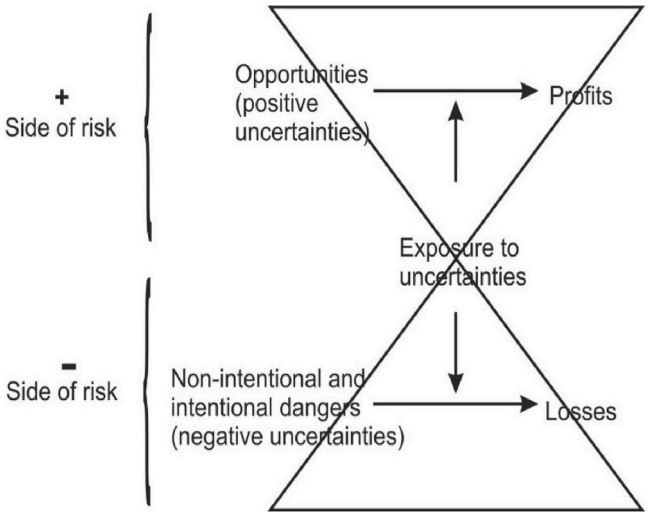


Fig. 1. Risk sandglass. Adapted from (Meyer and Genserik, 2016).

The essence of security protection practices consists of security data, threats and vulnerabilities reviews, security procedures and awareness training. These elements need to be integrated into a security management document that is implemented in the organization on an on-going basis (Meyer and Genserik, 2016).

SRMSs are indeed a must for organizations to handle security risks at an operational level. SRMSs deal with assessing all the security risks and treating them, that is, trying to prevent the events associated with them, and, in the case of an unfortunate event happening despite all measures taken, trying to mitigate the consequences.

To develop a solid and effective SRMS, physical security risk managers can make use of experience and knowledge that has been developed and built up in safety science. In the present study, some models and principles that have been worked out by safety scientists over the past century will be discussed in the light of security science.

Dealing with security risks is actually a part of managing operational risks, and thus, security management can be situated within the field of 'engineering risk management'. Obviously, other risks such as financial risks, quality risks, environmental risks, ethical risks, and health risks are all risks that need to be controlled and managed within this field. Before diving into the similarities and differences between managing safety risks and managing security risks, the concept of 'risk' should be defined.

International guidelines can be employed to obtain a better understanding of the concept of risk. According to ISO 31000 (ISO-International standardization organization, 2009), the umbrella 'Risk Management' Guideline by the International Standardization Organization, 'risk' can be defined as "the effect of uncertainty on objectives". This is a very broad definition of risk, indicating that without objectives (or aims) or without uncertainties, risk does not exist, and that both making profits and incurring losses are intrinsically linked to the risk concept.

In other words, risk features an "upside" potential, associated with the positive outcome and opportunity to make profits by carrying out certain activities (i.e., "taking risks"). At the same time, there is a "downside" potential given the potential negative outcomes and losses that can be suffered due to carrying out these activities (i.e., "risking").

If only looking at the downside potential of risk, a number of different definitions of the risk concept exists and some examples (out of a large list) are: "risk is the likelihood that a loss will occur", "risk is the probability that a hazard will be transformed into damage or loss", or "risk is the possibility that positive expectations will not be realized". These are all definitions describing risk in a negative way. However, as mentioned above, the most recent scientific insights indicate that risk

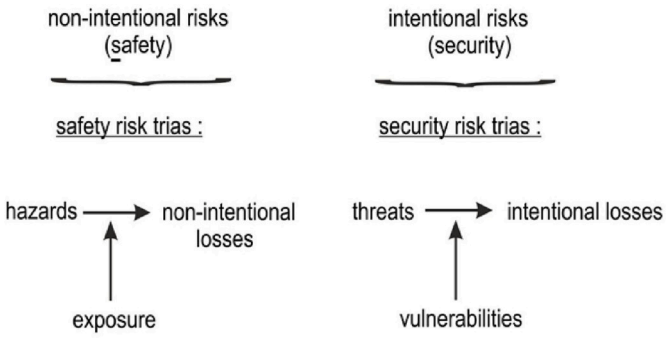


Fig. 2. Analogy between safety risk and security risk.

should be viewed as a coin with two sides, where one side does not exist without the other side. It depends on the observer which side he wants to tackle (or both sides, preferably). The two sides can be represented by using the risk sandglass. The risk sandglass is a metaphor making the two sides of risk obvious. On the positive side there are the opportunities (positive uncertainties) that may lead to profits if you are exposed to them, while on the negative side dangers exist (negative uncertainties) that may lead to losses given exposure.

The negative triangle, at the bottom of Fig. 1, is the so-called 'risk trias' ('trias' is Latin and means triangle) composed of dangers, exposure, and losses. If the dangers are called 'hazards', we talk about the 'safety risk trias'. This terminology is used by safety management, however, the term 'hazard' does not hold in the case of security risk management; thus, a specific terminology is needed, which will form the 'security risk trias'.

From the above, it can be seen that safety and security are entangled, the only difference being the human intention of causing the losses. This difference translates into the description of the two concepts and the resulting approaches, and also the way the risk is managed and treated with regard to each concept. For non-intentional risks (safety) three issues need to be determined and dealt with: hazards, exposures to hazards, and possible losses. In the case of intentional risks (security), an analogy can be made: threats, vulnerabilities towards the threats, and potential losses. Together, the three latter terms form the so-called 'security risk trias' (Fig. 2).

The existing risk assessment techniques for non-intentional risks (for instance Hazop, What-if analysis, Fault Tree Analysis, the bow-tie method, and many others (CCPS - Center of Chemical Process Safety, 2000)) are designed to identify as many hazards as possible, all thinkable exposures to these hazards, and considering as many loss scenarios as realistically feasible due to the combinations of hazards and exposures. Afterwards, safety investment decisions can be made based on the known safety risks. Remark that violations can be seen as "intentional hazards" and as such are part of the safety domain. They cannot be regarded as 'threats' which may result in intentional losses. The intention of a violation is to increase production or to gain time, not to deliberately cause losses. Hence, violations are no part of security.

For the case of intentional risks, there is an analogy: security risk assessments should determine as many threats as possible, identify the vulnerabilities through which the threats may be exploited, and take into account as many potential consequence scenarios as deemed realistic. When the threats, vulnerabilities and possible intentional losses are known, adequate security control and management measures can be taken. Indeed, if these are known, measures can be thought of to decrease or eliminate these factors, since:

- no/decreased threats = no/decreased security risks,
- no/decreased vulnerabilities = no/decreased security risks,
- no/decreased intentional losses = no/decreased security risks.

If we know *all* threats, *all* vulnerabilities, and *all* possible

Fig. 3. Physical security risk management set. Adapted from (Meyer and Genserik, 2016).

intentionally caused losses (which in reality is evidently not possible), we could really make optimal decisions with respect to decreasing or eliminating security risks. This is actually not as straightforward as it seems at first sight.

Furthermore, analogous to safety, a distinction should be made between two types of security risks:

- Type I: small/regular security risks,
- Type II: disastrous security risks

Remark that black swan security risks (Paté-Cornell, 2012) can be seen as an extremum of type II risks. Type I security risks regularly occur on a daily basis and feature high likelihood and a small impact. These risks concern typically well-known and (relatively) low-level security matters such as theft, manslaughter and murder. Type II risks are rare but occur regularly on a global scale, and usually have a rather high to a very high impact (even on a societal level). A typical example of a type II security risk is a terrorist attack. Black swan risks are those that have never occurred before (unprecedented) and can only be imagined with the fantasy of the mind. For instance, the 9/11 attacks to WTC towers in New York City was a black swan before it occurred (pre 2001) but is now a type II security risk as it has already occurred (post 2001).

