Quantitative Security Risk Assessment for Industrial Control Systems: Research Opportunities and Challenges

Matthias Eckhart[1,2*], Bernhard Brenner[1,2], Andreas Ekelhart[1,2], and Edgar Weippl[1,2]
[1]Christian Doppler Laboratory for Security and Quality Improvement
in the Production System Lifecycle, TU Wien, Vienna, Austria
{firstname.lastname}@tuwien.ac.at
[2]SBA Research, Vienna, Austria

Abstract

Due to the gradual implementation of the Industry 4.0 vision, information technology is becoming increasingly important in industrial control systems (ICSs), such as production systems. Although the digital transformation of ICSs represents the foundation for resource-efficient and flexible industrial plants, this change increases the attack surface, leading to the emergence of new threats. Moreover, ICSs constitute an attractive target for attackers who may disrupt plant operation, causing severe physical/material damages (PD/MD), such as machinery breakdowns. In further consequence, asset owners (i.e., plant operators) may suffer from business interruption (BI) and loss of profit (LOP). Thus, security risks must be managed in all phases of the ICSs' lifecycle, starting from engineering to decommissioning. Risk assessment is an integral part of the risk management process in which risks are identified, analyzed, and evaluated. In this context, the quantitative assessment is vital, since measuring cyber risks is required to establish an effective decision-making process for security investments. This survey article reviews the state of the art concerning quantitative security risk assessments for ICSs and identifies promising opportunities for future research and associated challenges. We report that the current state of quantitatively assessing cyber risks for ICSs is characterized by the absence of adequate (dynamic) security risk assessment methods tailored to the peculiarities of ICSs. This is aggravated by the fact that the complexity of the threat landscape increases in the light of Industry 4.0, and historical data on security incidents is lacking. As a consequence, asset owners may fail to quantitatively assess their cyber risk exposure, leaving them uncertain about security decisions. Furthermore, if they purchase cyber insurance in order to transfer the risks of non-PD BI, the underlying problem remains unsolved as (re)insurers potentially take on these unassessed risks. As an initial step to guide individuals seeking to improve the quantification of cyber risks pertaining to ICSs, this article concludes by outlining several directions for further research that are worth pursuing.

Keywords: Information Security, Industrial Control Systems, Security Risk Assessment, Cyber Risk Quantification, Cyber Insurance

1 Introduction

In the light of the precarious threat landscape of industrial plants as well as the complex interconnections among (i) vendors, (ii) systems integrators, (iii) operators, (iv) insurers, and (v) reinsurers, security risks[1] pertaining to industrial control systems (ICSs) must be managed in a holistic and systematic manner in order to mitigate potential consequences of cyber attacks. In line with the expression of how risks and hazards interrelate, provided by Kaplan and Garrick [58], viz., $risk = hazard/safeguards$, holistically

Journal of Internet Services and Information Security (JISIS), volume: 9, number: 3 (August, 2019), pp. 52-73

*Corresponding author: SBA Research, Floragasse 7, Vienna, Austria, Tel: +43 (1) 505 36 88, Web: https://www.sba-research.org/team/researchers/matthias-eckhart/

[1]Following the definition given by Coburn et al. [19], *"[r]isk means the likelihood of loss."*

managing security risks for ICSs means that all of the aforementioned parties have to mitigate security threats (i.e., hazards or sources of danger) by applying safeguards (e.g., security measures) in a way that will lead to an acceptable level of risk. According to the ISO 31000 [2], the international standard for risk management, the assessment of risks can be considered as a core element of the risk management process. This includes the following subprocesses: (i) risk identification, (ii) risk analysis, and (iii) risk evaluation [2]. In essence, first, the sources of risks and potential consequences are identified, then the likelihood and impact of risks are analyzed, and, finally, the risks are evaluated to assess the need for subsequent treatment [2]. This standard for risk management leaves the choice of the risk analysis method to users [2]. Although multiple security guidelines and standards (e.g., VDI/VDE 2182 [109]) suggest a qualitative approach (typically based on a scoring system and represented as a risk matrix or heatmap), there appears to be a growing trend toward the use of quantitative methods. The reason for this is that qualitative security risk assessment approaches have been subjected to considerable criticism (cf., for instance, [52, 38, 13]) due to their inherent vagueness. Quantitative risk assessments, on the other hand, aim to provide quantitative estimates of the uncertainty of potential outcomes of events [110]. Obtaining a quantitative understanding of risks can support the decision-making process and is therefore beneficial for improving information security in a cost-effective manner [39]. The IEC 62443 series of standards for ICS security even declares that the definition of security levels and requirements in quantitative terms represents a long-term goal, making cyber risk quantification methods eventually indispensable in the context of ICSs [1, 3]. Toward this end, all three risk assessment steps should foster a quantitative understanding of the security risk exposure.

