VTT Technical Research Centre of Finland

Review of cybersecurity risk analysis methods and tools for safety critical industrial control systems

Alanen, Jarmo; Linnosmaa, Joonas; Pärssinen, Juha; Kotelba, Adrian; Heikkilä, Eetu

Published: 21/04/2022

Document Version
Publisher's final version

VTT
http://www.vtt.fi
P.O. box 1000FI-02044 VTT
Finland

RESEARCH REPORT

VTT-R-00298-22

Review of cybersecurity risk analysis methods and tools for safety critical industrial control systems

Authors: Jarmo Alanen, Joonas Linnosmaa, Juha Pärssinen, Adrian Kotelba, Eetu Heikkilä

Confidentiality: VTT Public

Version: 12.4.2022

VTT

beyond the obvious

Report's title Review of cybersecurity risk analysis methods and tools for safety critical control systems	
Customer, contact person, address SAFIR 2022 programme. Contact person: Programme Director, Dr. Jari Hämäläinen, VTT	**Order reference** SAFIR 7/2021
Project name Safety and security assessment of overall I&C architectures	**Project number/Short name** 126332 / SAFIR2022_SEARCH_2021
Author(s) Jarmo Alanen, Joonas Linnosmaa, Juha Pärssinen, Adrian Kotelba, Eetu Heikkilä	**Pages** 46
Keywords review, risk analysis methods, cybersecurity	**Report identification code** VTT-R-00298-22

Summary

In this report, we have reviewed cybersecurity risk analysis methods and tools. A specific focus is given to methods suitable for industrial control systems in the nuclear domain. For the review purpose, we developed a template for reviewing, but not for systematically comparing, the methods. Using the template, we reviewed twelve methods suitable for conducting cybersecurity or combined safety and security risk analysis. The methods to review were selected based on expert judgement after a literature review focusing on finding methods that are straightforward to implement in the context of nuclear power plant instrumentation and control systems. In addition to reviewing the analysis methods, the paper also includes a short review of a selected set of cybersecurity analysis tools. The main finding of the review was that the array of security analysis methods is vast, both separate methods and methods that also concern safety, but that the practices are not that well-established than with safety risk analyses, and more work is needed to determine the optimal security analysis methods in general or for each domain separately, such as nuclear power plant instrumentation and control systems. It is anticipated that several methods and tools are needed to comply with the stringent requirements and expectations set for a safety and security critical control system.

Confidentiality	VTT Public

Tampere 12.4.2022

Written by	**Reviewed by**
Jarmo Alanen Senior Scientist	Timo Malm Senior Scientist

VTT's contact address
VTT Technical Research Centre of Finland Ltd, P.O. Box 1000, FI-02044 VTT, Finland

Distribution (customer and VTT)

SAFIR2022 Programme
VTT Archives
Publicly available

Approval

VTT TECHNICAL RESEARCH CENTRE OF FINLAND LTD

Date:	21 huhtikuuta 2022
Signature:	DocuSigned by: Antti Pulkkinen D7E56E6C236F49D...
Name:	Antti Pulkkinen
Title:	Research Team Leader

Preface

This report has been written within the SEARCH project (Safety and security assessment of overall I&C architectures) in the context of the SAFIR2022 programme (The Finnish Research Programme on Nuclear Power Plant Safety 2019–2022). The SEARCH project for year 2021 consisted of several tasks of which this report relates to Task 1.4 (I&C security engineering methods and tools) of Work package 1 (Defence-in-Depth assessment of I&C architectures). The members of Task 1.4 were Jarmo Alanen (VTT), Joonas Linnosmaa (VTT), Juha Pärssinen (VTT) and Adrian Kotelba (VTT). The goal of Task 1.4 was to"…*try to find and study off-the-shelf tools that are specific to cybersecurity analysis, tools that could be utilised in cybersecurity threat analysis of nuclear I&C systems… [and] to find established cybersecurity analysis methods to be used instead of or as a complement to our STA method*." (An excerpt from the SEARCH 2022 project plan.)

The goal of this report is to provide the Nuclear Power Plant (NPP) community with presentation of alternatives to carry out security analyses or combined safety and security analyses of NPP Instrumentation & Control (I&C) systems. The goal is not to compare the different methods with each other, but only to present them.

Task 1.4 as well as the whole SEARCH project was steered by the SAFIR2022 Reference Group 2 (Plant Level Analysis).

The authors thank Henri Pirinen from Dovre Group for reviewing the earlier version of the report. Since that review, the presentation of the STPA-Extension method (Section 3.13) by Eetu Heikkilä (VTT) was added. Furthermore, the Pros and Cons sections of the methods were updated, and some grammatical errors were corrected.

This work was funded by the Finnish Research Programme on Nuclear Power Plant Safety 2019–2022 (SAFIR2022).

Tampere 12.4.2022

Authors

Contents

1. Introduction

At the same time as operational and information technologies join to permit remote and real-time access to plant operating data and control functions, the systems become gradually more vulnerable to cyber-attacks. Cybersecurity risk assessment and analysis is the root of information protection and cybersecurity risk management in companies of all domains. Generally, cybersecurity risk assessment identifies the various IT related assets that could be affected by a cyber-attack, identifies various risks that could affect them and evaluates their capability to defend the cyber environment of the organization. The cybersecurity environment comprises of humans (users), systems components, software, services, processes, and data connected directly or indirectly to networks. Goal of the cybersecurity risk management is to prevent and mitigate cybersecurity threats and vulnerabilities, thus reducing cybersecurity risks.

As a part of the risk assessment, a risk analysis, including identification and evaluation of risks, is performed. Conducting the cybersecurity risk analysis can be a complex process that requires considerable planning, special domain knowledge, and cybersecurity expert guidance. To help the process there are a wide range of cybersecurity risk analysis methods and tools available. These assessment methods often provide structured and guided ways to assess the strength of attackers (sometimes attributed by attacker capabilities, intention, and knowledge), the target system resistance (security arrangements classified by the system reachability, structure, and required attack tools) and the impact of a successful attack. With help of formal methods, the attacker strength and the system resistance can be combined to estimate the probability of a potentially successful attack. The attack probability and impact determine the criticality level of a security threat, which is also used to indicate the safety relevance of the threat [1].

It is important to select a proper analysis method for its purpose. Each one uses a certain approach to achieve its goal, requiring certain input material and a level of skill from the users. The selection of the method can be done, for example, based on comparisons and surveys done by other security practitioners or by the research community. Each survey or comparison is usually based on certain established comparison criteria, and can suggest suitable methods for different scenarios, domains, and lifecycle phases. This paper tries to contribute to support selecting cybersecurity analysis methods and tools for industrial control systems in nuclear domain. We reviewed cybersecurity risk analysis methods using an attribute-based template to present the methods in a commensurate manner. Even though not an easy target for attacks, as it requires quite specialized knowledge of the installed information technology (IT) and operational technology (OT), nuclear power plants (NPP) might be striking targets because of their strategic or tactical values.

The paper is structured as follows: this first chapter explains the motivation and goals of this research work. Chapter 2 presents studies and reviews done by other research groups in the recent past. In Chapter 3, we first present our template for reviewing the most relevant cybersecurity analysis methods for NPP instrumentation and control (I&C) systems and then present our review results. Some interesting off-the-shelf cybersecurity risk analysis tools are reviewed in Chapter 4. Finally, Chapter 5 concludes the paper with discussion about the overall findings of the study.

In this paper, we focus on cybersecurity, not security as a whole, such as physical access to a building. Hence whenever we simply write ‘security’, we mean cybersecurity.

2. State-of-the-art

Other research groups have made similar reviews, or surveys, about cybersecurity analysis methods and tools. In this chapter, we briefly go through some of the interesting studies by other groups. Agrawal [2] made a comparative study of four cybersecurity risk analysis methods, CORAS, CIRA, ISRAM and IS (the first two are qualitative methods; the last two are quantitative methods). He presents a table which compares these methods with the following attributes: methodology, purpose, input, effort, outcome, scalability, pros and cons. They conclude, for instance, that if the IT standards need to be strictly followed, CIRA and IS methods are not viable choices, and if the requirement is to get a quantitative risk level estimation instead of subjective classification, ISRAM is a suitable candidate. For the comparison, he also utilizes the Campbell [3] classification scheme. In another study, Kriaa et al. [4] provides a survey of existing approaches to industrial facility design and risk assessment that considers both safety and security. They identified over 40 different approaches supporting risk co-analysis and classified them according to their place in the system lifecycle. Their interest was particularly the capability to identify and treat interdependencies between safety and security.

From the cybersecurity risk analysis tool point-of-view, there also exists academic studies. For example, a recent study by Roldán-Molina et. al [5], where they focused on the evaluation of tools available for risk assessment and decision making in the cybersecurity domain. They evaluated 9 tools, Nessus Home, Saint8, EyeRetina, GFILanguard, nCIRCLE IP30, Security System Analyzer, OpanVAs, QualusGuard and Nexpose. These all are tools connected to a company's ICT network, and they collect detailed data about the infrastructure. These tools utilize cybersecurity metrics, standards, protocols, and strategies to identify, understand and anticipate potential cybersecurity threats. Most of the tools use Common Vulnerability Scoring System (CVSS) standard for their metrics.

In safety critical systems, poor cybersecurity is one potential source of safety incidents. Hence it is advisable to carry out safety and security co-analysis, either by using a uniform risk analysis method or by integrating the separate safety and security risk analyses processes in one way or the other; an example of the former is the FMVEA method [6] and the unified security and safety risk assessment procedure by Chen et al.[7], and of the latter the hybrid risk assessment information ontology by Alanen et al. [8] and the UFoI-E method by Guzman et al. [9]. Kavallieratos et al. [10] carried out a comprehensive survey to compare 68 different safety and security co-analysis methods. They evaluated the methods against a list of attributes and characteristics that describe the properties of each method in a comparable manner; the comparison criteria by Kavallieratos et al. [10] are listed below:

- type of joint analysis: unified vs separated but integrated
- modelling type: graphical vs formal, or both
- based on safety / security standards and utilizes them: Yes vs No
- application domain: CBS and/or Internet-Of-Things (IoT) and/or automotive and/or control systems
- approach: quantitative vs qualitative
- ensures: safety vs security or both
- lifecycle: requirements capture and/or risk analysis and/or generic (any phase)
- involved stakeholders: safety experts and/or security experts and/or developers and/or designers and/or user or system experts.
- applies systematic and structured process: Yes vs No
- scales well: Yes vs No

- stimulates creativity among stakeholders: Yes vs No
- provides models and other to augment communication between different stakeholders: Yes vs No
- facilitates identification and analysis of conflicts between safety and security goals: Yes vs No
- software tool to apply the method exists: Yes vs No.

The comparison criteria above also provide a good set of selection criteria for a company to establish safety and security risk co-analysis methods. Kavallieratos et al. [10] found that despite the fact that the proposition of safety and security co-analysis has been studied for decades, there still are open issues to be studied and solved. They mention the following topics needing further studies and development:

- resolving conflicting results from safety and security risk analysis should be supported better;
- a standard, application independent, methodology for safety and security co-analysis should be provided;
- evaluation and validation of the developed methods should be done more diligently and against comparable criteria;
- to support industry to apply the existing safety and security standards in context of safety and security co-analysis, the standards should be revised to resolve ambiguities between them;
- a wider range of application domains should be covered; currently transportation domains seem to be best supported;
- the risk analysis methods should better cope with the dynamic nature of Cyber-Physical Systems (CPS);
- the methods should provide the advantages of both graphical (and qualitative) and formal (and quantitative) modelling;
- the methods should be more holistic to cover the human aspects and ecosystem of the sociotechnical CPS. [10]

Based on this observation by Kavallieratos et al. [10] we can state that there is no single method to optimally satisfy all the expectations for an effective, easy to use, and cost effective safety and security co-analysis. In the next chapter, Chapter 3, we will present some interesting safety and security co-analysis and security analysis methods for safety critical industrial control systems, especially for nuclear power plant I&C systems.

3. Cybersecurity analysis methods for ICS

During the study, we interviewed Finnish nuclear industry stakeholders about their current practices and future wishes but did not get much input for the selection process, simply due to confidentiality reasons. Hence, through an extensive search, we selected methods that we foresee, based on expert[1] judgement, to be applicable and straightforward to implement for cybersecurity risk analyses of NPP I&C systems. We have included in the review such methods that support safety and security risks co-analysis, but also methods that are intended solely for cybersecurity risk analysis. The initial literature search included some tens of possibly interesting methods, from which we selected the most suitable ones to be included in this paper.

The reviewed methods are:

- FMVEA (Section 3.2)
- Methodology for vulnerability assessment using Attack Trees (Section 3.3)
- Risk and vulnerability analysis by Aven (Section 3.4)
- Integrating cybersecurity into LOPA (Section 3.5)
- STA (Section 3.6)
- Cyber PHA (Section 3.7)
- STRIDE and DREAD (Section 3.8)
- UFoI-E (Section 3.9)
- CCE, Consequence-driven, Cyber-informed Engineering (Section 3.10)
- Cyber Security Argument Graph (Section 3.11)
- PRISM (Section 3.12)
- STPA-Extension (Section 3.13).

We reviewed the methods using a template, which is presented below in Section 3.1.