No widely accepted definitions exist for the different types of risk, making it very hard to make a distinction between them in a way that is accepted and understood by everyone. An organization thus needs to decide about the concrete difference between type I and type II risks. Both types of risks demand their own security risk assessment and management approaches. An organization needs to identify them separately, analyze them with different security risk analysis methods, evaluate and prioritize them separately, with separate decision making on their treatment, and deal with them with different security countermeasures.

In case of security, the lack of knowledge and information regarding causal factors and likelihood assessment is thus a true challenge. It is extremely difficult to assess the probability (or frequency) of type II security events, and even type I security events. Despite specific databases, such as the Global Terrorism Database – GDT (START, 2019), or the Repository of Industrial Security Incidents – RISI (Department of Homeland Security, 2017), or dedicated past accident studies (Casson Moreno et al., 2018) are available, security related statistics are unreliable and usually highly uncertain. Besides the difficulties to use the expected value formulas for security, it is very important to adequately manage security risks. Hence, the importance of security risk management.

Risk management can be defined as the systematic and regular study of (negative) risks threatening people, tangible and intangible assets, and activities and formulating and implementing an integrated policy with respect to risk reduction, risk transfer and risk financing. According to the most widely accepted definition of the ISO31000 Guide 73 (ISO-International standardization organization, 2009), risk management comprises the coordinated activities to steer and control an organization when risks are concerned. These are very complex definitions, but to put it in simple terms, risk management can be considered everything that is needed to manage and control risks. To this end, risk management uses a set of approaches, concepts, models, theories, and disciplines, especially developed to manage risks and to make sure that they are adequately controlled.

Risk management is therefore much more than merely looking after the legislative aspect of compliance, or dealing with the technical aspects of risk identification, risk analysis and risk evaluation. Risk management also includes risk communication, human and organizational aspects, economic aspects, business continuity planning, learning from accidents, risk governance, etc.

Fig. 3 provides a non-exhaustive overview of the various domains

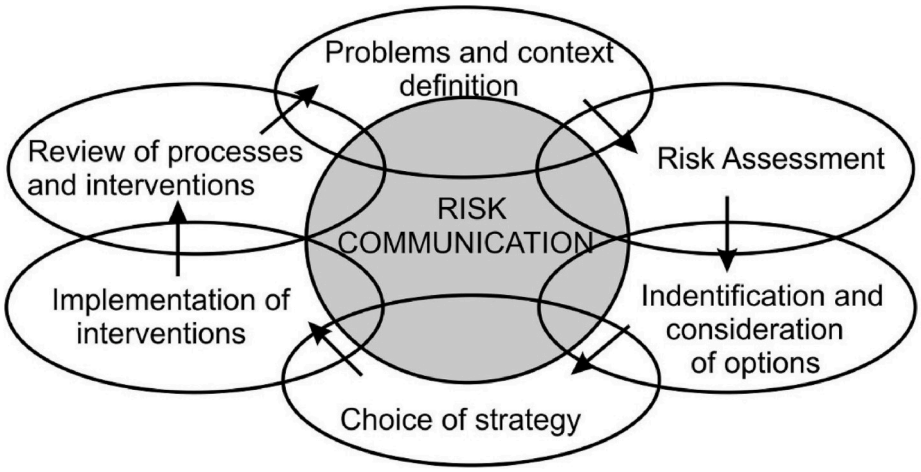


Fig. 4. The engineering risk management process. (Based on Meyer and Genserik, 2016).

that (operational) security risk managers should be concerned with. Physical security risk management is a term used for managing and controlling all physical security risks.

All the domains mentioned in Fig. 3 can be applied to the field of physical security, which denotes all security matters besides cyber security. Security managers obviously need to comply with legislation, and organizations often also set their own security objectives and targets. These activities also comprehend the assessment of physical security risks (composed of threats, vulnerabilities, losses) and prioritized. Furthermore, economic aspects of security investments need to be considered: insurance premium costs, security countermeasures costs, hypothetical benefits due to security investments, etc. Emergency planning and crisis management need to take security matters into account, for instance by involving law enforcement in contingency planning, or by developing a bomb incident plan. Security awareness needs to be created in the organization, requiring an adequate security climate and culture. All security incidents, small and large, need to be reported and investigated thoroughly, and a company memory needs to be built up regarding physical security, using security performance indicators. A security management system is developed to streamline all security efforts and to treat security risks. A security risk communication plan is drafted to make sure that in case of a major security incident good communication is guaranteed.

The basics of security risk management, similar to all other management domains, can be summarized as a "Plan-Do-Check-Act" cycle. This management cycle was originally developed in quality management science and is used to continuously improve not only product, service quality, or safety, but also security. In the first phase (Plan), a plan for making changes (improvements) is conceptualized. The next phase (Do) is the step of the implementation of the envisioned plan. In the third phase (Check), results of the implementation are obtained (e.g. using security performance indicators) giving input for the last phase (Act) where the evaluation of the results leads to further improvement strategies and measures. These improvement actions are put into a new plan, and the cycle starts again.

2. Models for security based on safety science

2.1. Security risk management models

Security management is one form of risk management and, more specifically, engineering risk management (ERM). Many flowcharts exist in the literature to describe the sequences of ERM; the main steps involved are displayed in Fig. 4. The process is based on a structured and

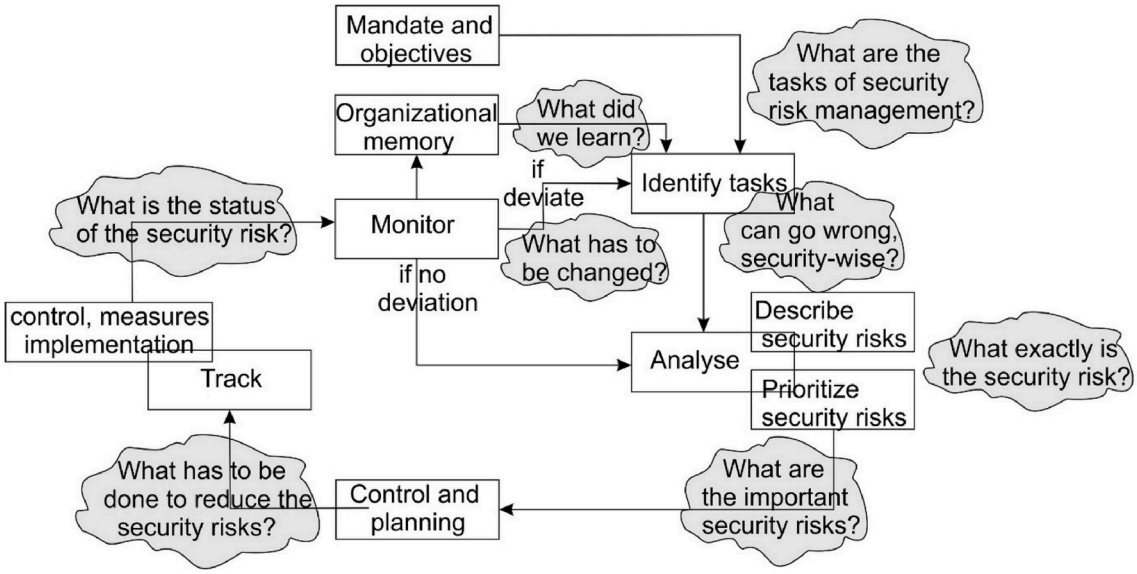


Fig. 5. Main questions of the security risk management process. (Based on Meyer and Genserik, 2016).