Quantitative risk assessment methods for assessing the ICS's safety and reliability (e.g., the quantitative analysis of fault trees) are already well established in the engineering domain [66, 21]. Engineers are actively involved in safety risk assessments, since they provide system knowledge that is essential for understanding the involved risks. Extending this notion to the security domain, methods for quantitatively assessing security risks need to be applicable in production systems engineering (PSE) in order to take advantage of the knowledge that engineers acquire when developing and integrating these systems. Thus, engineers and security analysts may regularly assess the security risks of the ICS to be developed during engineering. In line with the procedural method defined in the VDI/VDE 2182 guideline [109], systems integrators may then hand over results of quantitative risk assessments in addition to the external technical documentation. Asset owners could use these results as a basis for ongoing security risk assessments.

Although standards and regulations, especially in connection with cyber insurance, appear to gradually shift to a quantitative risk-based approach, it still seems that the wide adoption of cyber risk quantification methods remains a vision for the future. Yet, existing survey papers [21, 18] indicate that quantitative ICS security risk assessment is an active field of research within the scientific community, as numerous methods have been proposed thus far. It is therefore necessary to identify unresolved issues, challenges and concerns that need to be addressed by researchers. The work at hand aims to shed light on these unexplored topics. More specifically, the contributions of the article are twofold. First, we review scientific works that fall within the scope of quantitative ICS security risk assessment with the objective to extend existing survey papers on this subject [21, 18]. Second, we highlight research issues that remain to be addressed and provide pointers to research directions that seem to be promising.

The remainder of this article is organized as follows. Section 2 provides background information to establish the context of the work. Section 3 discusses the state of the art concerning (i) threat modeling and security analysis, and (ii) cyber risk quantification, both in the context of ICSs, as we consider these areas fundamental for quantitatively assessing ICS security risks. Based on this, Section 4 presents gaps in the literature and possible future research directions. Finally, concluding remarks are given in Section 5.

2 Background

ICSs can be considered as a subset of cyber-physical systems (CPSs), meaning that the behavior of the "cyber part" of the systems interrelate with the activities that take place within the physical world. As a result, the threat landscape is fundamentally different from that of purely software-based systems. Following the CPS attack taxonomy described in [118], threat actors can launch (i) cyber-to-cyber, (ii) cyber-to-physical, (iii) physical-to-physical, and (iv) physical-to-cyber attacks against CPSs. In other words, threats can not only emerge via the cyber and physical domain, but also endanger assets in both of them. For instance, an adversary may launch a cyber-to-physical attack by remotely exploiting a vulnerability in a programmable logic controller (PLC) to manipulate control parameters, creating low water conditions in a boiler that will cause severe damages to the equipment (cf. [8] for a description of potential cyber-physical threat scenarios). The physical properties add another layer of complexity to assessing security risks, due to the fact that the process under control is closely related to the system under consideration and therefore cannot be ignored. The importance of the physical domain in the context of securing ICSs can be illustrated using findings from intrusion detection research. Adversaries with a deep understanding of their attack target may be able to trigger actions that are legitimate per se, but if viewed holistically (e.g., in relation to preceding control commands), clearly put the system in an unsafe state (countermeasures have been presented, e.g., in [37, 16]). It is evident that to estimate the risks of such sophisticated attacks, knowledge of the underlying physical process is required.

In addition to physical effects, there are several other aspects that are central to the assessment of ICS security risks. The following considerations further motivate our effort to identify research gaps.

A Changing Threat Landscape In essence, attacks may be executed on any level of the automation pyramid according to IEC 62264-3 [4], viz., (i) physical process level, (ii) field level (e.g., sensors, actuators, controllers), (iii) supervisory level (i.e., SCADA), (iv) operations level (i.e., MES), and (v) enterprise level (i.e., ERP). Strategic initiatives such as Industry 4.0 [57] call for an enhanced connectivity between these levels and the integration of modern IT systems into ICSs, causing the information and operational technology (IT/OT) domains to converge [44]. This convergence contributes to the expansion of the attack surface of ICSs and, hence, leads to drastic changes of the threat landscape. The increased risk of attacks emanating from cyber space requires novel approaches that yield an efficient and manageable threat modeling process for ICSs.