3.1 Template for the study

To make the review of each cybersecurity risk analysis methods commensurate with each other, we created a structured template to guide the review and to report the results. The template is presented below in Table 1.

[1] The expertise is based on long experience with both safety and security risk analysis methods and practical risk analysis work, and on our long history with Nuclear I&C systems research.

Table 1. Template to study and review the cybersecurity risk analysis methods.

Guideword / Title of the sub-section	**Topics to consider, study and report**
Description	A short description of the risk analysis method such that it does not address the details that are described in the later chapters
Scope	Purpose and scope of the risk analysis method; in which life cycle stage of the system-under-analysis the method is planned to be used
Analysis method characteristics	Is the method bottom-up or top-down method; is it systematic; is it based on guideword lists, such as threat and vulnerability type lists or to observed threats and vulnerabilities; is the method mathematically formal; is it qualitative or quantitative or both
Maturity	Is the method proven in use or otherwise mature enough to be trusted in NPP:s
Standard based	Is the method based on a standard; is the method published as a standard
Applicability	Is the method only academic or is it used in industry; where used; is it suitable to nuclear industry
Software tool availability	Are there tools available to carry out analysis based on the method; is it is easy to carry out a risk analysis according to the method by using standard tools, such as a spreadsheet tool
Future prospects	Is the method still living (what is the latest reference); future plans as written in the corresponding literature; our estimation about the future
Pros and cons	What are the pros and cons the author of the method considers, or others see, or we see

Some of the attributes and characteristics by Kavallieratos et al. [10], presented in Chapter 2, are somewhat overlapping with our template in Table 1, but our template is more targeted for structuring the presentation of the methods, and is thus not as formal as the study by Kavallieratos et al. [10], which is targeted for systematic comparison of the methods.

3.2 FMVEA

3.2.1 Description

FMVEA (Failure Modes and Vulnerabilities Effect Analysis) [6] is a safety and security analysis method based on the traditional Failure Mode, Effects and Criticality Analysis (FMECA) [11] and on the STRIDE threat model [12]. It interprets the FMECA cause-effect chain, *failure cause – failure mode – failure effect – failure severity & failure probability – failure criticality,* to corresponding security threat cause-effect chain as follows: *vulnerabilities – threat agent – threat mode – threat effect – attack severity & probability – threat criticality*. The main distinctive difference in the cause-effect chains is the introduction of ‘threat agent’ in the threat chain. The rationale for the ‘threat agent’ factor is trivial: for failures, there is no active, intelligent, agent that deliberately causes the failure mode, whereas the security threat modes are always triggered by a threat agent, i.e., an attacker, that exploits the vulnerabilities of the system. Another difference between the FMVEA safety and security analyses is in the evaluation of the probability of the threat mode. Again, the difference is caused by the deliberate nature of the security threat modes. The threat probability is a sum of threat agent properties ‘motivation’ and ‘capabilities’ and system susceptibility properties ‘reachability’ and ‘unusualness’; in FMECA, the probability is simply given as a probability of occurrence (which can in some cases be calculated from the failure rates) or as a combination of the probability of occurrence of the failure modes and the probability to be able to identify and eliminate the failure before it propagates to a harm.

To provide a view of the system under analysis for FMVEA, a functional analysis is done. As a result of the functional analysis, both the system functions (a functional break-down structure) and the system elements (components and/or sub-systems) and their interconnections are identified, and allocation of the system functions onto the system elements is showed up. Thereafter the effects of the failure modes and threat modes to the function(s) of each system element separately is analysed.

3.2.2 Scope

FMVEA is aimed for industrial software intensive control systems, including complex mission critical systems. Its objective is to provide an equal method to identify both safety and security threats and to assess their criticality. Hence FMVEA is a system analysis tool to make decisions about the system design, but it can also be used as a conformity assessment tool to verify and validate the design. Schmittner et al. [6] express the scope of FMVEA as follows: "…FMVEA is best suited for a qualitative high-level analysis of a system in the early design phases."

3.2.3 Analysis method characteristics

FMVEA is based on FMEA, which is a systematic, bottom-up, analysis method, based on systematic list of system elements failure modes, the effects and criticality of which are systematically assessed by the analysis team. Compared to a typical FMEA analysis flow, an additional aspect, namely 'threat agent' (attacker), has to be considered during the analysis of security threats.

Although the attack probabilities are counted as a sum of four attack properties, attacker motivation (1-3), attacker capabilities (1-3), system reachability (1-3) and system unusualness (1-3), FMVEA is qualitative in nature, not quantitative, despite the claim by Schmittner et al. [6] that the probability assessment of FMVEA is semi-quantitative. The values 1-3 of the attack properties have no correspondence to any real-world observance or assumption (such as statistical probabilities); the property values could as well be manifested with any values or even letters or words.

For the identification of the threat modes, STRIDE [12] threat model is used.

3.2.4 Maturity

Although FMVEA is rather new (Schmittner et al. paper [6] is from 2014), the method can be considered mature due to the fact that it is heavily based on the very mature FMEA, which is standardised by IEC 60812 [11].

3.2.5 Standard based

As FMVEA is based on traditional FMEA, it is from that sense based on IEC 60812 [11] (Schmittner et al. [6] refer to the standard). On the other hand, the FMVEA method as a whole – with all the security threat analysis related additions – is not based on any standard. In fact, Schmittner et al. [6] claim that there is no standard which "considers both safety and security equally".

3.2.6 Applicability

Like FMEA, FMVEA is a general-purpose method and fits therefore for any kind of safety and security critical systems, including NPP I&C systems. The developers of the method apply the method for safety and security analysis of intelligent and cooperative vehicles in [13] and of railways systems in [14]. Currently there is no reference about further industrial use, but it does not mean that it is not used by industrial companies; they typically keep the security control activities secret. Despite the academic origin of the FMVEA method, the fact that it is based on the industry proven FMEA makes it well applicable to safety and cybersecurity risk analysis of industrial systems.

3.2.7 Software tool availability

Like FMEA, FMVEA can be carried out using a simple spreadsheet table. Hence it is not expected that a dedicated SW tool will emerge, although a tool with dynamic selection lists for failure and threat modes, vulnerabilities etc. would facilitate the analysis work a lot; lists of vulnerabilities could, for example, be retrieved from the CWE (Common Weakness Enumeration) vulnerability lists [15] hosted by CWE Community (which is hosted by MITRE Corporation).

3.2.8 Future prospects

In [13], Schmittner et al. plan to extend the FMVEA method to model and analyse multi-stage attacks. They also plan to go beyond the STRIDE generic threat mode catalogue to build a catalogue of more specific threat modes such that various industrial domains are covered, especially cyber-physical and intelligent systems.

Dobaj et al. [1] (Schmittner also included), in 2019, published a paper in which they wrote about combining several popular security risk assessment methods (FMVEA, SAHARA, FAIR and Diamond model of intrusion analysis) as an effort towards "*integrated quantitative security and safety risk assessment*". They want to map the classifiers described by the two integrated risk analysis methods SAHARA and FMVEA, into the diamond model that has its origin in the field of security incident analysis.

3.2.9 Pros and cons

FMVEA provides an integrated analysis method for safety and security. Since FMVEA inherits the analysis practise from FMEA, it is easy to adopt by anyone familiar with FMEA (which is easy to adopt). FMVEA is a systematic method.

FMVEA, as well as FMEA, does not identify hazards caused by several causes; hence more complex attack modes cannot be identified with the method [6]. Therefore, Schmittner et al. [6] considers FTA with attack trees (such as [16]) as a complement to FMVEA to discover complex attack modes. Furthermore, Peischel et al. [17] compare FMVEA with analysis based on attack patterns of misuse cases. The comparison was done in a student experiment to let the students try both methods to identify security risks of a web application. The result of the experiment was that the method with attack patterns of misuse cases provided a better set of security test cases that also more comprehensively covered the security requirements.

3.3 Attack trees

3.3.1 Description

Attack trees are a well-known method for modelling attack scenarios and evaluating the security level of systems. They are considered an extension from their safety counterpart, the fault trees. While both are more used in their respective disciplines, they can also be combined to support a hybrid analysis, for example as presented by Steiner and Liggesmeyer in [16], in which component fault tree (another extension of fault trees) are extended by attack trees, which model attacks that can cause security events in the fault tree.

A formal way to carry out attack tree analysis in combination with fault tree analysis is to use BDMP (Boolean logic Driven Markov Processes) modelling formalism introduced by [18] and applied to security threat modelling by [19] and developed for combined safety and security analysis by [20]. BDMP combines traditional fault-trees with Markov models to take advantage of the modelling easiness of fault-trees and modelling power of Markov models, especially dynamic modelling, which allows taking into account component dependencies [18]. EDF company has developed tools to support BDMP based analysis. The tool to create BDMP models and quantitatively analyse the probabilities of the top event scenarios is called KB3 platform [19,20]. Commercial availability of KB3 could not be verified, but at least a demo version is available [21]. Another formal method to carry out safety and security related fault tree analysis is presented by Roth & Liggesmeyer [22]. They present a method to amplify the state/event fault trees (SEFTs) [23] with security aspects (i.e. attacker model) to treat safety and security equally in a single, uniform process.

Another method utilizing attack tree is described by Ten et al. [24–26]. They propose an analytical method to measure a probability, what they call ‘vulnerability index’, of a potential cybersecurity intrusion scenario to an interconnected system. Their method uses attack trees to calculate the currently most vulnerable component of a system based on the selected intrusion scenario and the related attack vectors (a.k.a. leaves). It also gives an overall vulnerability index for the whole system against the selected intrusion scenario.

As Schmittner et al. [6] suggest, FMVEA could be complemented by attack trees (such as [15]) to discover complex attack modes.

3.3.2 Scope

Bruce Schneier [27], in the year 1999, presented the attack trees for modelling the security of a system by considering a security breach as an attack goal and describing it with a set of events that lead to the goal in a combinatorial way. Since then, attack trees have become a widespread technique of mathematically and visually representing the sequence of events that lead to a successful cybersecurity attack. Attack trees can be applied basically in any domain which has to deal with cybersecurity vulnerabilities. Attack trees are aimed to assess the probability of an attacker accomplishing an adversary action and harming the system in some way.

3.3.3 Analysis method characteristics

According to [28], attack trees can be considered as a somewhat systematic top-down way of characterizing diverse system threats, with intuitive representation of possible attack and possibility of formal mathematical frameworks for analysing them both in qualitative and quantitative manner. These trees can provide a formal method to describe how varying attacks, modelled as leaf nodes of the tree, harm the overall security property of a system. This property is modelled as the root node of the tree, connected via logical gates with its leaves.

For example, for the method by Ten et al. [24] three parameter (called conditions) values are needed (the paper guides how to determine these a numerical value based on a selection list):

- evidence (or lack of) of attempted intrusion,
- technological countermeasures,
- password policy enforcement.

The usefulness of the methods seems to heavily lean on a prior information about the parameters above. List of intruder scenarios and security vulnerabilities (leaves of the attack tree) are also needed to calculate the probabilities from the attack tree. The paper does not mention any systematic ways to find these.

3.3.4 Maturity

Attack trees have been used for decades in research and industry. However, there is little empirical or comparative research which evaluates the effectiveness of these methods, according to [29].

3.3.5 Standard based

Lallie et al. [29] studied in their review paper, that even despite their popularity, there is no standardised way of represent an attack graph with a visual syntax configuration, and they found more than seventy different configurations described by the literature, where each of which presents attributes such as preconditions and exploits in a different way. They conclude that their survey demonstrates that there is no standard method of representing attack graphs or attack trees and that more research is needed to standardise the representation.

3.3.6 Applicability

Attack tree is a general method for modelling threats against basically any system and describing the security arrangements of the system, against such attacks. Based on literature, they have been used in a variety of applications during the years, including industrial control systems (e.g., in [30]), even safety critical I&C systems and nuclear domain (e.g., in [31,32]). Thus, they are also applicable in our focus.

3.3.7 Software tool availability

The attack tree method itself, in general, can be quite simple and be done with basic tools. However, if the attack trees are large (as with complex system they usually are), the calculation of the different probabilities takes a lot of effort and will need some computing software to be effective, especially if it is developed into an optimization problem to solve the pivotal leaves for security improvements to avoid exhaustive manual search. Tool support is available, both commercial (such as Secur/Tree by Amenaza, AttackTree by Isograph and ATA by ENCO) and open source (such as ADTool by Cornell University and SeaMonster by the SeaMonster SourceForge project) (usually Eclipse-based).

3.3.8 Future prospects

The research topic of attack trees is active and is foreseen to continue in the future as well, just during the year 2021 there have been hundreds of new research papers published regarding attack trees. They are under extensive research and development activities by wide range of research groups, examples of the latest ones are e.g., in [29,33]

3.3.9 Pros and cons

Attack tree is one of the most used model for information security assessment, relatively intuitive and simple to learn, while still having formalized basis and quantitative analysis means [28] for cybersecurity vulnerability assessment to find out the most obvious and vulnerable access points for attacks. Attack trees are illustrative and describe well the effect of multiple causes.

In practical industrial applications, attack trees largely remain a tedious and error-prone exercise with noticeable time investment for the tree design and analysis [28]. They also often do not cover the temporal aspects of the attacks, i.e., in which sequence the attack leaves are penetrated in the scenario.