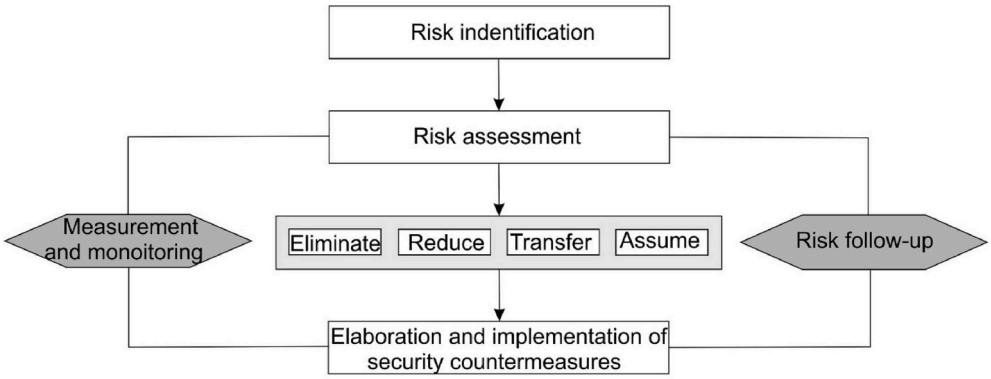


Fig. 6. Simplified risk management process. Adapted from (Meyer and Genserik, 2016).

systematic approach covering all of the following phases: the definition of the problem and its context, risk evaluation, identification and examination of the risk management options, the choice of management strategy, intervention implementations, process evaluation and interventions, as well as risk communication. The phases are represented by circles, and the intersections show their interrelations.

The process normally starts at the problem definition step and proceeds clockwise. The central position of the risk communication phase indicates its involvement in the whole process, and the particular attention this aspect should receive during the realization of any of these phases.

Although phases must generally be accomplished in a successive way, the circular form of this process indicates that it is iterative. This characteristic enables the revision of phases in light of all new significant information that would emerge during or at the end of the process and would enlighten the deliberations and anterior decisions. The made decisions should be, as often as possible, revisable while the adopted solutions should be reversible. Although the iterative character is an important quality of the process, it should not be an excuse to stop the process before implementing the interventions. Selecting an option and implementing it should be realized even if the information is incomplete.

The flexibility must be maintained all along the process in order to adjust the relative importance given to the execution and revision of the phases, as well as to the depth level of analysis or the elements to take into consideration.

It is also interesting to look at the risk management iterative ring through the questions that must be answered in order to get the process moving forward. A summary of these questions is presented in Fig. 5.

The starting point of the iterative process is realizing what is the mission and the set of activities devoted to the risk management by answering the question "What are the tasks of security risk management?" Hence, we should identify "What could go wrong, security-wise?" in the identification step. Answering "What exactly is the security risk?" allows for describing, analyzing and prioritizing risks. Then, in order to control and plan, the question "What are the important security risks?" is raised. To implement the adequate measure for risk reduction, we have to answer "What has to be done to reduce the security risk?" This allows also for controlling and tracking the implementation of security measures. The task is not yet over, as we should not forget to monitor the situation by asking several other questions: "What is the security risk status?" allows following the time evolution of the considered security risk. If something begins to deviate, then "What has to be changed?" brings us back to the risk identification step. Another important point, often forgotten in risk management, is the answer to "What did we learn?". In summary, the security risk management process is not only an identification and treatment process, it is a learning process that never ends and must be continuously performed.

Another characteristic of engineers is to simplify complex systems in order to be able to model and analyze them more efficiently. From this perspective, a simplification of the risk management process as depicted in Fig. 6 can be envisioned.

Going back to the principles of risk management, ISO 31000:2009 (International Organization for Standardization, 2009) indicates that for risk management to be effective, an organization should at all levels comply with the principles below:

- Risk management creates and protects value. Risk management contributes to the demonstrable achievement of objectives and improvement of performance in, e.g., human health and safety, security, legal and regulatory compliance, public acceptance, environmental protection, product quality, project management, efficiency in operations, governance and reputation.
- Risk management is an integral part of all organizational processes. Risk management is not a stand-alone activity that is separate from the main activities and processes of the organization. Risk management is part of the responsibilities of management, including strategic planning and all project and change management processes.
- Risk management is part of decision-making. Risk management helps decision-makers make informed choices, prioritize actions and distinguish among alternative courses of action.
- Risk management explicitly addresses uncertainty. Risk management explicitly takes account of uncertainty, the nature of that uncertainty, and how it can be addressed.
- Risk management is systematic, structured and timely. A systematic, timely and structured approach to risk management contributes to efficiency and to consistent, comparable and reliable results.
- Risk management is based on the best available information. The inputs to the process of managing risk are based on information sources such as historical data, experience, stakeholder feedback, observation, forecasts and expert judgment. However, decision-makers should inform themselves of, and should take into account, any limitations of the data or modeling used or the possibility of divergence among experts.
- Risk management is tailored. Risk management is aligned with the organization's external and internal context and risk profile.
- Risk management takes human and cultural factors into account. Risk management recognizes the capabilities, perceptions and intentions of external and internal people that can facilitate or hinder achievement of the organization's objectives.
- Risk management is transparent and inclusive. Appropriate and timely involvement of stakeholders and, in particular, decision-makers at all levels of the organization, ensures that risk management remains relevant and up-to-date. Involvement also allows stakeholders to be properly represented and to have their views taken into account in determining risk criteria.
- Risk management is dynamic, iterative and responsive to change. Risk management continually senses and responds to changes. As

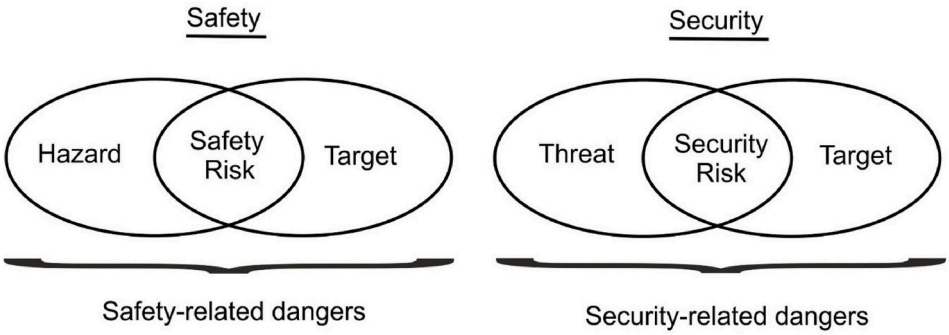


Fig. 7. Physical risk Model (hazards and threats can be seen as parent nodes for safety and security).

external and internal events occur, context and knowledge change, monitoring and review of risks take place, new risks emerge, some change, and others disappear.

- Risk management facilitates continual improvement of the organization. Organizations should develop and implement strategies to improve their risk -management maturity alongside all other aspects of their organization.

The success of risk management will depend on the effectiveness of the management framework that provides the foundations and arrangements to embed it throughout the organization at all levels. The framework assists in managing risks effectively through the application of the risk management process at varying levels and within specific contexts of the organization. The framework ensures that information about risk derived from the risk management process is adequately reported and used as a basis for decision-making and accountability at all relevant organizational levels.

It is not really important what scheme is used, the most important aspect is that with time one remains consistent in the use and in the follow-up. It is better to have a simplified system in adequate use rather than a complex scheme that will be only partially used.

A variety of risk management schemes and frameworks are available to be used in industrial practice. A framework should always have a feedback loop built into which, where one is certain that risk management efforts never stop. Risk policy, assessment, communication, and monitoring should also always be part of the scheme.

2.2. Physical model of security risk

As pointed out in Section 2.1 (see Fig. 2), security risks are characterized by three factors: threats, vulnerabilities, and intentional losses, which together form the "Security Risk Trias" (see Fig. 1). Nonetheless, risk is obviously a theoretical concept, and can be described in another way. To have a profound understanding of risk, we also need to discuss the following alternative – more "physical" - approach, which is well-known for safety and based on safety science.