The Importance of Threat Modeling Threat modeling aims to identify and evaluate attack vectors [100] and can therefore support the assessment of security risks. This activity is typically performed early in the development lifecycle with the objective to identify design issues [100] and, as such, cannot be considered as a substitute for other security-improving efforts (e.g., secure coding practices, penetration tests). However, given the importance of taking security aspects along the PSE process [29] into account and, in particular, during the design phase, threat modeling represents a vital part of security-aware engineering. The developed threat models aid in identifying risk sources and may also further advance the knowledge of possible consequences. Moreover, certain techniques also enable a quantitative understanding of potential threats (e.g., attack–defense trees [62]).

The Need for Cyber Risk Quantification As already indicated, qualitative risk assessments, in which risks are typically categorized in risk classes (e.g., low, medium or high), appear to be predominant. Although this approach may be more convenient to apply and requires less effort by tendency, the estimates are typically vague [13]. Moreover, analysts may rely on numerical estimates in the decision-making process for security investments [39]. In particular, the treatment of risks should be driven by the cost-

effectiveness of controls. In other words, the implemented security measures should reduce the risks to an acceptable level so that the mitigation costs do not exceed the potential loss incurred by an incident. As obvious as this may seem, risks are in practice often not treated in a cost-effective manner. For instance, the findings of a study conducted by Stewart and Mueller [102] suggests that, given the observed probabilities of terrorist attacks on airports, the costs of airport security measures to prevent them are too high. While this study is not related to information security per se, the results highlight the importance of a cost-benefit analysis, which evidently follows a quantitative approach. Besides the cost-effective treatment of security risks, which primarily concerns vendors, systems integrators, and asset owners, quantitative methods are also vital to the cyber insurance underwriting process (e.g., to calculate the economic impact of security incidents). In the supervisory statement 4/17, published in 2017, the Prudential Regulation Authority states that it *"[...] expects firms to be able to identify, quantify and manage cyber insurance underwriting risks"* [90]. These expectations apply to Solvency II firms, referring to affirmative as well as non-affirmative cyber risk. In particular, a special emphasis is placed on non-affirmative cyber risk, i.e., cyber risk that may be implicitly included in insurance policies [90]. According to this supervisory statement, firms are expected to reduce the "silent" cyber risk exposure, i.e., policies that do not explicitly exclude cyber risk coverage [90]. As the Prudential Regulation Authority suggests, firms may (i) increase premiums and offer explicit cover for cyber risks, (ii) introduce exclusion clauses, and/or (iii) limit cover for cyber risks [90]. To achieve these regulatory requirements, the quantification of cyber risks is crucial for (re)insurance providers.

Managing Complexity through Knowledge Transfer In [18], Cherdantseva et al. determined that risk assessment methods for ICSs may be characterized by a fragmented, disintegrated consideration of the steps in the risk management process. In particular, Cherdantseva et al. [18] point out that establishing the context for the risk management process, according to ISO 31000 [2], is prone to be neglected, because risk analysts may not be able to reduce the complexity of ICSs to manageable levels without omitting fundamental factors, such as the interdependencies of systems. It can be argued that the VDI/VDE 2182 [109] guideline attempts to counter this problem. As this guideline specifies, the activities of vendors, integrators, and operators should be viewed holistically when protecting ICSs, as actions taken by all three parties may affect the security throughout the systems' lifecycle. In particular, the procedure model proposed in the VDI/VDE 2182 [109] guideline suggests that vendors, integrators and operators work together by exchanging requirements and documentation regarding the security of ICSs. However, since industrial espionage in the context of PSE is a major concern [60], the realization of this approach is challenging. The lack of adequate security mechanisms to protect the PSE process further exacerbates this issue [113, 60].