List of intruder scenarios and security vulnerabilities (leaves of the attack tree) are also needed to calculate the probabilities of security events from the attack tree, but the acquisition of input data can be difficult and tedious [28]. This is quite a well-known problem regarding the trees. Another analysis before Attack trees may be needed.

The method guides as how to calculate the final probabilities with the help of formed attack tree. Formulating the wanted tree layout is also left for the user to decide, which is another current weak spot of the trees, the absence of empirically founded best practices for designing the tree [28].

3.4 Risk and vulnerability analysis by Aven

3.4.1 Description

In his paper [34], Aven defines a combined safety and security analysis method that focuses on uncertainty analysis of the assumed consequences of hazards and threats. The method is based on assessing the probability of attacks based on uncertainties of the real observable quantities related to a potential attack. The flow of the analysis method goes as follows:

- Identify the system or service under analysis, its functional and performance requirements; the relevant performance measures produce the observable quantities, the uncertainties of which will affect the determination of the risk probability factor. This step makes it possible to identify the vulnerabilities of the system or service under analysis.
- Identify the relevant security threats and safety hazards and their causes (the threat and hazard scenarios); analysis methods such as HAZOP and FMECA can consulted to facilitate the identification.
- Perform an uncertainty analysis to assess the uncertainty of the determined risk probability.
- Perform consequence analysis such that the uncertainties quantified in the previous step are considered; analysis methods such as ETA and FTA can be utilised here supported by vulnerability check lists (which are also relevant to the uncertainty analysis); consequence analysis can utilise the risk classification scheme developed by Klinke and Renn [35] and modified by Kristensen et al. [36], where the consequences are characterised by eight categories to broaden the consequence analysis

to go beyond the typical consequence analysis in which simply the impacts to costs, income, production volumes, deliveries, loss of lives, etc. are determined.

- Describe the identified risks and vulnerabilities summarising the results of the analysis phases and providing the overall risk assessment results with the classification of the risk level, which can be determined by diverse ways, e.g., using traditional consequence – probability matrix or using a consequence – uncertainty matrix; note that uncertainty is not same as improbability (i.e., 1 - probability), but reflects the uncertainty of the probability of the determined consequence.

3.4.2 Scope

The risk analysis method by Aven [34] is developed for critical infrastructure systems, such as electrical grids to provide decisions support. Hence it falls into the category of system analysis methods, not determination methods to provide evidence for the conformity assessment.

3.4.3 Analysis method characteristics

The analysis method is more of a bottom-up method (mentions, for example, FMECA, HAZOP and ETA), but mentions fault trees as a method to identify possible scenarios that lead to the identified events (hazards and threats); fault tree (FTA) is a top-down analysis method. The analysis method uses a list of conceptual vulnerability attributes by [37] with which the actual vulnerabilities for the system under analysis can be identified. The method is characterised by emphasizing the uncertainties of the observable quantities that have been used to determine the probability of the negative impact (i.e., the top consequence).

3.4.4 Maturity

Aven's risk analysis framework uses (or can use) mature analysis methods, such as FMECA, HAZOP, FTA and ETA, to identify hazards and threats and to analyse their consequences. From that perspective it has mature elements, but the uncertainty analysis is not so well known in industry. Also using the list of conceptual vulnerability attributes by [37] and the risk classification scheme by Klinke and Renn [35] (and modified by Kristensen et al. [36]) would require some learning period from a typical safety engineer prior to productive risk assessments.

3.4.5 Standard based

The analysis framework is not directly based on a standard, but applies standardised analysis methods, such as FMECA, HAZOP, FTA and ETA.

3.4.6 Applicability

The author of the risk analysis framework, Terje Aven, is from the University of Stavanger. Hence the method can be considered to have an academic origin, but with clear industrial goal, especially in infrastructure systems, such as electrical grids. Thus, its applicability to nuclear power plant is good, especially due to the profound vulnerability analysis and assessment of the uncertainties of the estimated probabilities of negative impacts.

3.4.7 Software tool availability

There is no hint about availability of software tools that fully implement the Aven's risk analysis framework, but the framework can use commercial FMECA, HAZOP, FTA and ETA tools, and typical office software applications, in its various phases.

3.4.8 Future prospects

No plans for Aven's method could be found. Even though Aven's method was published in 2006 there still is no hint of wider industrial acceptance; this makes us assume that the method is not developing nor spreading well.

3.4.9 Pros and cons

The Aven's method considers several aspects and integrates multiple analysis methods. Partly due to that, the method is somewhat complex, laborious, and difficult to describe and learn for a typical safety engineer, especially due to the uncertainty analysis. But on the other hand, attacks to infrastructure systems and their consequences are complex and are prone to compromise national security. Hence there is a good motivation to learn a more complex analysis method.

3.5 Integrating cybersecurity into LOPA

3.5.1 Description

In their article, Cormier & Ng [38] introduce a method for integrating cybersecurity vulnerability analysis as a part of Layers of Protection Analysis (LOPA), to systemically evaluate and monitor process control networks and the instrumented safeguards to identify potential weaknesses and to ensure the safeguards against cyber threats. Similar study for integrating cybersecurity into LOPA has been also done in a very recent article by Tantawi et al. [39], they call their method Cyber LOPA (CLOPA).

LOPA as a method itself is a generic risk analysis technique that provides estimates for event likelihoods along various points throughout the incident scenario. So, in a sense, adding security analysis as a part of LOPA is not a new idea.

3.5.2 Scope

The scope of the method is in process plants and control networks. In their paper, Cormier & Ng argue that traditional, currently widely used, safety hazard and risk analysis methods could and should be further adapted to identify and assess vulnerabilities of process plants against cyber-attacks.

For example, in a process plant, LOPA is usually performed after the Process Hazard Analysis (PHA) or Hazard and Operability study (HAZOP), in which the PHA or HAZOP teams have identified some scenarios requiring further analysis to make sure risk are manageable. Now, in this closer, more careful assessment, LOPA team might also include security experts to consider possible cyber-attacks in the scenarios and the evaluate the existing cybersecurity safeguards of the system under analyses.

Furthermore, they also suggest that integrating cybersecurity more closely together with the other elements of process safety management (PSM) (apart from safety analyses), could make process industry more resilient against both traditional and cyber threats.

3.5.3 Analysis method characteristics

According to authors of [38], the security LOPA can be considered as a semi-quantitative, bottom-up analysis. In addition to the interesting possibly hazardous scenarios, it requires certain other information to be available for conducting the analysis. Severity of consequences in terms of multiple impact categories are needed, as well as the likelihoods of different initiating events of cyber-attacks and availabilities of existing Independent Protection Layers (IPL) to determine the overall expected risk, which is then assessed using company's own risk acceptance criteria. The paper itself does not guide where these lists or values might be attained.

3.5.4 Maturity

Layer of Protection Analysis (LOPA) is a mature method, with plenty of guidance and consultancy available. According to [40] the use of LOPA started in the chemical process industry already in the late 1990s. Since then, it has become one the many analysis methods available for assessing a given scenario to determine if the risks involved are acceptable. An order of magnitude technique is used to evaluate the adequacy of existing or proposed layers of protection against known hazards.

The use of LOPA for cybersecurity analysis is much newer idea in the light of scientific publications. The Cormier & Ng article [38] referenced in this paper is new, from 2020, and has only 2 citations and only work as an overview to the principles of security LOPA; it is clearly not a guide as to how to conduct the assessment. There is no evidence that the method presented has been used for industrial case, the example in the paper seems to be fictitious.

3.5.5 Standard based

Usually using LOPA is connected to the safety standard IEC 61511, which itself does not specify LOPA, but LOPA is a very common method to fulfil the analysis requirements of the standard. However, there is not yet any such strong connections to standards from the security point-of-view to using LOPA as an analysis method for evaluating security safeguards.

3.5.6 Applicability

We see security LOPA applicable to industrial cases; the method is based on LOPA method already much used in the process industry. However, the paper by Cormier & Ng is quite a brief introduction to the ideology of their method and requires thus more in-depth treatment with practical examples and methods of integration; it seems that is left for the readers to do.

3.5.7 Software tool availability

The papers [38,39] do not hint at any readily available tools to conduct specifically the security related LOPA. However, there are varied models or templates available for conducting the traditional LOPA, and it should not be a big issue using these tools also to perform security related LOPA.

3.5.8 Future prospects

Previously, in 2018, Cormier & Ng (the authors of the method discussed here) have published another paper [41], in which they consider PHA and HAZOP from the security point-of-view. It seems like LOPA is one of those quite many risk analysis methods, which are getting the treatment of being more and more influenced by cybersecurity aspects, as security risks are growing. It is likely that this trend is going to continue in the future with LOPA as well.

3.5.9 Pros and cons

As the authors of the method consider, traditional hazard and risk analysis methods should be adapted to identify and assess vulnerabilities of process plants against cyberattacks. Using already existing methods and concepts such as IPLs (Independent Protection Layer) and SILs (Safety Integrity Level) it might be easier for cybersecurity to become more tightly knit as a part of the already existing risk management and Process Safety Management (PSM) elements of the company. Nevertheless, the security SL (Security Level) concept used by IEC 62443-3-2 [42] is not mentioned.

The method systemically evaluates and monitors process control networks and the instrumented safeguards to identify potential weaknesses (vulnerabilities) and to ensure the safeguards against cyber threats. All safeguards are considered.

As said, the idea of combining security as part of safety LOPA is good, and we, the authors of the paper, fully agree that safety and security assessment cannot be carried out independently. However, the methods presented here still needs further treatment to be fully useable. Other analyses are needed to identify all the relevant threats.

3.6 STA

3.6.1 Description

Security Threat Analysis (STA) method is developed by VTT [8]. It resembles HAZOP (Hazard and Operability study), or guideline based PHA (Preliminary Hazard Analysis) but is aimed at cybersecurity risk analysis.

STA does not require a certain risk assessment procedure to be followed, but STA is data driven in the sense that it exactly specifies the information items (and their relations) related to a risk assessment task. Nevertheless, the risk analysis is expected to be started either by using a list of the vulnerability types or threat types as guidewords to identify the system specific cybersecurity threats.

3.6.2 Scope

STA is targeted to be used in cybersecurity risk assessments of I&C (Instrumentation and Control) system in early design phase, i.e., the phase ZCR-2 (Perform an initial cyber security risk assessment) of IEC 62443-3-2 [42], but is expected to be applicable in the phase ZCR-5 (Perform a detailed cyber security risk assessment), too. The initial target has been NPP I&C systems, but STA is not restricted to nuclear domain; machinery automation, for example, is another suitable domain for STA.

3.6.3 Analysis method characteristics

STA is based on a pre-defined lists of vulnerability types according to NIST SP 800-30 [43] and threat types according to ISO/IEC 27005 [44] that are used as the guidewords to identify the system specific cybersecurity threats. The demonstrations of STA apply the risk matrices of Annex B of IEC 62443-3-2 [42], but any risk estimation method is allowed to determine the level of an identified risk.

If a risk analysis is started from vulnerabilities, STA can be regarded as a bottom-up method, but if started from threat types, STA is neither bottom-up nor top-down method but starts from the middle of the harm scenario identifying causes to the bottom direction and consequences to the top direction.

3.6.4 Maturity

The method is new. It is tested only in one artificial NPP I&C case [8] and in one real world machinery automation case (not published). The method is thus immature, but due to its similarities with HAZOP and PHA, it inherits some maturity from the safety risk analysis practices.

3.6.5 Standard based

STA exploits the standards, IEC 62443-3-2 [42] and NIST SP 800-30 [43], ISO/IEC 27005 [44] as explained above in sections 3.6.2 and 3.6.3, but is not claimed to be standards compliant.

3.6.6 Applicability

Although Section 3.6.4 mentions two application domains, NPP I&C and machinery automation, STA has the same broad application field as that of IEC 62443-3-2 [42], i.e., any type of industrial automation and control system. Although STA has been created by a research institute, it has been presented in a way that makes it easy to adopt by security engineers of industrial companies.

3.6.7 Software tool availability

There are no specific commercial STA software tools available. The two demonstrations mentioned in 3.6.4 apply Polarion REQUIREMENTS (the NPP I&C case) and a proprietary database-based tool by the machinery automation company. STA can be implemented onto any platform that provides a structured way to store information such that the relations between the information items support traceability features, such as impact analysis (i.e., it provides suspect indication of the related information items if an information item is updated).

3.6.8 Future prospects

According to [8], in future, STA method is planned to be tested relating to the scalability and exhaustiveness of the method, and to automatic generation of risk assessment documentation, and to implementing STA with other off-the-shelf tools.

3.6.9 Pros and cons

STA is a very new method with very thin experience, for example, about its exhaustiveness. Nevertheless, STA considers well and systematically vulnerabilities and threats. It is scalable. Its advantage is that it resembles safety analysis methods which are familiar to safety engineers and is thus easy to adopt by novice security engineers that come from the safety discipline. On the other hand, that is also a disadvantage; security engineers may find well established security analysis methods and tools, such as MITRE offering, more appropriate.

Events with multiple causes may be difficult to detect.