In order to physically describe what a security risk is, some of its key components should be defined. The notion of the "target" needs to be introduced. The target can be represented by:

- A human
- The environment
- A natural monument
- A process in a Company
- A Company
- The brand image
- Etc.

A danger is the potential of a hazard or a threat to cause damage to a target. A danger can be intentional – then it is related to the field of security and a threat is involved – or it can be accidental or by coincidence, where it is safety-related and a hazard is involved.

Risk exists as soon as a hazard or a threat affects one or many possible targets. An identified hazard that does not affect any target does not represent a risk, and the same goes for an identified threat not affecting any target. For example, life in Iraq or Syria may be full of threats, but as long as these threats do not affect targets in or from Canada, there are no losses possible in Canada, and hence no security risk from the identified threats in Canada. Risk is found at the interface, or at the cross section, of a hazard/threat and a target, as illustrated in Fig. 7.

Basically, a risk is physically characterized by four elements:

1. A hazard/threat.
2. One or several targets threatened by the hazard/threat.
3. The level of exposure of the target to the hazard/threat (the interface)
4. The measures taken to reduce the danger.

These elements, depicted in Fig. 8, show that a protection and/or prevention barrier in case of safety, and a countermeasure in case of security, is required to prevent a hazard or a threat, that may be (come) out of control, from reaching the target. Thus, the risk formulation is influenced by the type of constitutive elements associated with the different domains.

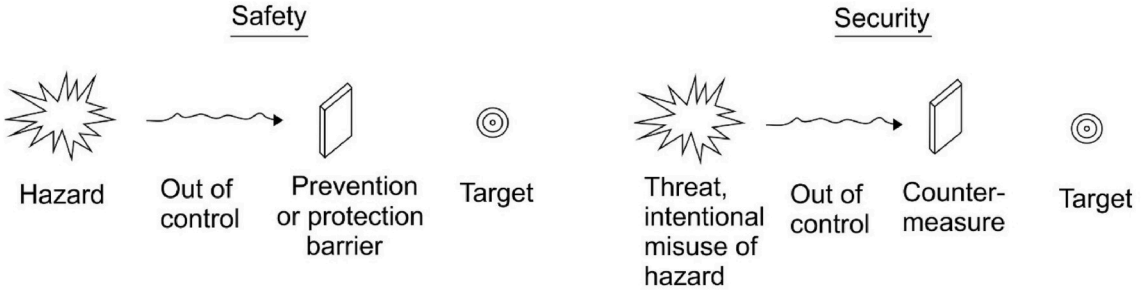
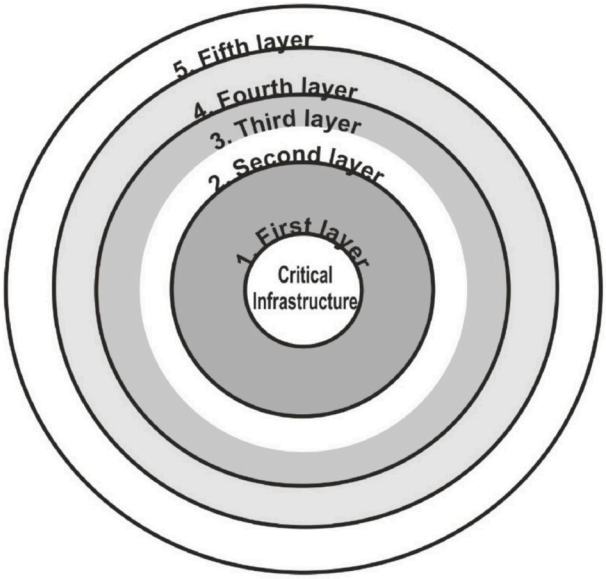


Fig. 8. Constitutive elements of safety risk and security risk.



1. First layer of security protection (Inner ring):
- Alert personnel
- Door and cabinet locks
- Network firewalls and passwords
- Visitor escort policies
- Document shredding
- Emergency communications
- Secure computer rooms
- CCTV
- Intelligence

2. Second layer of security protection (Inner Middle ring) :
- Locked doors
- Receptionist
- Badge checks
- Access control system
- Parcel inspection
- Carry out SVAs

3. Third layer of security protection (Outer middle ring):
- Lighting
- Fences
- Entrance/exit points
- Bollards
- Trenches
- Intrusion detection
- Intrusion sensors
- Guards on patrol at property fenceline

4. Fourth layer of security protection (Outer ring):
- Badge checks
- Access control system
- Turnstiles
- Window bars
- Receptionist

5.Fifth layer of security protection Law enforcement (Outside ring):
- Police
- Fire fighters
- Other law enforcement organisations

Fig. 9. Security rings of protection illustrated as 'five layers of security protection'. Adapted from (Meyer and Genserik, 2016).

2.3. Rings of protection model

The fundamental basis of security management can be expressed in a similar way to the layers of protection used in chemical process plants to illustrate safety barriers. In a similar concept to the concentric rings of protection (CCPS, 2003a), the spatial relationship between the location of the target asset and the location of the physical countermeasures are used as a guiding principle. Fig. 9 exemplifies the rings of protection in terms of five 'layers of security protection' and a non-exhaustive list of possible component countermeasures.

In security terms, the target is broadly defined as people (employees, visitors, contractors, nearby members of the community, etc.), information (formulae, prices, processes, substances, passwords, etc.), and property (buildings, vehicles, production equipment, storage tanks and process vessels, control systems, raw materials, finished products, hazardous materials, natural gas lines, rail lines, personal possessions, etc.) that are believed crucial to preventing from major business disruption and substantial economic and/or societal damage.

By considering the sequence of events that might lead to a potentially successful attack, another representation can be given, illustrating the effectiveness of the rings of protection (Fig. 10).

Firstly, Companies can clearly protect themselves in a much better way against external attacks than against attacks from within the company itself, because in the latter case, there only exists indoor security to avert the threat, and there are only two layers of security protection (first and second layer). Secondly, as the effective prevention, protection and mitigation of attacks depend on meticulously carrying out security risk assessments, the latter is of crucial importance to deter, detect, deny, delay and defend (also known in security management as the 5D strategy) against possible threats within a single company as well as within an industrial area of companies.

2.4. Swiss cheese model

The "Swiss cheese" model was developed by the British psychologist Reason (1997) to explain the existence of accidents by the presence of "holes" (he called them 'pathogens' which may lead to accidents) in the risk management system. Fig. 11 displays the Swiss cheese model adopted for security. A solid insight into the working of the organization allows for the possibility to detect such "holes", while risk assessment