The Scarcity of Historical Data In addition, numerous sources (e.g., [18, 21, 94, 114]) state that reliable data on cyber incidents, which would aid the cyber risk quantification step (to derive the likelihood and severity of attacks), is scarce. While property underwriters can rely on an abundance of data and experiences gained over the past several decades, underwriting cyber risks is in its infancy. Information sharing strategies, e.g., as suggested by the World Economic Forum [114], are an attempt to improve the availability of data. Also, this type of risk is still poorly understood. The consequences of cyber attacks against ICSs can be diverse, highly depend on the system under consideration, and can even result in cascading effects. Downtime in manufacturing that causes business interruption (BI) and the resulting loss of profit (LOP), physical/material damages (PD/MD), (vapor) cloud explosion in petrochemical processes, or erroneous product output of industrial processes are the main manifestations of possible negative impacts from cyber attacks against ICSs. The estimation of the potential frequency or probability of cyber attacks is even more complex, since attack vectors and the attackers' abilities are highly

dynamic variables. Failure to deal with this complexity could induce incorrect assumptions concerning security threats, resulting in too simple, transparency lacking cyber risk models. This may in turn fuel skepticism regarding the use of quantitative methods.

Cyber Accumulation The modeling of cyber accumulation poses a further issue that reinsurers must address. When calculating risks of natural hazards (e.g., flood), underwriters can assess the risk exposure with a certain level of confidence, since, for example, a single event is typically geographically bound. As past cyber epidemics have shown, this is not the case when calculating cyber risks. For instance, the *WannaCry* ransomware attack affected more than 200,000 computers in 150 countries, including ICSs (e.g., factories of Nissan, Renault, and Honda) [85]. Since ICSs are not only used in manufacturing, but also in critical infrastructure sectors (e.g., energy), the global spreading of malware could lead to a worldwide "cyber catastrophe". In a worst-case scenario, multiple reinsurers cannot deal with such accumulated events (e.g., caused by a zero-day vulnerability affecting ICSs), potentially leading to a collapse of the insurance industry. This extreme, but still plausible scenario would have a devastating impact on the economy with long term consequences for our society. As a result, the quantification, monitoring and effective management of cyber accumulation deserves particular attention.

The Dynamic Nature of Security Risks Irrespective of whether the insured or the (re)insurer quantifies cyber risks in the course of their risk management or underwriting process, both parties must take account of the dynamics of the risk exposure. It can be argued that this is less relevant to safety risk assessments, where failure behavior leading to hazardous events are comparatively more predictable and better understood [66]. Security-relevant quantitative parameters, such as the probability of a successful attack or the time to compromise, are not static, but rather change continuously during the system's lifecycle. As a matter of fact, cyber risks can change rapidly, and a single discovered vulnerability may concern a multitude of systems. In this context, the recently exposed *Meltdown* [77] and *Spectre* [61] vulnerabilities, which affect numerous modern processors, serve as prime examples. In addition to newly disclosed security weaknesses, adversary behavior constantly changes. Thus, adversary groups, targeted attack campaigns, and attack trends need to be monitored to ensure that the obtained view on cyber risks is current.

3 A Brief Review of the State of the Art

In the following, we give a synopsis of relevant literature, providing a basis for the identification of research gaps presented in Section 4.

3.1 Threat Modeling & Security Analysis for Industrial Control Systems

Due to the changing threat landscape and the increasing complexity of CPSs, including ICSs, a systematic and efficient approach to threat modeling is required. Over the past few years, researchers published numerous works that attempt to address this challenge.

In particular, several papers have been published on system-centric CPS threat modeling approaches. When applying such a system- or software-centric modeling approach, the system (or software) under consideration is first modeled and then used as a basis for finding threats [100]. Data flow diagrams (DFDs) are widely used for representing system components and how data is transferred among them [100]. In [117], the authors evaluate the applicability of DFDs to the CPS domain and extend them with multiple elements that enable users to represent cyber-physical components and interactions. Based on the DFDs, threats can be analyzed, for instance, by applying STRIDE. STRIDE is a mnemonic for