3.7 Cyber PHA

3.7.1 Description

Cyber PHA[2] is HAZOP-like method to assess cybersecurity risks of industrial process automation [45]. In principle, Cyber PHA risk assessment workflow has two main phases, assessment of the vulnerabilities (and gaps) and assessing the risks (threats, consequences, and risk level) with risk control planning. For the vulnerability assessment, the system under assessment is documented to elicit the system and network architecture and data flows. After identification of the vulnerabilities, the system is partitioned into zones and conduits (according to IEC 62443-3-2) to support the actual risk assessment by providing a list of vulnerabilities per zone. Thereafter the risk assessment is carried out by first studying the results – especially the potential harms identified – of the former safety risk analyses, such as PHA and LOPA (Layers of Protection Analysis). The Cyber PHA workflow continues in workshops, in which the security threat scenarios are identified, the existing risk controls are documented, and new ones are recommended, and the risk level is estimated using a typical two-dimensional risk matrix. After the workshop, the new risk controls are determined and prioritised. [46,47]

3.7.2 Scope

The scope of Cyber PHA is process automation, but it is suitable, due to its HAZOP-like nature, for other domains as well.

3.7.3 Analysis method characteristics

Cyber PHA is safety oriented in the sense that it focuses on safety and environmental consequences of security threats. Cyber PHA workflow is similar to HAZOP studies and can thus be regarded to be a systematic method, although it doesn't seem to be based on a fixed list of guide words to identify the threats; nevertheless, it is assumed here that the list of vulnerabilities identified and registered into a vulnerability register works as a source of reusable 'guide words' for further analyses.

3.7.4 Maturity

Compared to HAZOP, FMECA and other well-known analysis methods, Cyber PHA is rather young method, but as its workflow resembles the typical risk assessment workflow familiar from the safety analyses, it is easy to adopt, and it provides a natural complement to them to cover security risk assessments in a similar manner. Furthermore, Cyber PHA has been used in industrial context, especially

[2] PHA here means Process Hazard Analysis, not Preliminary Hazard Analysis.

in process industry, such as chemical industry [48]. Cyber PHA can be thus considered mature enough for industrial use without further development.

3.7.5 Standard based

Cyber PHA is based on IEC 62443-3-2 [42]. In fact, we could say it vice versa: IEC 62443-3-2 is based on Cyber PHA. This is because the father of Cyber PHA, John Cusimano, was the chairman of the IEC 62443-3-2 standard, and he writes that Cyber PHA "*…is documented in the IEC 62442-3-2 standard*" [45].

3.7.6 Applicability

Cyber PHA does not have an academic flavour, but was created with industrial objectives, especially for process industry, such as petrochemical industry. The authors of this paper do not see any hinderance to use it in context of NPPs, especially because it resembles the STA method (see Section 3.6), which was created for NPP I&C systems.

3.7.7 Software tool availability

The former employer (aeSolutions) of the author of Cyber PHA (John Cusimano) used to offer a service to carry out Cyber PHA risk assessments. But now that the division responsible for Cyber PHA was acquired by Deloitte, the future of Cyber PHA service there is unknown (see Section 3.7.8). However, Exida another previous employer of John Cusimano, offers a tool called exSILentia Cyber that includes a tool called CyberPHAx, which implements Cyber PHA [49]. The demonstration of exSILentia Cyber [50] provides a good overview, not only about the tool, but also about the Cyber PHA.

It seems that Cyber PHA could be implemented to some extent using a generic spreadsheet or database software tool.

3.7.8 Future prospects

Just recently (Summer 2021), Deloitte company acquired the aeCyberSolutions division (the host of Cyber PHA services) of aeSolutions. It is assumed here that Cyber PHA service will be offered by Deloitte, but currently CyberPHA is not explicitly mentioned on their web site. Hence the future of Cyber PHA is somewhat unsure.

3.7.9 Pros and cons

The advantage of Cyber PHA is that it resembles safety analysis methods which are familiar to safety engineers and is thus easy to adopt by novice security engineers that come from the safety discipline. On the other hand, that is also a disadvantage; security engineers may find well established security analysis methods and tools, such as MITRE offering, more appropriate. Cyber PHA is good for identification of risks, but other analyses may be needed to identify complex scenarios.

3.8 STRIDE and DREAD

3.8.1 Description

STRIDE [51], developed by Microsoft in the late 1990s, is a practical and simple model for threat analyses. It is used to help reason and find threats from a system and to expose possible security design flaws. The name comes from the initials of the method’s six threat classification categories: **S**poofing of user identity, **T**ampering, **R**epudiation, **I**nformation disclosure, **D**enial of service, and **E**levation of privilege. STRIDE is one of the most often referenced and widely used source for threat modelling/classification.

STRIDE is often used in conjunction with DREAD [51], another method by Microsoft. DREAD, which stands for **D**amage, **R**eproducibility, **E**xploitability, **A**ffected Users, and **D**iscoverability, is used to rate, compare and prioritize the severity of risk presented by threats. In other words, it does risk evaluation, whereas STRIDE does threat identification. It is a flexible method, which uses the five categories to guide the evaluation work. The aim is the to give each threat a numerical value based on the categories and thus discover the most potent threats.

3.8.2 Scope

STRIDE is used to describe a set of threat scenarios as vulnerabilities in a system under analysis, while DREAD can be used to evaluate the severity of these threats. The system under analysis can practically be any system from any domain, as long as it has some of properties that can be exploited by a possible attacker. Thus, there is no specific scope, but usually they are used in a context of software intensive systems.

Since STRIDE and DREAD are originally, and often used, for software system design, they are by nature data-centric, but this does not mean they cannot be used for other contexts. They are useful both in the design and operation phase of the system lifecycle but are more aimed to be used during the design phase. They are best when used in the early design phase, as is the case with most of the risk analysis methods, when it is relatively easy and cost-effective to resolve potential security issues.

3.8.3 Analysis method characteristics

STRIDE as a method does not define a formal model for threats classification, and thus does not aim for completeness, but is useful, practical, structured and cost-effective methodology to uncover threats. It can be considered to be a top-down method of finding vulnerabilities in the system, by starting from the scenarios and working down to the system components causing potential problems. Practically STRIDE is a qualitative checklist to work through the system under analysis.

In STRIDE, threat is a possible violation of a desirable property of a system. The threats and desired system properties are listed in Table 2. The simplest way to apply STRIDE threat model is to consider how each of the threat categories affect the system under analysis and each of its connections and relationships with other systems. To do this you need to be able to model your system, the components, and its data flows, data stores, processes and interactors.

Table 2. STRIDE threats categories and system properties [52].

Threat	Definition	Desired property of system
Spoofing	*Impersonating something or someone else*	Authenticity
Tampering with data	*Modifying data or code*	Integrity
Repudiation	*Claiming to have not performed an action*	Non-repudiability
Information disclosure	*Exposing information to someone not authorized to see it*	Confidentiality
Denial of service	*Deny or degrade service to users*	Availability
Elevation of privilege	*Gain capabilities without proper authorization*	Authorization

DREAD is by nature a qualitative method, but it helps giving numerical values for the threats to calculate their severity. First, a numerical value for each DREAD category is decided (see Table 3 for an example scale between 0-10), then a total score is calculated using some formula, for example:

DREAD Risk total score = (Damage + Reproducibility + Exploitability + Affected users + Discoverability) / 5.

In this case, the formula produces a number between 0 and 10, where a higher number means more serious risk. The scale of the categories depends on the application and can be freely decided by the users to be one that fits their needs.

Table 3. DREAD risk keywords and definitions [52].

Category	Definition	Example scale
Damage potential	If a threat occurs, how much damage will be cause?	0 = Nothing 5 = Information disclosure that could be used in combination with other vulnerabilities 8 = Individual/employer non sensitive user data is compromised. 9 = Administrative non sensitive data is compromised. 10 = Complete system or data destruction. 10 = Application unavailability
Reproducible	How easy is it to reproduce the threat exploit?	0 = Very hard or impossible, even for administrators of the application. 5 = Complex steps are required for authorized user. 7.5 = Easy steps for Authenticated user 10 = Just a web browser and the address bar is sufficient, without authentication.
Exploitability	What is needed to exploit this threat?	2.5 = Advanced programming and networking knowledge, with custom or advanced attack tools. 5 = Exploit exits in public, using available attack tools. 9 = A Web Application Proxy tool 10 = Just a web browser

Category	Definition	Example scale
Affected users	How many users will be affected?	0 = None 2.5 = individual/employer that is already compromised. 6 = some users of individual or employer privileges, but not all. 8 = Administrative users 10 = All users
Discoverability	How easy it is to discover this threat?	0 = Very hard requires source code or administrative access. 5 = Can figure it out by monitoring and manipulating HTTP requests 8 = Details of faults like this are already in the public domain and can be easily discovered using a search engine. 10 = the information is visible in the web browser address bar or in a form.

3.8.4 Maturity

Both methods can be considered mature and tested as a threat identification and evaluation methods and tools. They have been used for decades, and both are referenced by a great number scientific publications from wide range of domains and applications over the years.

3.8.5 Standard based

STRIDE or DREAD are not based on any standard, they are originally based on publications by Microsoft security experts.

3.8.6 Applicability

STRIDE method is extensively used both in academic and industrial, especially in IT domain. For example, it is used alongside IEC 62443 by Fockel et al. [53] in their threat analysis or by Rouland et al. [54] in their effort to formalize threats and security requirements. There exists academic papers where using STRIDE has been also studied in nuclear field, e.g., [55,56]. Thus, we see it also suitable for the cybersecurity risk assessment also in nuclear systems. However, as many groups have done, it might be essential to do one’s own extensions and additions to the STRIDE categories and DREAD keywords to be more suitable for the domain in question.

3.8.7 Software tool availability

There exist an official Microsoft Threat Modeling Tool for doing a thorough analysis of the system with the help of diagrams and models. But a simpler analysis can be carried out with basic office tools, like Word or Excel.

3.8.8 Future prospects

STRIDE is quite a commonly used method to do a basic threat identification quickly and cost-effectively on a system. The threat categories of STRIDE are often referenced in literature, and it seems to be holding its ground as a popular approach. Threat modelling is a core element of the Microsoft Security Development Lifecycle (SDL). However, there were talks around 2010 that Microsoft would be moving away from DREAD, towards something simpler, with fewer scales per keyword (low, medium, high, critical). But at least considering the number of recent online articles and research publicity the methods are far from dead.

3.8.9 Pros and cons

You do not need to know much about STRIDE to use it. It's a way of answering to questions: “*What are we working on, and what can go wrong?”.* While allowing a simple compilation of categorized threat lists, there is not much more to it. STRIDE gives you simple method to find threats from your system, it does not promise to find all of them, but it is a good starting point. Neither it does tell you how to mitigate those threats, but it does give you insights into the nature of the mitigations you need.

When STRIDE is combined with DREAD, they together give more complete risk assessment process, including risk identification and evaluation steps. DREAD’s greatest benefit might also be its simplicity and straightforwardness, maybe flexibility too.

Both methods are very subjective and depending on the systems and the evaluators; the ratings might not be very consistent and subject to debate. They might not be detailed enough methodologies for some security critical cases.

STRIDE and DREAD are cost-effective methods, but other methods are needed to carry out a more detailed risk assessment.

3.9 UFoI-E framework

3.9.1 Description

The Uncontrolled Flow of Information and Energy (UFoI-E) framework [57,58] consist of three constituents:

- CyPHASS (Cyber-Physical Harm Analysis for Safety And Security) analysis method supported by a metamodel (an ontology) of harm scenarios;
- a metamodel, “CPS master diagram”, as to how to model the Cyber-Physical System under analysis for the CyPHASS analysis;
- UFoI-E causality concept that defines a causation model “to abstract the causal chains in physical harm scenarios” [58] thus also modelling the fact that security threats can cause critical safety consequences and physical damages. [58]

The two first constituents are practical; they are based on the third one, which is conceptual.
The CPS master diagram depicts the CPS under study as a three-layer system, Cyber Layer (CL) (operations layer), Cyber-Physical Layer (CPL) (control layer), and Physical Layer (PL) (physical manifestation layer, such as energy flows).

The CyPHASS analysis starts by identifying the expected harms, i.e., the ultimate safety consequences; hence it is a top-down method. Thereafter the causes for the harms are determined by using a database of checklists and guidewords, such as HAZOP guidewords. The CyPHASS analysis is thus kind of a HAZOP analysis, but in vice versa order, i.e. the top event is identified first and thereafter the analysts determine, which deviations could cause the top event (in HAZOP, deviations is the starting point). The authors of UFoI-E find similarities with fault tree analysis and event tree analysis (ETA), but also with attack trees, especially with the one suggested by Abdo et al. [30]. [58]

The CyPHASS database also contains a list of possible risk controls starting from prevention of hazards and threats at each level (CL, CPL and PL) separately, and continuing to list the potential hazard and threat event detection methods and safeguard methods against the detected hazard and threat events, this also at each CPS master diagram levels separately. Thus, CyPHASS implements a layers of protection scheme.

3.9.2 Scope

UFoI-E is targeted for cyber-physical systems to identify safety and security risk scenarios and to determine the risk controls against the risk scenarios. UFoI-E can be used beyond the early design phase, i.e., in phases in which the system model is mature.