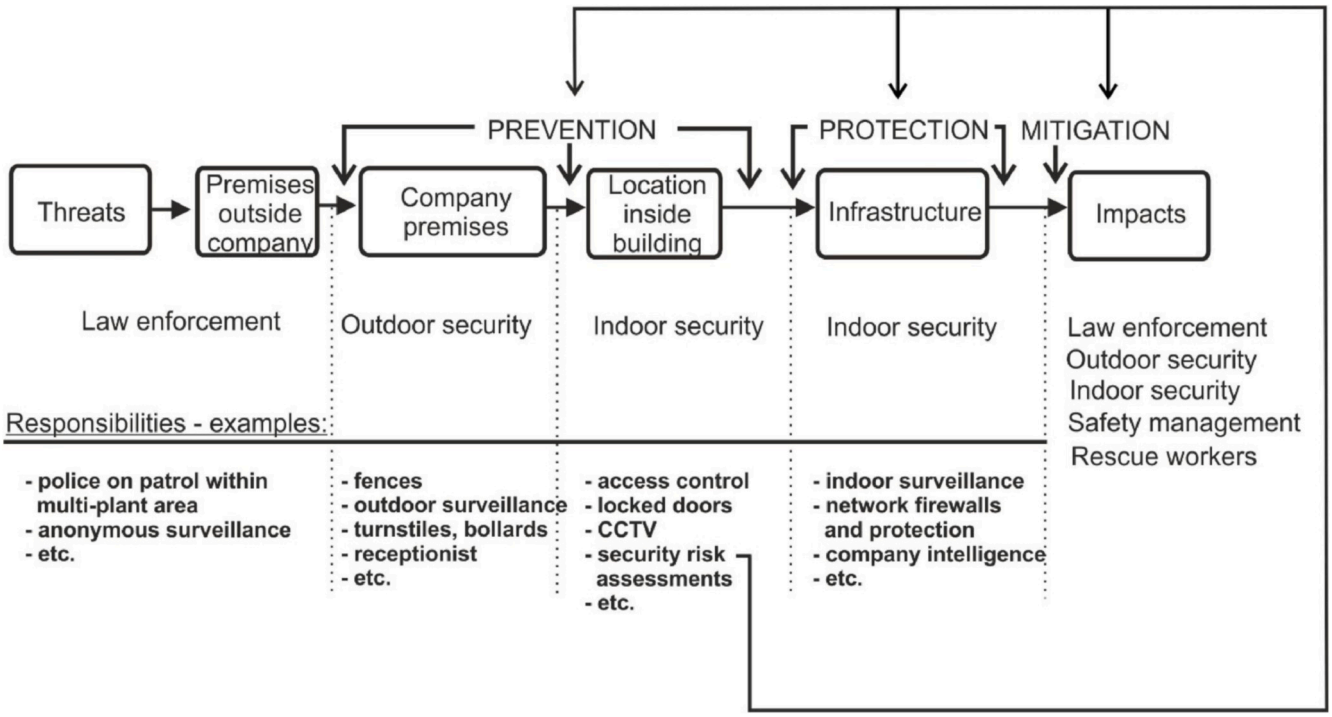


Fig. 10. Anatomy of an attack: the role of the rings of protection described in Fig. 9. Adapted from (Meyer and Genserik, 2016).

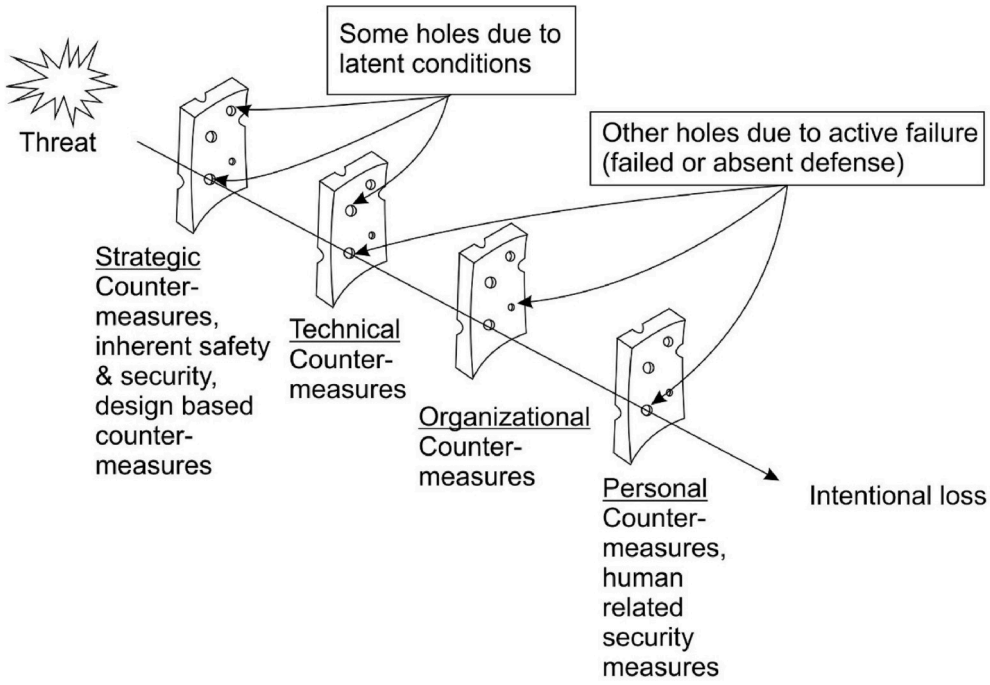


Fig. 11. The Swiss cheese model for security.

includes the identification of suitable measures to "close the holes".

It is important to notice that the Swiss cheese is dynamic: holes may increase in number or size (e.g., caused by mistakes, errors, violations, etc.), but they may also decrease (because of solid risk management and adequate countermeasures). This model is very powerful in its use of "barrier" thinking (or "rings of protection" thinking). The holes within the barriers should be made as small as possible through adequate risk management, and this should be done for type I (e.g., thefts, sabotage) as well as type II (e.g., terrorist attacks) security risks.

2.5. *Security incident bipyramid model*

Heinrich (1950), Bird and Germain (1985) and Pearson (James and Fullman, 1994), amongst other researchers, determined the existence of a ratio relationship between the numbers of (safety-related) incidents with no visible injury or damage, over those with property damage, those with minor injuries, and those with major injuries. This accident ratio relationship is known as "the accident pyramid" (European terminology) or "the safety triangle" (USA terminology). Accident

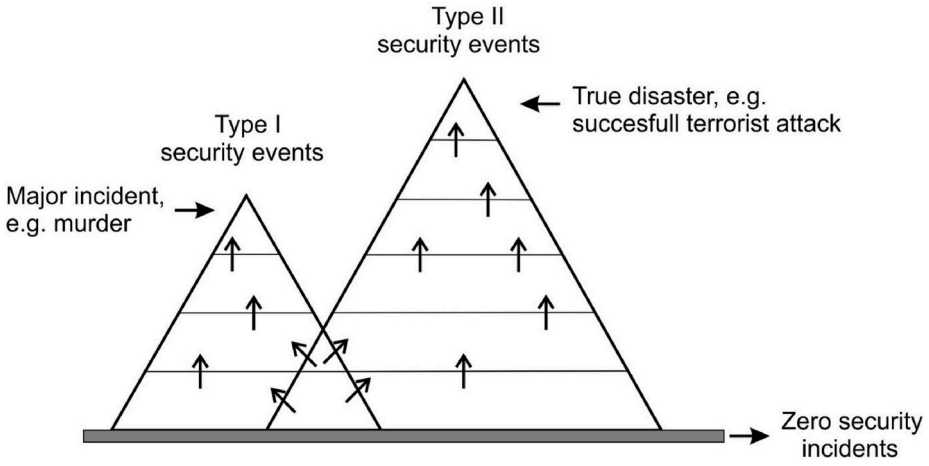


Fig. 12. The Security Incident bi-pyramid Model.

pyramids unambiguously indicate that accidents are "announced". Hence the importance of awareness and incident analyses. Different ratios were found in different studies (varying from 1:300 to 1:600) depending on the industrial sector, the area of research, cultural aspects, etc. However, the existence of the accident pyramid has obviously been proven from a qualitative point of view. It is thus possible to prevent serious accidents by taking preventive measures aimed at near-misses, minor accidents, etc. These "classic" accident pyramids clearly provide an insight into type I accidents where representative statistical data are at hand.

If one looks upon this accident pyramid paradigm with security goggles, and taking type I and type II events into consideration, the following analogy can be made. The accident pyramid possibly and probably exists for security, forming a "security incident pyramid", with some specific conditions, that is, under the paradigm with the following assumptions:

(i) All minor criminal incidents are not the same in their potential for extremely serious crime. A small sub-set of low severity crimes come from vulnerabilities that act as a precursor to serious crime.
(ii) Criminal and security-related events of differing severity have differing underlying causes.
(iii) Reducing serious criminal events often requires a different strategy than those required for reducing less serious security-related incidents.
(iv) The strategy for reducing serious criminal events and major security-related incidents (such as terrorism) should use precursor data derived from minor criminal facts, security incidents of all kind, near misses and vulnerabilities.