six types of security threats, viz., (i) Spoofing, (ii) Tampering, (iii) Repudiation, (iv) Information Disclosure, (v) Denial of Service, and (vi) Elevation of Privilege [100]. Khan et al. [59] have adopted this way of modeling threats, as their proposed five-step CPS threat modeling methodology utilizes DFDs and STRIDE. To demonstrate how their proposed approach can be put to use, the authors of [59] enumerated threats according to STRIDE using a real-world example, namely a synchrophasor-based system. In [120], Zalewski et al. investigate how the DREAD model [103] and the Common Vulnerability Scoring System (CVSS)[2] can be used for the assessment of threats in CPSs. The authors have utilized the developed threat models for obtaining the transition probabilities of a Discrete-Time Markov Chain (DTMC) model, which may provide insights into the CPS behavior when under attack. In this way, conclusions concerning the degrading performance or even total failure of CPSs, induced by attacks, can be drawn. Guan et al. [43] have proposed the use of directed graphs for modeling the structural and behavioral characteristics of ICSs for the purpose of risk identification. The authors have shown the benefits of their method (viz., simplicity, flexibility, and preciseness), using a distillation column as a real-world example. Furthermore, there have been research efforts to structure system-centric CPS threat modeling for the purpose of automated processing. In [79], Martins et al. present a threat modeling tool that builds upon the Generic Modeling Environment (GME) [71] to design a metamodel representing the components of CPSs. As the authors have shown in a case study using a real-world railway temperature monitoring system, the model can be analyzed in a systematic fashion owing to the utilization of GME interpreters. Schlegel et al. [98] have attempted to address the issue of bridging the gap between specificity and generality from which existing CPSs threat modeling tools appear to suffer. Their proposed methodology is based on (i) a data model, which includes elements to represent components, threats, impacts, and security control, and (ii) relationships between these elements. Owing to this flexible data model, the authors of [98] claimed that the attainable level of detail of threat models is at the user's discretion, and algorithms can be designed that automate the analysis.

In addition to system-centric approaches, researchers also studied threat modeling methods in the context of ICSs that focus on the attackers' perspective (e.g., attack steps, capabilities, cost to attack). For instance, CPS misuse patterns [35] can be used to specify the steps of complete attacks on the basis of architectural aspects. Several scholars (e.g., [15, 108, 115, 96]) also proposed to leverage attack trees (or a variant thereof) for identifying security threats pertaining to ICSs. Attack trees allow to describe attacks against a system in a tree structure (i.e., the root represents the attacker's goal and subnodes the steps to achieve the goal) [99]. The beauty of adopting attack trees for threat modeling is that its applicability certainly goes beyond the mere identification of risk sources. In particular, the survey paper published by Kordy et al. [63] indicates that the concept of attack trees is widely used for risk quantification purposes. Moreover, research has revealed that attack trees can be automatically generated for analyzing the security of CPSs and the underlying engineering processes. For example, while Lemaire et al. [74] and Depamelaere et al. [23] proposed such methods for conducting CPS security analyses, Eckhart et al. [30] focused on the security of a subprocess of PSE (namely, the testing of industrial automation software).

It is also worth noting that progress has been made toward developing software tools that support users in conducting CPS security analyses. Lemaire et al. [73] reviewed five tools that have been developed for this purpose, viz., *CSET*[3], *Cyber Security Modelling Language (CySeMoL)* [47, 101], *ADVISE* [76, 36], *FAST-CPS* [72, 75], and *CyberSAGE* [111]. The authors performed an evaluation using a real-world case study and compared them by means of their required input and the provided output [73]. Interestingly, their comparison has shown that there are significant differences among the tools regarding their input/output and that none of the tools is clearly superior. In view of the overall theme of this article,

[2] `https://www.first.org/cvss`
[3] `https://cset.inl.gov`

it is noteworthy that CySeMoL, ADVISE, and CyberSAGE have quantitative analysis capabilities.

It is self-evident that the quality and usefulness of the output of security analysis tools depends on the input (e.g., details concerning the system's architecture). In the context of (input) knowledge representation, researchers can also build upon prior work on developing information security knowledge models, for instance, by means of ontologies. Works such as [32, 31, 34, 45, 83] discuss ontology-based knowledge models for IT security, while [106] proposes one specifically for the OT domain. Owing to the formal representation of security-relevant information, it has been demonstrated in [42, 41, 105] that such knowledge-based approaches are particularly well suited for automating ICS security analyses. The sources required for establishing an ICS-specific security knowledge base have been studied in [104].

In addition to ontology-based approaches, some research efforts have been made in developing risk assessment methods that utilize a (semi-)formal model representation of the system(s) under consideration. For instance, Apvrille and Roudier [6, 7] introduced *SysML-Sec*, i.e., a security extension for SysML that enables engineers to represent security properties as part of SysML diagrams and allows the formal verification thereof (cf. [95] for a review on the state of model-based security risk assessment in the context of CPSs). Moreover, as the survey papers [78, 66] indicate, model-driven risk assessment approaches may enable users to leverage the synergies between security and safety and provide the means to conduct a combined analysis.