3.9.3 Analysis method characteristics

The method is a top-down method with similarities to FTA, ETA and attack trees, but also with HAZOP, although in vice versa order as explained in Section 3.9.1. UFoI-E is a qualitative method lacking quantitative aspects. Therefore Guzman et al [58] refer to Abdo et al. attack tree method [30] to complement UFoI-E with quantitative analysis.

3.9.4 Maturity

The method is very new, from past few years, but has been tested in some systems already with success, such as autonomous surface vessels [9,57] and a nuclear facility, Halden Safety Fan Enclave [58]. Due to similarities with FTA, ETA and HAZOP, UFoI-E is easy to adopt, especially with the database support (see Section 3.9.7) and can thus be considered mature enough for NPP I&C systems.

3.9.5 Standard based

UFoI-E is not based on any particular standard, neither is it itself standardised.

3.9.6 Applicability

UFoI-E has academic origin, but with strong industrial target. It is well suitable to NPP I&C systems; this judgement is evidenced by the Halden Safety Fan Enclave case study [58].

3.9.7 Software tool availability

The CyPHASS database is available as an open source Excel file [59]. The Excel file also presents the CyPHASS method and the sequence of steps to carry out the analysis. See a more detailed review of the CyPHASS database in Section 4.5.

3.9.8 Future prospects

As the UFoI-E is very new, it is expected to be developed further. Guzman et al. [58] mention the possibility to complement UFoI-E with the quantitative aspects of the attack tree method by Abdo et al. [30]. Due to its clarity and open source tool support (see Section 3.9.7) there is a good probability for UFoI-E to be among the risk analysis methods used by the industry, although methods that are better aligned with standards, especially with IEC 62443 (Industrial communication networks - Network and system security) series of standards, are more likely to be embraced.

3.9.9 Pros and cons

UFoI-E is easy to adapt by safety engineers familiar with typical analysis methods such as FTA, ETA and HAZOP. Its power is in its clarity, which is mainly driven by the two powerful metamodels, CPS master diagram and harm scenario ontology, and by the database support with pre-defined lists of analysis guidewords, checklists, and risk controls (risk mitigation methods). It is illustrative and describes well the effect of multiple causes.

UFoI-E lacks quantitative and temporal aspects. It also lacks direct links to standards, such as the IEC 62443 family of industrial control systems security standards.

3.10 Consequence-driven Cyber-informed Engineering (CCE)

3.10.1 Description

Idaho National Laboratory (INL) has created an operational process for performing cyber-informed consequence analysis and engineering mitigations. Consequence-driven Cyber-informed Engineering (CCE) is a cyber defence concept that focuses on the highest consequence events from an engineering perspective. The CCE process has four phases which help to determine the most critical functions, to identify methods an adversary could use to compromise the critical functions, and to apply proven engineering, protection, and mitigation strategies to isolate and protect an industry’s most critical assets.

Initial assumption of the CCE process is that adversaries have logical access, including all credentials, IP addresses, firewall, and application access. They have an understanding of critical equipment and processes and all the knowledge to impact the system with sufficient resources. Adversaries have access to the required equipment, engineering expertise, and tools to conduct a successful attack. [60]

The four CCE phases are the following [60]:

- Phase 1: Consequence Prioritization
    - The goal of this phase is to identify High-Consequence Events (HCEs) that would potentially disrupt an organization’s ability to provide the critical services and functions deemed fundamental to their business mission. HCEs will be scored based of severity of their consequences and most critical of them will be selected for next phase.
- Phase 2: System-of-Systems Analysis
    - The goal of this phase is mapping the playing field. To achieve this, block diagrams and functional descriptions relevant to each HCEs from previous phase will be developed.
    - The aim is to analyse system-of systems and to find access paths related to each HCE, evaluate initial assessment of attack feasibility and find what is the required knowledge of adversaries.
- Phase 3: Consequence-Based Targeting
    - The goal of this phase is to develop for each selected HCE a kill-chain or Concept of Operations (CONOPs) for attacker as to how they could reach their goal. This includes the desired end effect of the ICS payload, the precise technical element or elements being targeted, the highest

confidence access paths, and the information and access required to develop and to deploy the payload.

  - Attacks are not executed in CCE but all material available are used to ensure that all the technical details are as correct as possible, and the human process aspects are captured also.
  - Knowing CONOPs helps the CCE team focus on the most plausible attack paths in next phase and to identify the choke points to stop attackers.
  - After the scenarios are developed, they will be prioritised for next phase.
- Phase 4: Mitigations and Protections
  - The goal of this phase is to identify and develop potential protection strategies that can be implemented within a participating organization to mitigate those attack paths and cyber CONOPs developed in previous phases.
  - In each HCE scenario, the CCE team will find out what do the engineers and operators closest to the target processes recommend as ways to protect the most critical, long-lead-time-to-replace equipment. These recommendations could include both digital and non-digital protections, including adding human in the decision loop.

3.10.2 Scope

The scope of the CCE is the system-of-systems, including also human and supply-chain related issues. The CCE does not attempt to evaluate the strength or effectiveness of current cyber defence. It does not seek to factor in the likelihood of a successful attack. The CCE is (almost) entirely focused on determining the consequence of a cyber-event, and preventing the worst consequences from occurring when adversaries reach their targets. [60]

3.10.3 Analysis method characteristics

CCE is a systematic top-down process, which uses different kinds of methods in different phases of process. CCE draws from multiple sources including but not limited to Design Based Threat, Crown Jewels Analysis, Process Hazards Analysis, and ICS Cyber Kill Chain.

An example of the CCE process can be found from [61].

3.10.4 Maturity

The development of the CCE is based on several other existing methods. According to [60], US Federal Government has been using the CCE to secure their National Critical Functions.

3.10.5 Standard based

CCE has not been published as a standard.

3.10.6 Applicability

According to [60], the US Federal Government has been using the CCE to secure their National Critical Functions. The INL has strong connections to NPP security. According to [62], "*The CCE process helps* *nuclear asset owners to identify high-impact / high-consequence events that could result in interruption of critical functions, analyze the infrastructure which could be subverted to enable those events, and develop specific mitigations to avoid, or engineer out, these consequences*".

3.10.7 Software tool availability

According to the available information there are no software tools which have specific support for the CCE.

3.10.8 Future prospects

CCE seems to be in active use, and in the INL, training is available. [63]

3.10.9 Pros and cons

The method considers the threat consequences well. To go through the whole CCE process looks laborious and time-consuming. However, most of the work is something that organizations should have done already. The threats and vulnerabilities may be understated if the consequences are not determined to be high.

3.11 Cyber Security Argument Graph

3.11.1 Description

Cyber Security Argument Graph method [64] is a model-based method for assessing the security risks for cyber-physical systems. In particular, the method takes advantage of the so-called workflow models [65] to generate security argument graphs. Workflow is a high-level description how a system provides its intended functionality. A security argument graph, on the other hand, is a graphical formalism that integrates security-related inputs, such as,

- Goal: a system-level property or requirement for the specified workflow, for example, availability
- Workflow: a model of the actors and interactions occurring in the system, for example, UML activity diagram
- System: a model describing the system's devices, connections, and configurations
- Attacker: a model describing the skills, resources, and knowledge of the attacker under consideration

to argue about the security of the target system. A security argument graph visually represents potential attacks on the system components implementing a workflow. The graph is created automatically, provided the above inputs are present. The structure of the graph determines dependency relationships between security-related inputs which, in turn, can be used to calculate system-level security metrics from the low-level data, for example, probability to launch an attack.

3.11.2 Scope

The proposed method is flexible and general enough to be applied as a risk assessment method for any cyber physical system. The main functionality, that is, generation of a security argument graph, can be extended using the so-called extension templates. An extension template is a formal reusable rule for connecting a security-related statement or claim with relevant supporting arguments, which also carries the logic about how numerical evidence associated with supporting arguments affects metrics associated with the higher-level statement. However, in most of the cases, extension templates need to be created manually.

3.11.3 Analysis method characteristics

As observed in [66], the proposed method shows some similarities to attack trees method in the sense that both are graph-based methods. Thus, Cyber Security Argument Graph method can be considered a systematic way of characterizing diverse system threats, with intuitive representation of potential attack and possibility of formal mathematical frameworks for analysing them in a quantitative manner.

It is a top-down method to argue about the security of the target system with respect to the security-related input parameters, such as, goal, workflows, system structure, and attacker's capabilities. Values for these input parameters need to be determined for the method to work, for example, based on the earlier empirical evidence or subjective assessment of security experts.

3.11.4 Maturity

The original paper was published in 2014 and has been cited 15 times. In the original paper, there is no mention of industrial use, or an industrial case study, only a research-based study on the electric power grid. The authors of the original paper conducted two cases studies for electrical grid network [66] and railway transportation network [67] in 2015 and 2016, respectively.

3.11.5 Standard based

The method is not based on any standard.

3.11.6 Applicability

The risk assessment of electrical grid network, conducted in 2015, uses failure scenarios defined by US National Electric Sector Cybersecurity Organization Resource (NESCOR). More specifically, the paper integrates the NESCOR failure scenarios into the Cyber Security Argument Graph method. However, the paper only illustrates the first failure scenario (DER.1) in distributed energy resources scenario (DER) where inadequate access control of distributed energy resources causes electrocution, which could be of limited interest to nuclear industry. Unfortunately, more interesting failure scenarios related, for example, to energy generation or supervisory control and data acquisition (SCADA) systems, are not discussed.

3.11.7 Software tool availability

Construction of a security argument graph for a complex cyber-physical system can be costly and error prone. To better deal with the complexity, the authors of the original paper developed software tool called CyberSAGE [68], which is available at [69] under a non-exclusive, royalty-free, non-transferable, and restricted license to academic developers.

3.11.8 Future prospects

The latest found reference to the method is from 2016. To the best of our knowledge, there is no recent evidence of the method gaining popularity in industrial use.

3.11.9 Pros and cons

The proposed method is flexible and general enough to be applied as a risk assessment method for any cyber physical system. The main functionality, generation of a security argument graph, is fully automated, and can be further extended using the so-called extension templates; the security argument graph is well descriptive.

However, the extension templates are usually created in a time-consuming and error-prone manual process. Similarly, whereas attacker's goals or attacker's capabilities can be used systematically across many use cases, the workflows and system model need to be created manually for each target system. Software tool support is need.

Thus, to summarize, the application of the method may require significant manual and system-specific efforts to be applied in practice.

3.12 PRISM

3.12.1 Description

The prioritize-resource-implement-standardize-monitor (PRISM) [70] is a strategic decision framework for cybersecurity risk assessment. The framework was created in 2020 to address the gap in traditional risk-management frameworks, namely, a lack in terms of addressing risks through a process of prioritization to include trade-offs and risk acceptance for optimal decision-making in a resource-constrained environment. According to the authors of PRISM, traditional frameworks miss the key step of prioritization that would ensure that the planned risk management actions are consistent with the priorities, mission and business objectives. Prioritizing includes identifying the main risk drivers and interdependencies among them. The remaining steps, that is, resourcing, implementing, standardizing, and monitoring, ensure that resourcing and implementation of the identified and necessary security controls are integrated into the organization's enterprise systems and processes.

3.12.2 Scope

The PRISM framework is a strategic framework. The framework can be used to assess the strategic orientation of a firm with respect to its cybersecurity posture. The main goal is to assist top-management-team with tailoring their decision-making about security investments while managing cyber risk at their organization. In particular, the framework expands the focus of achieving cybersecurity objectives, such as identifying and reducing vulnerabilities, meeting mission requirements, standardizing operations and simplifying processes by enabling organizational leadership to identify and operationalize a tailored approach for cyber risk management.

The PRISM framework allows for the inclusion of strategic objectives into the organization's cyber security risk management process, and the prioritization emphasis reduces the organization's daunting task of managing the entire range of potential threat vectors. As such, the PRISM methodology would be most useful in the analysis of an organization's ability to deal with distinct threat scenarios, rather than addressing the whole of the organization's risk management capabilities as other risk frameworks tend to do.

3.12.3 Analysis method characteristics

In general, using PRISM, a systematic review of cybersecurity problems and identification of resources is undertaken for optimal planning to address targeted cyber risks. With a properly designed prioritization step, PRISM framework allows a top-down approach. Thus, the PRISM framework can be considered a systematic and top-down method.

To operationalize the PRISM approach, a step-by-step analysis workflow is used for prioritizing and scoring risks. The associated set of activities is:

- Identification of key risk areas/vectors: Major risk areas or vectors are identified based on historical and predictive future risk incidents;
- Identification of risk factors: The major components within each risk area or vector susceptible to risk incidents are identified;
- Prioritization weighting (P): The severity of risk factors to the organization are ranked using a relative scale;
- Resource allocation (R): Allocation of resources necessary to monitor and prevent risks are assessed;
- Implement (I): The stages, which organization needs to reach in order to detect and prevent risks, are evaluated; Implementation responsiveness levels are for example, reactive level, proactive level, and enterprise level;
- Standardize (S): Standard knowledge and solutions to be shared across organization are created;
- Monitor (M): Suitable monitoring procedures and tools to detect unusual behaviour and prevent risks are identified;
- Risk rating level: Finally, risk rating level for risk areas and factors are calculated to determine organization's preparedness. The preparedness level is ranked from 1 to 7, with 1-2 being considered poor, 3-4 considered fair, 5 considered good, 6 considered very good, and 7 considered excellent.

