Distinguishing Attacks and Failures in Industrial Control Systems
Knowledge-based Design of Bayesian Networks for Water Management Infrastructures

Chockalingam, S.

DOI
10.4233/uuid:17da1df4-3295-45d3-9119-9f92a547e7c6

Publication date
2020

Document Version
Final published version

Citation (APA)
Chockalingam, S. (2020). *Distinguishing Attacks and Failures in Industrial Control Systems: Knowledge-based Design of Bayesian Networks for Water Management Infrastructures*. [Dissertation (TU Delft), Delft University of Technology]. https://doi.org/10.4233/uuid:17da1df4-3295-45d3-9119-9f92a547e7c6

Important note
To cite this publication, please use the final published version (if applicable).
Please check the document version above.

Propositions

accompanying the thesis

DISTINGUISHING ATTACKS AND FAILURES IN INDUSTRIAL CONTROL SYSTEMS

KNOWLEDGE-BASED DESIGN OF BAYESIAN NETWORKS FOR WATER MANAGEMENT INFRASTRUCTURES

by

Sabarathinam CHOCKALINGAM

1. Knowledge-based approaches are appropriate for modelling cyber security of industrial control systems due to the difficulty to obtain real data (Related to Chapter 3 – 6 in the thesis).
2. Fishbone diagrams are more suitable than Bayesian Networks (BNs) themselves for knowledge elicitation in constructing the qualitative part of BN models that would help to distinguish between attacks and technical failures (Related to Chapter 4 in the thesis).
3. Correct diagnosis of the major cause for an observed problem is crucial for effective response in critical infrastructures. For instance, the effective response for a technical failure would be to repair or replace the component, whereas the effective response for an attack would be to block the attack vector (Related to Chapter 4 – 6 in the thesis).
4. The DeMorgan model is more suitable than conventional techniques like noisy-OR for reducing the number of conditional probabilities to elicit for Bayesian Network models that would help to distinguish between attacks and technical failures (Related to Chapter 5 in the thesis).
5. Critical infrastructure operators should think more proactively about reactive security.
6. As long as trust exists, social engineering attacks will be successful.
7. Water and words should be used with caution to avoid dire consequences.
8. Technological innovations should support people, but never completely replace them.
9. Social media are a double-edged sword for the scientific community. They help in dissemination of research findings, but they facilitate procrastination.
10. "No discussion during the scientific presentation" is a test result that will help to diagnose the problem "Audience did not understand the presented research".

These propositions are regarded as opposable and defendable, and have been approved as such by the promotors Prof. dr. ir. Pieter van Gelder and Dr. ir. Wolter Pieters, and copromotor Dr. André Teixeira.