3.2 Quantifying Industrial Control Systems Security Risks

The issue of cyber risk quantification received considerable attention from academics over the past two decades. Among the earliest works that stresses the importance of quantitative security risk assessments was published by Geer et al. [39] in the early 2000s. Since then, numerous papers have been written about leveraging probabilistic risk assessment (PRA) methods to quantify security risks [18].

In the ICS domain, PRA methods are prevailing when assessing security risks [18] and, according to Cook et al. [21] are even considered as the de-facto standard. When conducting a PRA, probabilities of undesirable scenarios, which consist of sequences of events (beginning with a start state and leading to an undesirable end state), are obtained based on historical or subjective data using statistical methods (e.g., Monte Carlo simulations, Bayesian networks, Markov models) [21, 18]. These PRA methods are also incorporated into methodologies to provide a systematic process on how they can be utilized.

The Factor Analysis of Information Risk (FAIR) [38] is one such methodology. Its underlying analysis process consists of (i) building scenarios on the basis of factors of risks to establish the analysis scope, (ii) acquiring expert estimates and modeling them using PERT distributions, and (iii) performing Monte Carlo simulations for stochastic modeling [38]. Hubbard and Seiersen [52] also promote PRAs and provide a comprehensive analysis on cyber risk quantification utilizing Monte Carlo simulations and Bayesian methods. Furthermore, the authors describe an approach that aims to calibrate the estimates from domain experts, which is central to FAIR, too [38]. In [112], cyber attack scenarios, targeting an instrumentation and control system of a nuclear reactor, have been generated using Monte Carlo sampling and quantitatively evaluated to determine their effects. Baiardi et al. [11, 9, 12, 10] also published several papers on utilizing the Monte Carlo method for conducting PRAs to quantify cyber risks. They introduce in [11] a tool named *Haruspex* that receives as input threat scenarios (based on a description of the system and attacker models) and uses the Monte Carlo method to obtain the success probability of simulated attacks. In subsequent works, the authors improve Haruspex by integrating a description builder (i.e., a tool that facilitates creating the scenario description) [9], extend the notion of Value at Risk (VaR) [56] by introducing *CyVar* [12], propose a robustness metric named *security stress* [10], and demonstrate their contributions based on an exemplary ICS [9, 12, 10]. CyVar [12] is of particular interest, as this risk measure indicates how robust a system is with respect to cyber attacks (measured in terms of the time it takes for an adversary to gain a foothold in the system) and the loss incurred (measured in

terms of the time an adversary has to achieve the attack goal).

In this context, it is worth reviewing VaR in order to understand how this notion has evolved from a risk measure commonly used in finance [56, 53] to one that finds its way into the information security domain. Simply put, VaR measures the maximum loss in value over a specific time frame that will not be exceeded with a given confidence level [56, 53]. Following the introductory example of VaR described in [56], a financial institution may calculate that for a time window of one trading day the VaR of its portfolio is \$50MM at the 99% confidence level, meaning that the probability of exceeding the loss of \$50MM is 1%. Controlling risk based on this measure is thoroughly understood [56, 53], which may make its application also appealing to decision makers in charge of information security investments. Indeed, CyVar proposed by Baiardi et al. [12] is not the only work that builds upon VaR. As a matter of fact, several others exist [93, 68, 114, 54, 97, 86] that discuss the application of VaR in the context of cyber risk quantification. For instance, in 2013, Raugas et al. introduced the *CyberPoint CyberV@R* model [93], which takes as input attack trees (augmented with information about countermeasures, assets, and the infrastructure) and computes a probability distribution representing the loss likelihood for a given time frame, allowing to calculate the value at risk. Bayesian networks (constructed based on the attack trees) and Monte Carlo simulations represent vital parts of CyberV@R, since they are used for modeling joint probability distributions of losses and for random sampling to compute VaR, respectively [93]. In addition to CyberV@R, the World Economic Forum (WEF) started an initiative that led to the *cyber value-at-risk* (Cyber VaR) concept [114]. Cyber VaR comprises three main components that need to be considered when quantifying the VaR induced by cyber threats, viz., vulnerabilities (e.g., as per known weaknesses and defenses in place), assets (tangible and intangible), and the profile of attackers (e.g., types and motivation of adversaries) [114]. Although the report does not provide a detailed description on how to calculate Cyber VaR, it suggests the use of Monte Carlo simulations [114]. Cyber risk practitioners from Deloitte further developed the Cyber VaR model and showed in a case study with major Dutch organizations how it can be applied [54]. Ruan [97] introduced the units *BitMort* and *hekla* based on MicroMort [48] and VaR, which can be used for measuring the economic impact of cyber risks pertaining to digital assets. A similar rationale is behind *IoT MicroMort* [92], i.e., a cyber risk unit specifically for the Internet of Things (IoT). While it can be argued that in industrial facilitates safety is paramount and digital assets (e.g., personally identifiable information, intellectual property) take on a secondary role in terms of their criticality, a gradual increase of their digital value and the prevalence in ICSs appears to be associated with the adoption of Industry 4.0 applications (e.g., due to the processing of trade secrets and potentially sensitive customer requirements for the purpose of mass customization).