All those steps are to be executed by a dedicated team of experts. Since the final risk rating level is using a simple ordinal scale, the PRISM framework is a qualitative one.

3.12.4 Maturity

The original paper was published in 2020 and has been cited 4 times since then. In the original paper, there is no mention of industrial use or an industrial case study. However, the authors of the original paper conducted a retrospective analysis of 4 real-world cyber risk incidents, including loss or theft of equipment and personal data breach, and demonstrated that PRISM framework would prevent occurrence of those incidents.

3.12.5 Standard based

The method is not based on any standards.

3.12.6 Applicability

The PRISM framework is a general-purpose meta-method and fits therefore for any kind of safety and security critical systems if a relevant compliance-based scheme is used to identify key risks areas and risk factors. In fact, PRISM framework, could complement rather than replace any standard-based or compliance-based risk management framework.

Currently, there is no reference about the industrial use of the PRISM framework.

3.12.7 Software tool availability

To the best of our knowledge, no software tools are available.

3.12.8 Future prospects

The original paper was published in 2020. To the best of our knowledge, there is no recent evidence of the method gaining popularity in industrial use.

3.12.9 Pros and cons

The major advantage of the PRISM framework is that it will help organizations identify and implement the most tailored risk management and cybersecurity approach applicable to their security challenges. The PRISM framework can also be used by organizations to set priorities, explore gaps in current processes and to steer an organization in the right direction to resolve risk management and cyber risks specific to an organizational strategy and functions. PRISM prioritises the risks well.

There is not much experience with PRISM.

3.13 STPA-Extension

3.13.1 Description

STPA-Extension is a safety and security co-analysis extension of the STPA (System-theoretic process analysis) hazard analysis method [57]. The underlying STPA method has been developed at MIT since the early 2000s. STPA applies a novel accident causality model, STAMP (System-theoretic accident model and processes), which is based on systems theory. STAMP considers safety as a control problem, instead of focusing on failures or linear event chains, which are typical in many traditional analysis methods [71]. It describes the system as a hierarchical control structure, which is a model consisting of feedback loops describing system elements and their interconnections. The aim is to cover various types of causal factors, such as software aspects as well as human and organizational factors.

STPA provides a defined procedure for the identification of unsafe control actions (UCAs) and causal scenarios using the system model. The generic STPA method is described in the freely available STPA Handbook by Leveson & Thomas [72].

While the generic STPA can be applied very broadly, its focus is on safety analysis. Thus, extensions to STPA have been proposed to cover security aspects (e.g. STPA-SEC [73]), as well as safety and security co-analysis (e.g. STPA-Extension [57], STPA-SafeSec [74]). Here the focus is on STPA-Extension.

3.13.2 Scope

STPA-Extension is a general-purpose method, and as such, there are no limitations on which types of systems it can be applied to. As it focuses on system-level hazards, it should preferably be applied starting from the early stages of the development process.

3.13.3 Analysis method characteristics

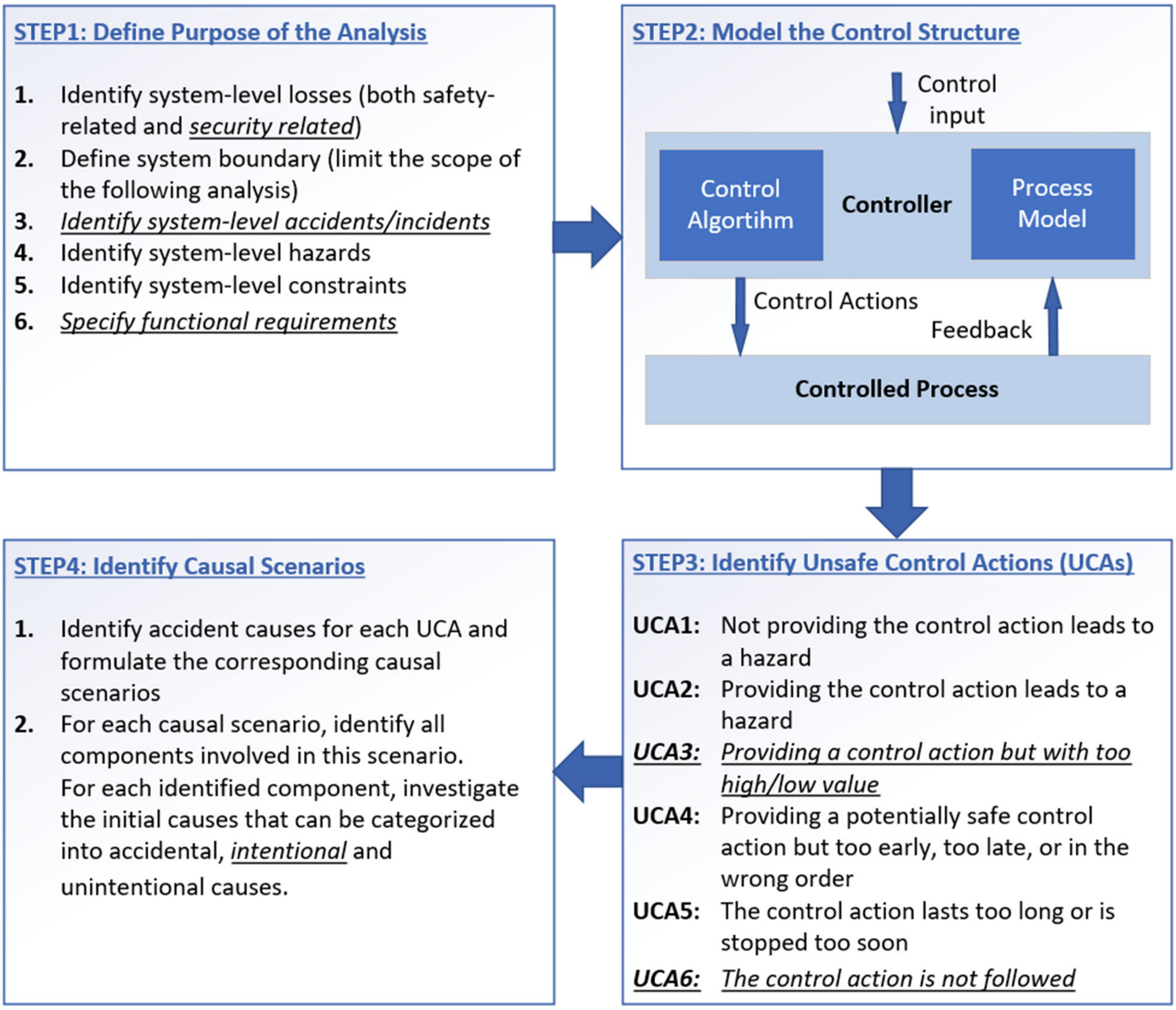
STPA-Extension is a qualitative top-down analysis method. The analysis process (illustrated in Figure 1) consists of four steps that have been elaborated based on the generic STPA:

- Step 1: Definition of the purpose of the analysis. This includes identification of system-level losses (both safety and security related), hazards, and constraints. The STPA-Extension adds specification of functional requirements to this step. In STPA-Extension, system-level security incidents are differentiated from safety accidents.

- Step 2: System is modelled as a hierarchical control structure. This is a graphical representation featuring controllers and controlled processes and the interactions between them (control and feedback). The hierarchy is illustrated by the vertical axis, i.e. highest control authority is at the top of the diagram.

- Step 3: The control structure is systematically analysed to find unsafe control actions (UCAs) that, in a particular context and worst-case environment, will lead to a hazard. In STPA, there are four pre-defined categories of UCAs (which, in practice, can be used as guidewords) to support identification, whereas STPA-Extension adds two categories related to security analysis (see Figure 1).

- Step 4: The analysis concludes with identification of loss scenarios, which describe the causal factors that can lead to UCAs and hazards. In STPA-Extension, also intentional causal factors are considered.



STEP1: Define Purpose of the Analysis

1. Identify system-level losses (both safety-related and *security related*)
2. Define system boundary (limit the scope of the following analysis)
3. *Identify system-level accidents/incidents*
4. Identify system-level hazards
5. Identify system-level constraints
6. *Specify functional requirements*

STEP2: Model the Control Structure

STEP3: Identify Unsafe Control Actions (UCAs)

UCA1: Not providing the control action leads to a hazard

UCA2: Providing the control action leads to a hazard

UCA3: *Providing a control action but with too high/low value*

UCA4: Providing a potentially safe control action but too early, too late, or in the wrong order

UCA5: The control action lasts too long or is stopped too soon

UCA6: *The control action is not followed*

STEP4: Identify Causal Scenarios

1. Identify accident causes for each UCA and formulate the corresponding causal scenarios
2. For each causal scenario, identify all components involved in this scenario. For each identified component, investigate the initial causes that can be categorized into accidental, *intentional* and unintentional causes.

Figure 1. STPA-Extension analysis process [57]. The underlined italics parts are extensions to the generic STPA method.

3.13.4 Maturity

STPA and its extensions are relatively new methods, and there is only limited experience of their practical applications. Currently, generic STPA is mostly applied in the automotive and aerospace industries. STPA-Extension is not used industrially.

Based on authors' experience on the guidance material (especially [72]), some parts of the analysis process seem more mature than others. Specifically, the steps from 1 to 3 are rather comprehensively defined and systematic, whereas the final step is more vaguely defined and leaves the analyst with little guidance for defining the scenarios.

3.13.5 Standard based

STPA or its extensions are not based on existing standards. Rather than proceeding towards a general, methodology-centric standard, the standardization is actively being developed within the domains where STPA is most widely used. The first standard with guidance on applying STPA in the automotive industry, *SAE J3187_20220 System Theoretic Process Analysis (STPA) Recommended Practices for Evaluations of Automotive Related Safety-Critical Systems*, has been published in February 2022 [75]. Additional standards are being developed in the aircraft industry (SAE AIR 6913 [76]). However, these standards do not cover the safety and security co-analysis extensions of STPA.

3.13.6 Applicability

STPA-Extension is a general method and can be applied to various types of systems, thus being applicable to NPP I&C systems. Its uses so far, however, have been academic. The authors of the method have applied to in the autonomous shipping domain.

3.13.7 Software tool availability

The software tool availability for STPA and its extensions is limited. The commercial *Risk management studio* software includes a module for documenting STPA analysis. Additionally, there are some freely available implementations available (XSTAMPP, STAMP Workbench), but these are not actively developed, and they lack active support. As the steps of STPA-Extension are mainly similar to those of generic STPA, it is likely that these tools could be easily modified to document the STPA-Extension as well. An alternative means is using of a general spreadsheet software and a suitable drawing software for documenting the analysis and drawing the system model.

3.13.8 Future prospects

STPA in general has seen increasing popularity over previous years [77]. It is likely that its usage in various domain areas continues to increase, further emphasizing the need for safety and security co-analysis and STPA-Extension.

3.13.9 Pros and cons

With academic debate ongoing on applicability of STPA, various pros and cons have been presented. These remarks are relevant for the STPA-Extension as well.

Pros:

- Can support identification of scenarios that would be difficult to identify with methods based on different accident models.
- The scope of the analysis is well defined, supporting efficient analysis activities.
- Supports consistent documentation as a specified syntax is defined for analysis outputs.
- The hierarchical system model supports system design.
- Considers well risk scenarios if the process model is comprehensively defined.

Cons:

- Evaluation of completeness of the control structure model is challenging. Some scenarios (unexpected vulnerabilities or threats), which are not identifiable from the model need to be considered separately.
- The analysis participants require knowledge of the analysis method and terminology used to be able to contribute.

- Software support is still lacking.

4. Cybersecurity analysis tools for ICS

In the following sub-sections, some cybersecurity tools potentially suitable for NPP I&C systems are presented. The tools are selected based on the findings during the literature review, but also based on former experience.

4.1 MITRE ATT&CK for ICS

MITRE ATT&CK for Industrial Control Systems (ICS) is a curated knowledge base for cyber adversary behaviour in the ICS technology domain. It reflects the various phases of an adversary's attack life cycle and the assets and systems they are known to target. ATT&CK for ICS originated from MITRE internal research focused on applying the ATT&CK methodology to the ICS technology domain. [78]

The major architectural focus of ATT&CK for ICS are the systems and functions associated with functional levels 0…2 of the Purdue architecture. Adversaries typically need to control these systems and functions to cause an impact to ICS.

ATT&CK for ICS describes the tactics, techniques and procedures (TTP) adversaries use to operate in the OT system. The adversary TTPs associated with ATT&CK for ICS fall under the following broad categories [79]:

- "Blocked or delayed flow of information through ICS networks, which could disrupt ICS operation.
- Unauthorized changes to instructions, commands, or alarm thresholds, which could damage, disable, or shut down equipment, create environmental impacts, and/or endanger human life.
- Inaccurate information sent to system operators, either to disguise unauthorized changes, or to cause the operators to initiate inappropriate actions, which could have broad negative effects.
- ICS software or configuration settings modified, or ICS software infected with malware, which could have broad negative effects.
- Interference with the operation of equipment protection systems, which could endanger costly and difficult-to-replace equipment.
- Interference with the operation of safety systems, which could endanger human life."