Fig. 12 shows the "security incident bipyramid", which can be drawn as two pyramids with a small overlap. One pyramid represents type I risks, leading at most to a serious event (e.g., a murder), but not to a major catastrophe, and the other pyramid represents type II security risks, with the possibility to lead to a true disaster (e.g., a terrorist attack with multiple fatalities).

The bi-pyramid illustrates that there is a difference between type I security risks and type II security risks. In other words, "regular criminal events" should not be confused with "major criminal events" such as terrorism. Not all small criminal events have the potential to lead to a disaster, but only a minority of such events may eventually end up in a security-related catastrophe. Obviously, to prevent disasters and catastrophes, security risk management should be aimed at both types of security risks, and certainly not only at the large majority of "regular" security risks. Last but not least, different performance indicators should be used for the two different types of security.

2.6. *The bow-tie model for security*

The bow-tie is a very powerful technique developed in the safety community for having an overview of possible scenarios related to a so-called central event in the middle of the bow-tie (loss of energy, leak, etc.) leading to unintentional losses. It can also be seen as a metaphor (such as the Swiss cheese metaphor) to visualize the scenarios. The approach dates back to the 1990s and is widely used for analyzing (major) labor and process safety incidents.

If applied to security, a bow-tie is able to present a clear overview of all causes (threats) and all consequences (potential intentional losses) of one particular undesired security-related event (for instance an explosion due to a successful terrorist attack on asset x). The method

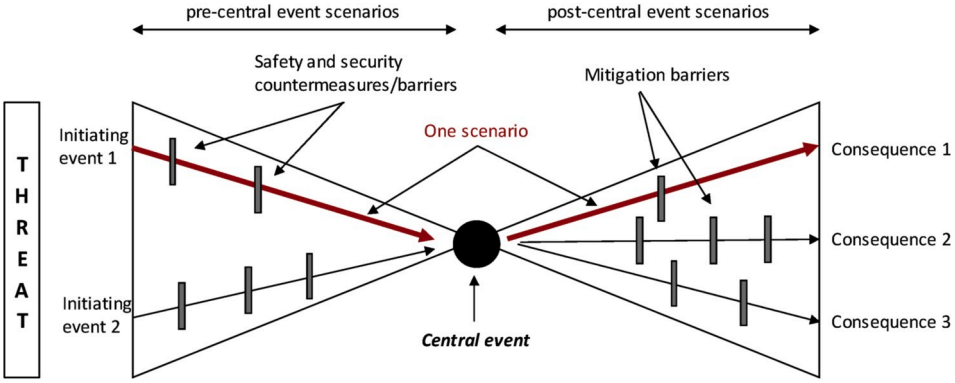


Fig. 13. The bow-tie technique/metaphor applied to security scenarios.

Table 1
The relation between Threat, Effect and Consequence.

Left bow-tie Pre-central event scenario	Central event		Right bow-tie Post-central event scenario	
Threat	*Effect* (intentional release of a hazard; loss of control of the threat)		*Consequence* (intentional losses)	
Deliberate misuse of Energy, flammable & toxic substances	Loss of Containment →	Heat radiation Overpressure Toxic concentration	Burn Internal injury Poisoning	→ Casualties, wounded, damage and/or production loss

combines a so-called fault tree with an event tree, and, as already mentioned, represents a number of different scenarios in the form of the cause of an event, its consequences and the barriers that stop the event from happening. In security terms, the bow-tie is a metaphor for an attack (malicious action) process. The bow-tie technique is illustrated in Fig. 13.

To understand the meaning of the concept of the 'central event', it is important to clarify the concept of process security in relation to the bow-tie model. As already explained, in process security the threat comes from the adversary misusing or intentionally attacking one or more processes or process installations, for instance causing a release of a hazardous substance or a release of energy (e.g., in the form of a blast wave). A 'central event' (Fig. 13) is a situation in which the threat (the deliberate release of a hazardous substance or energy) has become uncontrollable. As was also indicated above, a hazard is the intrinsic ability to cause any kind of losses (human and non-human). Cockshot (2005) describes hazard as 'a condition that could lead to injury, damage to property or the environment'. He defines a central event as 'the initial consequence which involves the release of a hazard'. If 'initial consequence' here is (freely) translated as an effect, effect is reflected in the central event and can be defined as the direct result of the release of the hazard. In the right part of the bow-tie the scenario develops further into the final consequences: victims, wounded, damage, production losses, etc.

Table 1 shows the relationship between threat, effect, and consequence. For example, the intentional release of a flammable gas can lead to a jet fire or fireball with a certain heat radiation, which in turn causes burns and possibly death. As another example, in the context of terrorism, the deliberate release of a toxic gas (*threat*), for instance chlorine, may lead to a toxic cloud with a certain concentration of the lethal material chlorine (*effect*), leading to the poisoning of a group of people (*consequence*).

3. Principles for security based on safety science

3.1. The inherent safety/security principle

It is obvious that the first and foremost approach to deal with safety and security problems is to cut away the hazardous or threatening phenomenon. If the hazard or threat is away, there is no possibility anymore for an undesired event, be it un-intentional or deliberate. Inherent safety also leads to inherent security: if there are no dangerous preconditions that can be exploited by adversaries, the target won't be attractive any more, and thus there will be no threats, and hence, no security risks and no security related dangers. The principle of inherent safety consists of five concepts, that is, intensification, substitution, attenuation by moderation, attenuation by limitation of effects, and simplification. The concepts are illustrated in Fig. 14.

The concepts have been developed in a safety context by Kletz (1998), and further improved by Kletz and Amyotte (2010). The first concept, intensification, indicates that by intensifying the activities and/or processes, for instance using less of a hazardous/dangerous material, safety can be bettered. In this concept, it is important to verify whether there is no risk homeostasis, since different operating conditions (higher pressure, higher temperature) may lead to other risks, or the risk may have been partially relocated. In the latter cases, that is, when the risks are relocated, the same total risk still exists. The second concept, substitution, aims at replacing substances and procedures by less hazardous ones, by improving construction work, adopting water instead of a flammable solvent for liquid-liquid extraction, etc. Also, in this case, care should be taken that there is not simply a replacement of the risk, as substitution may induce novel risks given the modification in process/operations. The third concept, attenuation by moderation, indicates that safety may improve by working under more benign conditions, for instance under less dangerous process conditions or by using improved/stronger equipment. The fourth concept, attenuation by limitation of effects, notes that it is always better to try to lower the total potential consequences of a single undesired event as much as possible. The idea is that minimizing the overlapping of losses from a single event will lower the severity of any unwanted event. This can for instance be done through facility siting (USA terminology, as documented by (CCPS, 2003b)) or land-use planning (European terminology, as per Article 13 of Seveso III directive (European Commission, 2012)), which boils down to the segregation by separation of high-risk units. Another way of segregation is by duplicating some essential (not to lose) high-risk units. The fifth concept, simplification, follows the simple observation that complex processes and situations always are more dangerous than simple ones. This is due to the fact that mistakes are much easier to make and/or be detected in complex facilities than in simple facilities.

3.2. STOP principle

If it is not possible to apply the inherent safety/security principle and to delete the hazard, for instance, by improving the construction work or by using less hazardous substances, we must then proceed with so-called add-on safety/security measures, that is, technical and organizational measures and as a last resort, human measures. This can also already be seen in the Swiss cheese barriers in Fig. 11.