As already indicated, Bayesian networks have been proposed in the literature for the quantitative analysis of security risks (e.g., [116]). *Bayesian Attack Graphs (BAGs)* [89] represent a valuable extension of Bayesian networks, as they enable to model dynamic security aspects. In particular, the beauty of BAGs is that information concerning occurred incidents can be factored into attack graphs in order to update the probabilities of nodes in the attack chain, meaning that different outcomes of attacks are reflected [89].

Researchers from KTH have developed the CySeMoL [47, 101] that builds upon a template for a probabilistic relational model (PRM) [40], which enables the generation of a Bayesian network from an object model, representing the system architecture to be analyzed, attack steps and countermeasures. Based on the user-supplied input, the implementation of CySeMoL provides likelihood estimates for cyber attacks, which are carried out by a penetration tester against the modeled system within one week. In a subsequent work [46], the authors propose the *Predictive, Probabilistic Cyber Security Modeling Language (P^{2}CySeMoL)* that extends the CySeMoL's scope, improves its computational efficiency and relaxes attack assumptions. Other scholars from KTH have also taken up the challenge of developing cyber risk quantification methods. In [55], Johnson et al. have introduced *pwnPr3d* that constructs attack graphs from a system model and estimates the attack likelihood by means of probability distributions

over the time-to-compromise for attack steps in the graphs.

Security modeling with *Boolean logic Driven Markov Processes (BDMP)* [88], which are composed of attack trees whose leaves are represented as Markov processes, provide another way of performing dynamic security risk assessments. The authors state that the proposed approach is well qualified for this use case, due to the powerfulness and expressiveness of the BDMP formalism while ensuring that its models are still readable and scale. Le and Hoang [70] have also studied Markov processes and their use for modeling security threats. Their proposed method is based on Markov chains and the transition matrices are derived from CVSS scores.

It seems that the aforementioned underlying probabilistic models also lend themselves well to assessing security risks in ICSs, since the approaches proposed in the literature are based on, inter alia, Bayesian networks and Markov models. Table 1 provides an overview of relevant works on quantitative security risk assessment methods that have been applied in the ICS domain.

On a final note, in contrast to quantitative security risk assessment methods for (business) IT systems, taking on a control theory perspective on risk assessment for ICSs can be particularly advantageous [107]. This perspective is also worth considering when quantifying the physical and economic impact of cyber attacks against ICSs [51, 84, 50].

4 Issues, Challenges, and Future Research Directions

The purpose of this section is twofold: First, we highlight open research issues that have been determined by reviewing the state of the art in the area of quantitative security risk assessment for ICSs. Second, based on the discussed open problems, we derive research directions that seem to be worth pursuing.

4.1 Research Issues & Challenges

In the following, we discuss research issues and challenges that primarily concern systems integrators and asset owners. The rationale behind focusing on these two parties is that they are in the position to draw on existing knowledge gained from engineering and operating ICSs, which can be leveraged for cyber risk quantification purposes. Efforts to promote the sharing of information on security risks among organizations (e.g., as per the WEF's virtuous circle of cyber quantification [114] or the executive order 13691 issued by President Obama [82]) have been initiated with the notion that they are aware of cyber risks and capable of maintaining relevant information. We hypothesize that addressing the identified research issues will enable systems integrators and asset owners to obtain more reliable estimates of security risks. In this way, information sharing among organizations may gain momentum, which would clearly have a positive impact on the cyber insurance industry as well.