The MITRE ATT&CK for ICS Matrix [80] is an overview of about 80 different tactics and techniques described in the ATT&CK for ICS knowledge base. It visually aligns individual techniques under the tactics in which they can be applied. Some techniques span more than one tactic because they can be used for different purposes.

ATT&CK for ICS can be used for adversary emulation, cyber threat intelligence enrichment, red teaming, SOC (Security Operations Center) maturity assessments, failure scenario development and educational purposes.

4.2 SHODAN

Shodan is a search engine for Internet-connected devices. Its geographically distributed crawlers select randomly next IPv4 address and port number to visit. This means that the crawlers don't scan incremental network ranges. The crawling is performed completely random to ensure a uniform coverage of the Internet and prevent bias in the data at any given time.

If any services will be found behind randomly selected address and port number, crawler will collect its banner and metadata. The banner is textual information that describes a service on a device; e.g., for web servers this would be the headers including information about web server software version and for industrial control systems there could be included more device specific fields like in next example from [81].

```
Copyright: Original Siemens Equipment
PLC name: S7_Turbine
Module type: CPU 313C
Unknown (129): Boot Loader A
Module: 6ES7 313-5BG04-0AB0 v.0.3
Basic Firmware: v.3.3.8
Module name: CPU 313C
Serial number of module: S Q-D9U083642013
Plant identification:
Basic Hardware: 6ES7 313-5BG04-0AB0 v.0.3
```

Shodan also grabs meta-data about the device such as its geographic location, hostname, and operating system. All information collected by Shodan is searchable using either main Shodan website or developer API. To use advanced filters in searches or to use developer API, users have to create account to Shodan main website and pay small fee. The primary users of Shodan are cybersecurity professionals, researchers, law enforcement agencies, and organizations and utilities which are searching what are their current exposure to public internet. During the years, Shodan has been used to found vast amount of devices which either have vulnerable software installed or should not have been connected to public internet.

4.3 CIARA

CIARA is a risk assessment and management platform from Radiflow. It is targeted for industrial control systems and is compliant with IEC 62443, the most relevant part of which in case of the risk assessment procedure is IEC 62443-3-2 [42].

CIARA is an automated tool that simulates attacks according to threats information retrieved from various sources. Simulation is done by using a digital twin of the actual I&C network. The digital twin is created by another Radiflow tool, iSID Threat Detection server, which reads the real network traffic to create the digital twin for CIARA risk assessments. The iSID server can be used along with another Radiflow tool called iSAP, which is a special purpose network traffic information collector that filters out unnecessary data and compresses the remaining information with 10:1 ratio and sends it to the iSID server. For cases in which the network is complex with several iSID servers, Radiflow offers another tool called iCEN to manage multiple instances of iSID servers.

CIARA goes through all the IEC 62443-3-2 [42] workflow ZCR (Zone and Conduit Requirements) steps, except ZCR 7 (Asset owner approval), which is beyond the scope of such tool. CIARA automatically generates the risk assessment report. CIARA generates a prioritised list of risk control suggestions with information about the costs of the risk controls implementation.

Due to its automated risk assessment, CIARA can be deployed to continuously monitor the networks of the I&C systems instead of periodic or occasional risk assessment updates.

Radiflow lists example application areas of CIARA:

- electrical power - electricity stations and substations
- water and wastewater facilities
- renewable energy
- process manufacturing
- building management systems.

They also list case studies from years 2018-2020 as follows:

- incorporating Radiflow's iSID in a managed OT SOC[3]
- detection of a crypto-mining malware attack at a water utility
- securing a Midwestern Generation and Transmission (G&T) Utility
- securing a global chemicals manufacturer
- securing a large-scale power plant in Central Europe
- securing a global chemicals manufacturer
- securing a large hospital campus
- securing an offshore oil-drilling rig in the North Sea
- securing petroleum storage tanks in Southeast Asia.

All the information above paragraphs is retrieved from [82].
David Bean, a solution manager of Mitsubishi Electric, reports that they use CIARA [83]. This and the case studies listed above suggest that CIARA is a potential tool also for security assessments of NPP I&C systems.

4.4 exSILentia Cyber and ARCHx

Exida provides a cyber security risk assessment tool called exSILentia Cyber [49], an option for the Exida exSILentia safety risk management tool. exSILentia Cyber includes two tools, CyberPHAx and CyberSL. CyberPHAx implements Cyber PHA method presented in Chapter 0, whereas the CyberSL is used to verify the adequacy of the risk controls and to quantify the residual risk. CyberSL can input the risk assessment data from CyberPHAx. exSilenta Cyber stores the user input data, such as vulnerabilities, threats, cyber event scenarios and risk controls to a database. Furthermore, exSILentia Cyber can generate a risk assessment report from CyberPHAx and a report from the CyberPL tool. [50]

[3] OT SOC companies are service providers that offer managed Security Operations Center (SOC) services for Operational Technology (OT) networks.

Exida provides another tool for device level cyber threat modelling called ARCHx. It is a FMECA or HAZOP like tool to capture the failure, deviation and threat data of a safety and security critical device. [84]

4.5 UFoI-E tool support

The UFoI-E framework is supported by an open source CyPHASS database (Excel-file) that includes description and list of analysis steps of its CyPHASS analysis method, and an ample set of check lists to guide the analysis. The database is available from [59]. The Excel-file has the following worksheets:

- UFoI-E framework diagram
- CPS master diagram (metamodel of the system under analysis)
- CyPHASS algorithm (sequence of analysis steps)
- CyPHASS harm scenario ontology diagram (‘CyPHASS bowtie’)
- Checklist for Cyber Layer uncontrolled flow of information
- Checklist for cyber threats/hazards to Cyber Layer
- Checklist for prevention barriers against cyber threats/hazards to Cyber Layer
- Checklist for physical threats/hazards to Cyber Layer
- Checklist for prevention barriers against physical threats/hazards to Cyber Layer
- Checklist for detection barriers against uncontrolled flows of information at the Cyber Layer
- Checklist for response barriers against uncontrolled flows of Information at the Cyber Layer
- Checklist for Cyber-Physical Layer uncontrolled flow of information
- Checklist for cyber threats/hazards to Cyber-Physical Layer
- Checklist for prevention barriers against cyber threats/hazards to Cyber-Physical Layer
- Checklist for physical threats/hazards to Cyber-Physical Layer
- Checklist for prevention barriers against physical threats/hazards to Cyber-Physical Layer
- Checklist for detection barriers against uncontrolled flows of information at the Cyber-Physical Layer
- Checklist for response barriers against uncontrolled flows of Information at the Cyber-Physical Layer
- Checklist and guidewords for Physical Layer process variables and functional deviations
- Checklist for physical threats/hazards to Physical Layer
- Checklist for prevention barriers against physical threats/hazards to Physical Layer
- Checklist for detection barriers against uncontrolled flows of energy at the Physical Layer
- Checklist for response barriers against uncontrolled flows of energy at the Physical Layer
- Checklist for Physical Layer uncontrolled flow of energy.

The CyPHASS harm scenario ontology diagram provides links from the diagram objects to the corresponding checklist worksheets.

5. Discussion and conclusions

The main finding of the review was that the array of security analysis methods is vast, both separate methods and methods that also concern safety, but that the practices are not that well established than with pure safety risk analyses, and more work is needed to determine the optimal security analysis methods in general or for each domain separately, such as nuclear power plant instrumentation and control systems. But there are good methods already, such as the ones presented in Chapter 0. There are also some software tools suitable for security risk analysis of industrial control systems, but not too many to select upon. In both cases – methods and tools – the company implementing safety and security critical control systems must be prepared to select more than one method and more than one tool to comply with the regulator requirements and the company specific safety and security policy. A holistic platform to manage, with traceability, the diverse data from the different methods and tools is needed. Alanen et al. [8] present an ontology for such a holistic repository; with the conformity assessment model developed by Alanen et al. [85] and demonstrated by Linnosmaa & Alanen [86], the traceability between the risk assessment artefacts and other systems engineering artefacts, such as system elements and requirements, is achieved.

6. Acknowledgments

This research was funded by the Finnish Research Programme on Nuclear Power Plant Safety 2019-2022 (SAFIR2022). Any opinions or findings of this work are the responsibility of the authors, and do not necessarily reflect the views of the sponsors or collaborators.

References

[1] Dobaj J, Schmittner C, Krisper M, Macher G. Towards Integrated Quantitative Security and Safety Risk Assessment. In: Romanovsky A, Troubitsyna E, Gashi I, Schoitsch E, Bitsch F, editors. Computer Safety, Reliability, and Security, Cham: Springer International Publishing; 2019, p. 102–16.

[2] Agrawal V. A Comparative Study on Information Security Risk Analysis Methods. Journal of Computers 2017:57–67. https://doi.org/10.17706/jcp.12.1.57-67.

[3] Campbell PL, Stamp JE. A Classification Scheme for Risk Assessment Methods 2004.

[4] Kriaa S, Pietre-Cambacedes L, Bouissou M, Halgand Y. A survey of approaches combining safety and security for industrial control systems. Reliability Engineering & System Safety 2015;139:156–78. https://doi.org/https://doi.org/10.1016/j.ress.2015.02.008.

[5] Roldán-Molina G, Almache-Cueva M, Silva-Rabadão C, Yevseyeva I, Basto-Fernandes V. A Comparison of Cybersecurity Risk Analysis Tools. Procedia Computer Science 2017;121:568–75. https://doi.org/10.1016/j.procs.2017.11.075.

[6] Schmittner C, Gruber T, Puschner P, Schoitsch E. Security Application of Failure Mode and Effect Analysis (FMEA). In: Bondavalli A, Di Giandomenico F, editors. Computer Safety, Reliability, and Security, Cham: Springer International Publishing; 2014, p. 310–25.

[7] Chen Y-R, Chen S-J, Hsiung P-A, Chou I-H. Unified Security and Safety Risk Assessment - A Case Study on Nuclear Power Plant . 2014 International Conference on Trustworthy Systems and Their Applications 2014:22–8. https://doi.org/10.1109/TSA.2014.13.

[8] Alanen J, Linnosmaa J, Malm T, Papakonstantinou N, Ahonen T, Heikkilä E, et al. Hybrid ontology for safety, security, and dependability risk assessments and Security Threat Analysis (STA) method for industrial control systems. Reliability Engineering and System Safety 2022.

[9] Carreras Guzman NH, Kwame Minde Kufoalor D, Kozine I, Lundteigen MA. Combined safety and security risk analysis using the UFoI-E method: A case study of an autonomous surface vessel . Proceedings of the 29th European Safety and Reliability Conference, ESREL 2019 2020:4099–106. https://doi.org/10.3850/978-981-11-2724-3_0208-cd.

[10] Kavallieratos G, Katsikas S, Gkioulos V. Cybersecurity and Safety Co-Engineering of Cyberphysical Systems—A Comprehensive Survey. Future Internet 2020;12. https://doi.org/10.3390/fi12040065.

[11] IEC. IEC 60812: Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA) 2006;Edition 2.:93.

[12] Anon. The STRIDE Threat Model. Microsoft Commerce Server 2002 Documentation 2005:1. https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN.

[13] Schmittner C, Ma Z, Smith P. FMVEA for Safety and Security Analysis of Intelligent and Cooperative Vehicles. In: Bondavalli A, Ceccarelli A, Ortmeier F, editors. Computer Safety, Reliability, and Security, Cham: Springer International Publishing; 2014, p. 282–8.

[14] Chen B, Schmittner C, Ma Z, Temple WG, Dong X, Jones DL, et al. Security Analysis of Urban Railway Systems: The Need for a Cyber-Physical Perspective. In: Koornneef F, van Gulijk C, editors. Computer Safety, Reliability, and Security, Cham: Springer International Publishing; 2015, p. 277–90.

[15] Anon. Common Weakness Enumeration (CWE). Mitre Web Site 2021:1. https://cwe.mitre.org/index.html.

[16] Steiner M, Liggesmeyer P. Combination of Safety and Security Analysis - Finding Security Problems That Threaten The Safety of a System. SAFECOMP 2013 - Workshop DECS (ERCIM/EWICS Workshop on Dependable Embedded and Cyber-physical Systems) of the 32nd International Conference on Computer Safety, Reliability and Security, 2013, p. 1–8.

[17] Peischl B, Felderer M, Beer A. Testing Security Requirements with Non-experts: Approaches and Empirical Investigations. 2016 IEEE International Conference on Software Quality, Reliability and Security (QRS), 2016, p. 254–61. https://doi.org/10.1109/QRS.2016.37.

[18] Bouissou M, Bon J-L. A new formalism that combines advantages of fault-trees and Markov models: Boolean logic driven Markov processes . Reliability Engineering & System Safety 2003;82:149–63. https://doi.org/10.1016/S0951-8320(03)00143-1.

[19] Pietre-Cambacedes L, Deflesselle Y, Bouissou M. Security Modeling with BDMP: From Theory to Implementation . 2011 Conference on Network and Information Systems Security 2011:1–8. https://doi.org/10.1109/SAR-SSI.2011.5931382.