The STOP (strategic, technical, organizational and personal measures) principle (see also Meyer and Genserik, 2016) underlines this approach by giving priority to the measures in the following order:

i ***S**trategic* measures: *strategic*, substitution of processes or substances giving a less hazardous/threatening result (e.g., substituting, eliminating, lowering, modifying, abandoning, etc.); abandon process or product, modify final product. (see also previous section)
ii ***T**echnical* measures: *technical* protection against hazardous/threatening phenomena that cannot be eliminated, lowering the likelihood of success of an adversary attack (Landucci et al., 2017), the attractiveness of a target (Argenti et al., 2015), decreasing the vulnerability (Argenti et al., 2018), and reducing the spread of impact (e.g., replacing, confining, isolating/separating, automating, firewall, EX zones, bodyguards, etc.).
ii ***O**rganizational* measures: *organizational* modifications of the work, training schemes, security instructions, information concerning residual security risk and how to deal with it (e.g., awareness training schemes, communication plans, planning, supervising, warnings signs, etc.)
iv ***P**ersonal* measures: *securing* people by means of personal protection equipment (PPE), improving security climate and culture, security training, security communication, etc.

The hierarchy of the priorities should be viewed upon in the following order:

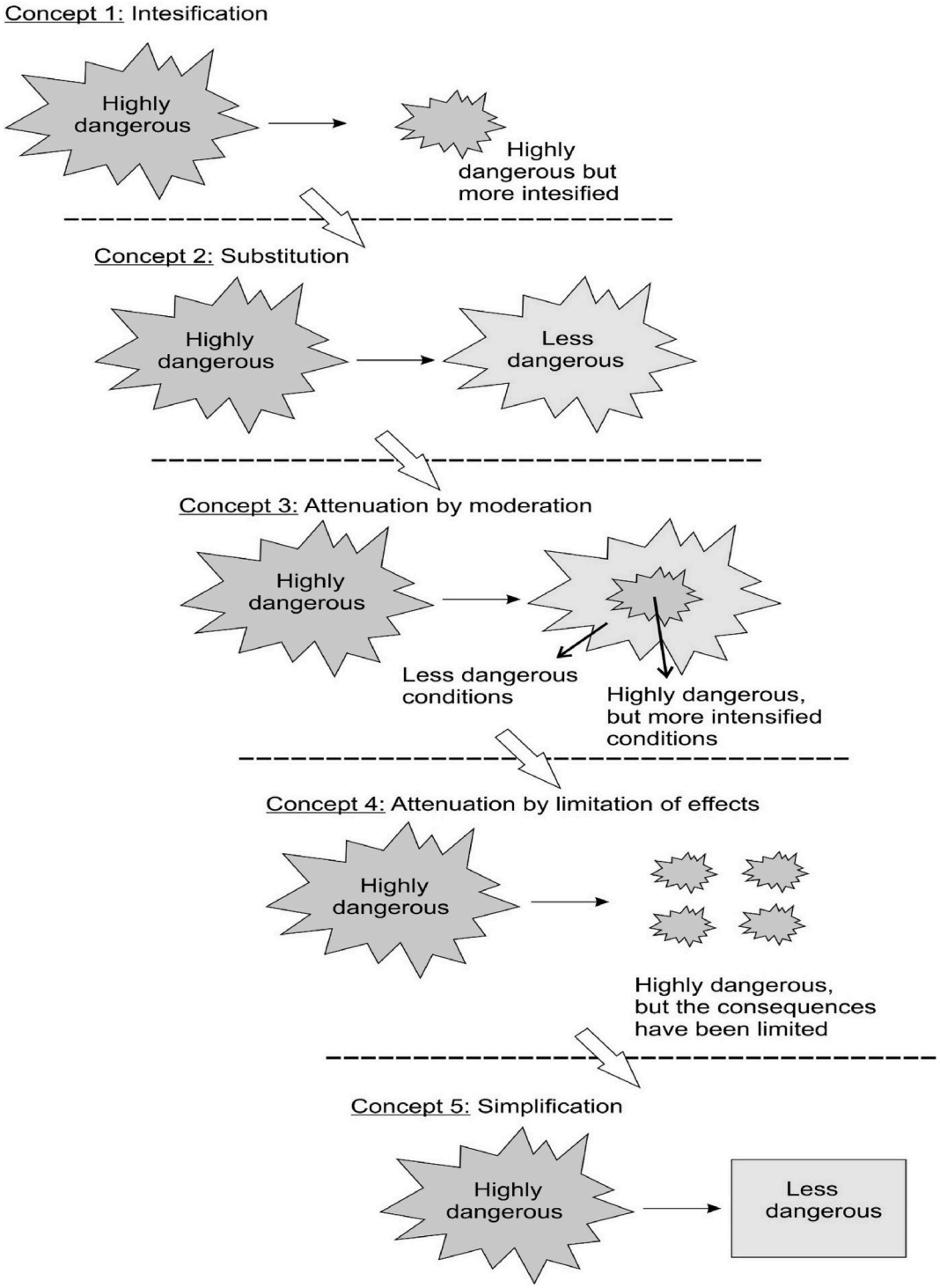


Fig. 14. Five concepts of Inherent safety/security (for taking Strategic measures from STOP principle).

i. Acting at the *source*: in case of security the source is the adversary, the person with malicious intent. He/she should be kept out of the organization as much as possible.
ii. Acting at the *interface* (on the trajectory between the source and the target): limiting the propagation (utilization of hardware measures, such as add-on barriers), catching/neutralizing (local or general ventilation, air purification, substance neutralization), people control (raising barriers, access restrictions, evacuation signs) and surveillance (cameras and sensors in the field, energy levels in the zone, excursions or deviations (alarms)).
ii. Acting at the *target*: different types of target can be envisioned: (i) *target 1 = infrastructure:* deleting the risk (substituting product or process, in situ neutralization), limiting target risks (re-enforcing the system, lowering the energy levels), predictive measures (rupture disk, valves) and surveillance (cameras and sensors at the installations). Increasing security awareness and social control on site. (ii) *target 2 = human capital*: lowering the vulnerability (personal security and protective equipment selection, special training), reducing exposure (e.g., automation), reducing the time (job

Table 2
The STOP table for security with illustrative examples (non-exhaustive lists).

	At the source (Outer Ring)	At the interface (Middle Ring)	At the target (Inner Ring)
Measures **S** (strategy)<	• Substitution • Change process	• Automation, telemanipulation • Land-use planning - redundancy of critical systems	• Criteria for selection of security-aware operators - enforced infrastructure
Measures **T** (technical)	• cameras/intrusion detection - fences - Bollards and trenches • intrusion sensors	• locked doors • access control system - turnstiles	• doors and cabinet locks - network firewalls and passwords - CCTV
Measures **O** (organizational)	• guards on patrol at property fence line - Passport controls at entrance	• visitor escort policies • receptionists in buildings - Badge checks	• security instructions - intelligence - emergency plans • document shredding
Measures **P** (personal)	• Education/training of the entrance guards	• Information/instruction on threats	• Instruction for the use of security equipment

rotation) and supervising (individual exposure, biological monitoring, medical survey, correct PPE use and following rules).

In general, we must combine measures to obtain the desired security level. It is important that the choice of security measures enables the reduction of the likelihood and severity of the threatening events. Once the priorities have been established, it is possible to determine the correct method to adequately deal with each of the identified security risks.

Table 2 presents a recap of the ordering of measures and the considered environment, along with a few illustrative examples for each category. Directions of approach are from top to down and then from left to right. Eliminating the hazard is the most favorable approach for reducing the risks; no hazard, no threat, no risk. Substitution is interesting as long as it does not generate new hazards or threats. In the STOP principle, the elimination and substitution phases are included in the strategic measure S. They are, however, rarely possible in practice, and may sometimes not be applicable.