[20] Kriaa S, Bouissou M, Colin F, Halgand Y, Pietre-Cambacedes L. Safety and Security Interactions Modeling Using the BDMP Formalism: Case Study of a Pipeline. Computer Safety, Reliability, and Security 2014;8666:326–41. https://doi.org/10.1007/978-3-319-10506-2_22.

[21] Bouissou M. Solution by KB3-BDMP and Figseq (A) or YAMS (M) n.d.:37.

[22] Roth M, Liggesmeyer P. Modeling and Analysis of Safety-Critical Cyber Physical Systems using State/Event Fault Trees. In: ROY M, editor. SAFECOMP 2013 - Workshop DECS (ERCIM/EWICS Workshop on Dependable Embedded and Cyber-physical Systems) of the 32nd International Conference on Computer Safety, Reliability and Security, Toulouse, France: 2013, p. NA.

[23] Kaiser B, Gramlich C, Förster M. State/event fault trees—A safety analysis model for software-controlled systems. Reliability Engineering & System Safety 2007;92:1521–37. https://doi.org/https://doi.org/10.1016/j.ress.2006.10.010.

[24] Ten C-W, Liu C-C, Govindarasu M. Vulnerability Assessment of Cybersecurity for SCADA Systems Using Attack Trees. 2007 IEEE Power Engineering Society General Meeting 2007:1–8. https://doi.org/10.1109/PES.2007.385876.

[25] Ten C-W, Liu C-C, Manimaran G. Vulnerability Assessment of Cybersecurity for SCADA Systems . IEEE Transactions on Power Systems 2008;23:1836–46. https://doi.org/10.1109/TPWRS.2008.2002298.

[26] Ten CW, Manimaran G, Liu CC. Cybersecurity for critical infrastructures: Attack and defense modeling. IEEE Transactions on Systems, Man, and Cybernetics Part A:Systems and Humans 2010;40:853–65. https://doi.org/10.1109/TSMCA.2010.2048028.

[27] Schneier B. Attack Trees. Dr Dobb's Journal of Spftware Tools 1999;24:60. https://doi.org/10.1002/9781119183631.ch21.

[28] Gadyatskaya O, Trujillo-Rasua R. New Directions in Attack Tree Research: Catching up with Industrial Needs. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 2017;10744 LNCS:115–26. https://doi.org/10.1007/978-3-319-74860-3_9.

[29] Lallie HS, Debattista K, Bal J. A review of attack graph and attack tree visual syntax in cyber security. Computer Science Review 2020;35. https://doi.org/10.1016/J.COSREV.2019.100219.

[30] Abdo H, Kaouk M, Flaus JM, Masse F. A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie – combining new version of attack tree with bowtie analysis. Computers & Security 2018;72:175–95. https://doi.org/10.1016/J.COSE.2017.09.004.

[31] Cho CS, Chung WH, Kuo SY. Using Tree-Based Approaches to Analyze Dependability and

Security on I&C Systems in Safety-Critical Systems. IEEE Systems Journal 2018;12:1118–28. https://doi.org/10.1109/JSYST.2016.2635681.

[32] Khand PA. Attack tree based cyber security analysis of nuclear digital instrumentation and control systems. The Nucleus, Vol 46, No 4 2009;46:415–28.

[33] Tantawy A, Abdelwahed S, Erradi A, Shaban K. Model-based risk assessment for cyber physical systems security. Computers and Security 2020;96. https://doi.org/10.1016/J.COSE.2020.101864.

[34] Aven T. A unified framework for risk and vulnerability analysis covering both safety and security. Reliability Engineering and System Safety 2007;92:745–54. https://doi.org/10.1016/j.ress.2006.03.008.

[35] Klinke A, Renn O. A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies . Risk Analysis 2002;22:1071–94. https://doi.org/10.1111/1539-6924.00274.

[36] Kristensen V, Aven T, Ford D. A new perspective on Renn and Klinke's approach to risk evaluation and management . Reliability Engineering & System Safety 2006;91:421–32. https://doi.org/10.1016/j.ress.2005.02.006.

[37] Antón PS, Anderson RH, Mesic R, Scheiern M. Finding and Fixing Vulnerabilities in Information Systems. 1st ed. RAND Corporation; 2003.

[38] Cormier A, Ng C. Integrating cybersecurity in hazard and risk analyses. Journal of Loss Prevention in the Process Industries 2020;64:104044. https://doi.org/10.1016/j.jlp.2020.104044.

[39] Tantawy A, Abdelwahed S, Member S, Erradi A. Cyber LOPA: An Integrated Approach for the Design of Dependable and Secure Cyber Physical Systems 2020.

[40] Willey RJ. Layer of Protection Analysis. Procedia Engineering 2014;84:12–22. https://doi.org/10.1016/J.PROENG.2014.10.405.

[41] Cormier A, Ng C. Cybersecurity consideration in process hazard analysis. Global Congress on Process Safety 2018, GCPS 2018 - Topical Conference at the 2018 AIChE Spring Meeting and 14th Global Congress on Process Safety 2018;3:1938–47.

[42] IEC. IEC 62443-3-2: Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design. Geneva: International Electrotechnical Commission; 2020.

[43] NIST. SP 800-30: Information Security - Guide for conducting risk assessments. 2012.

[44] ISO/IEC. ISO/IEC 27005: Information technology — Security techniques — Information security risk management. Geneva: International Organization for Standardization and International Electrotechnical Commission; 2018.

[45] Cusimano J. Safety Requires Cybersecurity. Control Engineering 2017:22–4.

[46] Anon. aeCyberPHA® Cyber Risk Assessment Methodology. Facebook 2020:1. https://www.facebook.com/aesolutions/videos/636807276892841/.

[47] Morella J. CyberPHA - A proven method to assess industrial control system cybersecurity risk 2019:33.

[48] Cusimano J, Da Costa C. Cyber Process Hazards Analysis (PHA) to Assess ICS Cybersecurity Risk. USA: S4 ICS Security Conference; 2017.

[49] Anon. Are you prepared for cyber attacks? Exida Web Site 2021:1. https://www.exida.com/exsilentiacyber.

[50] O´Brien P. The Cybersecurity Lifecycle (IEC 62443) and exSILentia Cyber. Exida Webinar 2020.

https://www.youtube.com/watch?v=staiJE4Aooo.

[51] Swiderski F, Snyder W. Threat Modeling. Microsoft Press; 2004.

[52] Application Threat Modeling using DREAD and STRIDE n.d. https://haiderm.com/application-threat-modeling-using-dread-and-stride/ (accessed December 22, 2021).

[53] Fockel M, Merschjohann S, Fazal-Baqaie M. Threat analysis in practice – Systematically deriving security requirements. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 11271 LNCS, Springer Verlag; 2018, p. 355–8. https://doi.org/10.1007/978-3-030-03673-7_25.

[54] Rouland Q, Hamid B, Jaskolka J. Specification, detection, and treatment of STRIDE threats for software components: Modeling, formal methods, and tool support. Journal of Systems Architecture 2021;117:102073. https://doi.org/10.1016/j.sysarc.2021.102073.

[55] Tolo S, Andrews J. Nuclear Facilities and Cyber Threats 2019. https://doi.org/10.3850/981-973-0000-00-0.

[56] Khan R, McLaughlin K, Laverty D, Sezer S. STRIDE-based threat modeling for cyber-physical systems. 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe, ISGT-Europe 2017 - Proceedings, vol. 2018- Janua, 2017, p. 1–6. https://doi.org/10.1109/ISGTEurope.2017.8260283.

[57] Carreras Guzman NH, Zhang J, Xie J, Glomsrud JA. A Comparative Study of STPA-Extension and the UFoI-E Method for Safety and Security Co-analysis. Reliability Engineering & System Safety 2021;211:107633. https://doi.org/https://doi.org/10.1016/j.ress.2021.107633.

[58] Carreras Guzman NH, Kozine I, Lundteigen MA. An integrated safety and security analysis for cyber-physical harm scenarios . Safety Science 2021;144:105458. https://doi.org/10.1016/j.ssci.2021.105458.

[59] Carreras Guzman NH. CyPHASS prototype: Cyber-Physical Harm Analysis for Safety and Security 2021:1. https://orbit.dtu.dk/en/projects/cyphass-prototype-cyber-physical-harm-analysis-for-safety-and-sec.

[60] Bochman AA, Freeman S. Countering cyber sabotage : introducing consequence-driven, cyber-informed engineering (CCE). CRC Press, Taylor & Francis Group; 2021.

[61] Reif M, Gellner JR, St Michel CP, Kuipers DG. CCE Case Study: Stinky Cheese Company. United States: 2020.

[62] Anderson R, Smith R. Consequence-driven Cyber-Informed Engineering. International Conference on Nuclear Security 2020, Vienna: International Atomic Energy Agency; 2020.

[63] Anon. Consequence-Driven Cyber-Informed Engineering. Idaho National Laboratory CCE Web Site 2021:1. https://inl.gov/cce/.

[64] Tippenhauer NO, Temple WG, Vu AH, Chen B, Nicol DM, Kalbarczyk Z, et al. Automatic Generation of Security Argument Graphs. 2014 IEEE 20th Pacific Rim International Symposium on Dependable Computing, Dependable Computing (PRDC), 2014 IEEE 20th Pacific Rim International Symposium on, Dependable Computing (PRDC), 2013 IEEE 19th Pacific Rim International Symposium On 2014:33–42.

[65] Chen B, Tan R, Temple WG, Tippenhauer NO, Vu AH, Yau DKY, et al. Go with the flow: Toward workflow-oriented security assessment. ACM International Conference Proceeding Series, 2013, p. 65–76.

[66] Jauhar S, Chen B, Temple WG, Dong X, Kalbarczyk Z, Sanders WH, et al. Model-Based Cybersecurity Assessment with NESCOR Smart Grid Failure Scenarios. 2015 IEEE 21st Pacific Rim International Symposium on Dependable Computing (PRDC) 2015:319–24.

https://doi.org/10.1109/PRDC.2015.37.

[67] Temple WG, Li Y, Tran BAN, Liu Y, Chen B. Railway system failure scenario analysis. vol. 10242 LNCS. Springer Verlag; 2017.

[68] Vu AH, Tippenhauer NO, Chen B, Nicol DM, Kalbarczyk Z. CyberSAGE: A tool for automatic security assessment of cyber-physical systems. vol. 8657 LNCS. Springer Verlag; 2014.

[69] Anon. CyberSAGE. A Web Page of The University of Illinois at Urbana–Champaign 2015:1. https://www.illinois.adsc.com.sg/cybersage/index.html.

[70] Goel R, Kumar A, Haddow J. PRISM: a strategic decision framework for cybersecurity risk assessment. Information and Computer Security 2020;28:591–625. https://doi.org/10.1108/ICS-11-2018-0131.

[71] Leveson N. Engineering a safer world: Systems Thinking Applied to Safety. The MIT Press; 2012.

[72] Leveson N, Thomas J. STPA Handbook. 2018.

[73] Young W, Porada R. System-Theoretic Process Analysis for Security (STPA-SEC): Cyber Security and STPA. 2017 STAMP Conference, Boston, MA: 2017.

[74] Friedberg I, McLaughlin K, Smith P, Laverty D, Sezer S. STPA-SafeSec: Safety and security analysis for cyber-physical systems. Journal of Information Security and Applications 2017;34:183–96. https://doi.org/10.1016/J.JISA.2016.05.008.

[75] SAE International. System Theoretic Process Analysis (STPA) Recommended Practices for Evaluations of Automotive Related Safety-Critical Systems - SAE International. SAE International; 2022.

[76] Anon. Using STPA During Development and Safety Assessment of Civil Aircraft - AIR6913 2018:1. https://www.sae.org/standards/content/air6913/.

[77] de Souza Borges SF, de Albuquerque MAF, Cardoso MM, Belderrain MCN, da Costa LEL. Systems theoretic process analysis (STPA): A bibliometric and patents analysis. Gestao e Producao 2021;28. https://doi.org/10.1590/1806-9649-2020V28E5073.

[78] Alexander O, Belisle M, Steele J. MITRE ATT&CK® for Industrial Control Systems: Design and Philosophy. McLean: 2020.

[79] Hakim S, Blackstone EA, Clark RM. Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level. Spronger; 2017. https://doi.org/10.1007/978-3-319-32824-9.

[80] Anon. ATT&CK® for Industrial Control Systems. A Web Page of The MITRE Corporation 2021:1. https://collaborate.mitre.org/attackics/index.php/Main_Page.

[81] Matherly J. Complete Guide to Shodan - Collect. Analyze. Visualize. Make Internet Intelligence Work for You. Shodan, LLC; 2017.

[82] Radiflow. CIARA - Cyber Industrial Automated Risk Analysis 2021:1. https://radiflow.com/products/ciara-cyber-industrial-automated-risk-assessment/.

[83] Bean D. Securing OT Systems Against Cyber-attack. Control Engineering Europe 2021:1.

[84] Anon. Get to Know ARCHx. Exida Web Site 2021. https://www.exida.com/archx.

[85] Alanen J, Linnosmaa J, Tommila T. Conformity assessment data model. Finland: VTT Technical Research Centre of Finland; 2017.

[86] Linnosmaa J, Alanen J. Demonstration of a conformity assessment data model. 17th IEEE International Conference on Industrial Informatics, IEEE; 2019.