Note that in practice, personal protection measures are usually put into place before the technical and organizational measures. This happens for many different reasons, including costs, delays, implementation simplicity, loss of responsibility, to have no time or take no time to analyze the situation, the simplicity, etc. Many organizations have invested heavily in personnel, processes and technology to better manage their security risk. However, these investments may often not be optimal. To manage security in a most efficient and effective way, scarce resources need to be managed well, making better decisions and reducing the organization's exposure to negative events by adequately implementing the four-level steps comprising strategic, technical, organizational and personal aspects.

4. Discussion

The present work illustrated relevant analogies between the fundamental basis of security management and the analysis of layers of protection used in the industrial domain and, particularly, in modern chemical process plants for addressing safety-related, accidental events.

In the similar security-related concept of rings-of-protections (CCPS, 2003a), the spatial relationship between the location of the target asset and the location of the physical countermeasures is used as a guiding principle. Moreover, specific management strategies devoted to "unintentional" events (i.e., safety management) may inherently serve as valiant means to stop accident chains or cascading events (Shaluf, 2007) induced by external acts of interference, thus related to security. For instance, fireproofing coating applied on hazardous materials tank cars to secure them against heat exposure from accidental fires during transportation (Scarponi et al., 2017) provide resistance against arson attacks from terrorists aimed at generating escalation scenarios.

Reniers et al. (2008) for instance reflected on the strategy of integrating safety and security elements in order to prevent cascading events in clusters chemical and process facilities. When eliminating terrorist groups and intentional attacks seems impossible, minimizing the potential consequences of intentional attacks can be considered as an effective approach to protect industrial plants against terrorist attacks (Reniers and Audenaert, 2014).

However, minimizing the potential consequences is challenging, not only due to the interactions among different systems, but also because the evolution of complex cascading events is a dynamic process (Pescaroli et al., 2018). Therefore, it is important to design rings of protection in a way that also cascading events are taken into account, accounting for their complex and dynamic features. For instance, Khakzad et al. (2013, 2017) reflected on cascading events triggered by fires and related complicating factors, such as synergistic effects.

More generally, security management at a single industrial site should, by means of the ring-of-protection concept, adopt a number of measures, combining physical security equipment, people and procedures but, at the same time, verify if the installed "safety" provisions may be able to cope with potential cascading events triggered by external attacks. This may be seen as a key strategy in order to offer the best chance of adequate asset protection against a variety of threats.

5. Conclusions and recommendations

Compared with safety, physical security is a relatively new field of science. It has taken a long time for security science to take its place in science, but finally, due to the growing interconnectedness of citizens and multidimensional nature of threats affecting the industrial and public domain, it has taken its place in academia. The maturity of security research is still at a low level but is climbing steadily. Since both safety and security are about avoiding or decreasing losses, many analogies exist. Therefore, the security research can learn from safety research and use developed models and principles of safety, when these are adapted to the security needs and situations. This paper discussed a number of such models and principles for security science and managing security risks.

References

Argenti, F., Landucci, G., Spadoni, G., Cozzani, V., 2015. The assessment of the attractiveness of process facilities to terrorist attacks. Saf. Sci. 77, 169–181.
Argenti, F., Landucci, G., Reniers, G., Cozzani, V., 2018. Vulnerability assessment of chemical facilities to intentional attacks based on Bayesian Network. Reliab. Eng. Syst. Saf. 169, 515–530.
Bird, E., Germain, G.L., 1985. Practical Loss Control Leadership, the Conservation of People, Property, Process, and Profits. Institute Publishing, Loganville, GA.
Casson Moreno, V., Reniers, G., Salzano, E., Cozzani, V., 2018. Analysis of physical and cyber security-related events in the chemical and process industry. Process Safety and Environmental Protection, 2018 116, 621–631.
CCPS - Center of Chemical Process Safety, 2000. Guideline for Chemical Process Quantitative Risk Analysis. American Institute of Chemical Engineers - Center of Chemical Process Safety, New York, NY.
CCPS, Center for Chemical Process Safety, 2003a. Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites. American Institute of Chemical Engineers, New York.

CCPS - Center of Chemical Process Safety, 2003b. Guidelines for Facility Siting and Layout. American Institute of Chemical Engineers - Center of Chemical Process Safety, New York, NY.
Cockshot, J.E., 2005. Probability bow-ties – a transparent risk management tool. Process Saf. Environ. Protect. 83 (B4), 307–316.
Department of Homeland Security, 2017. Chemical Facility Anti-terrorism Standards (CFATS).
European Commission, 2012. European Parliament and Council Directive 2012/18/EU of 4 July 2012 on control of major-accident hazards involving dangerous substances, amending and subsequently repealing council directive 96/82/EC. Off. J. Eur. Communities L197, 1–37.
Heinrich, H.W., 1950. Industrial Accident Prevention, third ed. McGrawHill Book Company, New York.
International Organisation of Standardization (ISO), 2009. Risk Management Standard – Principles and Guidelines. ISO, Geneva, Switzerland.
James, B., Fullman, P., 1994. Construction Safety, Security and Loss Prevention. Wiley Interscience, New York.
Khakzad, N., Khan, F., Amyotte, P., Cozzani, V., 2013. Domino effect analysis using bayesian networks. Risk Anal. 33, 292–306.
Khakzad, N., Landucci, G., Reniers, G., 2017. Application of dynamic Bayesian network to performance assessment of fire protection systems during domino effects. Reliab. Eng. Syst. Saf. 167, 232–247.
Kletz, T., 1998. Process Plants. A Handbook for Inherently Safer Design. Braun-Brumfield, Ann Arbor, USA.
Kletz, T., Amyotte, P., 2010. A Handbook for Inherently Safer Design, second ed. CRC Press, Boca Raton, USA.
Landucci, G., Argenti, F., Cozzani, V., Reniers, G., 2017. Assessment of attack likelihood to support security risk assessment studies for chemical facilities. Process Saf. Environ. Protect. 110, 102–114.
Meyer, Thierry, Genserik, Reniers, 2016. Engineering Risk Management, second ed. De Gruyter, Berlin.
Paté-Cornell, E., 2012. On “black swans” and “perfect storms”: risk analysis and management when statistics are not enough. Risk Anal. 32, 1823–1833. https://doi.org/10.1111/j.1539-6924.2011.01787.x.
Pescaroli, G., Wicks, R.T., Giacomello, G., Alexander, D.E., 2018. Increasing resilience to cascading events: the M.OR.D.OR. scenario. Saf. Sci. 110, 131–140.
Reason, J.T., 1997. Managing the Risks of Organisational Accidents. Ashgate Publishing Limited, Aldershot, UK.
Reniers, G.L.L., Audenaert, A., 2014. Preparing for major terrorist attacks against chemical clusters: intelligently planning protection measures w.r.t. domino effects. Process Saf. Environ. Protect. 92, 583–589.
Reniers, G.L.L., Dullaert, W., Audenaert, A., Ale, B.J.M., Soudan, K., 2008. Managing domino effect-related security of industrial areas. J. Loss Prev. Process. Ind. 21, 336–343.
Scarponi, G.E., Landucci, G., Tugnoli, A., Cozzani, V., Birk, A.M., 2017. Performance assessment of thermal protection coatings of hazardous material tankers in the presence of defects. Process Saf. Environ. Protect. 105, 393–409.
Shaluf, I.M., 2007. An overview on the technological disasters. Disaster Prev. Manag.: Int. J. 16 (3), 380–390.
National Consortium for the Study of Terrorism and Responses to Terrorism (START), 2019. Global Terrorism Database. https://www.start.umd.edu/gtd/. (Accessed 28 June 2019).