An Insufficient Integration of Security Modeling Languages into PSE As indicated in Section 3.1, representing security know-how to aid risk identification is a major area of interest within the field of information security. Although relevant modeling approaches proposed in existing works (e.g., ontology-based [106]) already provide rich semantic models to represent security know-how specific to ICSs, they do not support a seamless integration into PSE. In other words, security and domain experts have to model the target of inspection (e.g., the production system to be engineered) from scratch, requiring significant manual effort. A first step toward the integration of security modeling into PSE has been taken just a few years ago, as Glawe et al. [42, 41] propose the use of the Semantic Web Rule Language (SWRL) to logically connect engineering and security know-how, existing in AutomationML (AML) artifacts and a knowledge base built with the Web Ontology Language (OWL), respectively. This approach allows to reuse engineering artifacts for conducting security analyses. While their approach provides the

Ref.	Year	Methodology	Probabilistic Data Source(s)	Evaluation
[80, 81]	2006	Based on *compromise graphs*, i.e., directed graphs representing attack steps (nodes) and estimations of the time required for an attacker with certain capabilities to reach these steps (edges).	Time-to-compromise is modeled as a random process, considering three cases of the attacker's state (e.g., exploit available) and using an expert-based estimation of probability distributions.	Case study with a SCADA system consisting of eight devices. Risk reduction estimates for different attacks are provided.
[65]	2012	Utilizes the BDMP formalism, which employs attack trees and Markov processes. *Triggers* in models link attack steps and enable the representation of the dynamic properties of attacks (e.g., sequences, conditions).	BDMP leaves are modeled as the time needed for their realization (exponential distribution with a certain parameter) or as the probability of them occurring. Leaf values were estimated by the authors.	BDMP models of the Stuxnet attack, including quantification results (e.g., function relating attack success probability to time), are given.
[9, 12, 10]	2014, 2015, 2016	Scenario descriptions concerning the system, vulnerabilities, threat agents, and elementary attacks are obtained. Attacks are simulated by using the Monte Carlo method, generating random samples for computing statistics indicative of cyber risk.	CVSS scores of vulnerabilities are used to estimate the success probabilities of elementary attacks. Monte Carlo experiments on agent behavior yield the success probabilities of complex attacks.	Different ICSs are considered for applying the proposed methods, i.e., automating risk assessment [9], CyVar [12], and security stress [10].
[64]	2015	Generates attack and failure scenarios based on a knowledge base including ICS-specific information (e.g., architecture, attack steps, failure modes). Monte Carlo simulations are used for quantification purposes.	The attack frequency rates were estimated by the authors. Improving the quantitative dataset was left for future work.	Exemplary ICS, with assumptions concerning its security weaknesses, was used. Three of the most probable attack scenarios are provided.
[47, 101]	2015	Based on a template for a PRM that includes details about an ICS-specific object model. Bayesian networks, representing attack paths, can be generated to calculate the success probability of attacks.	Literature was used for obtaining the probabilities of certain attack steps (e.g., password cracking). In most cases, the authors had to resort to estimations from domain experts.	Verification (domain-dependent & -independent) and validation (by means of interviews/surveys with experts and a Turing test) was performed.
[49]	2017	Uses Bayesian networks with Leaky Noisy-OR (LNOR) gate (to account for unknown attacks) and parameter learning, viz. batch learning (offline, historical data) and incremental learning (online, real-time security events).	Authors propose the expectation–maximization (EM) algorithm to fill missing values in attack sample dataset used for batch learning. Parameters are also learned incrementally from observations.	Case study with a sample ICS for a chemical process. Three experiments were conducted to evaluate offline, online learning, and the capability to assess the risk of unknown attacks.
[20]	2018	Decision networks, which extend Bayesian networks, are used to model attack–defense scenarios, including a consideration of the costs of countermeasures.	Data were collected from testbed simulations performed as part of a research project. Authors suggest that using a risk rating scale could yield similar probabilities.	Case study with an exemplary ICS. Quant. analysis (success probability, importance measures, risk and impact metrics, return on investment) illustrates the method.
[87]	2018	Similar to [49], Bayesian networks and parameter learning are used. Bayesian networks are built from a knowledge base comprising information about vulnerabilities, device functions, and possible accidents.	Parameters of Bayesian networks are updated via incremental learning with data collected from the ICS in real-time. EM algorithm is used to deal with incomplete data.	Case study with a simulated ICS for the Tennessee Eastman process. The accuracy and dynamics of the method have been evaluated.
[22]	2018	Focuses on the risk analysis during security incidents. Consists of a risk analysis model for incidents, an elicitation technique for the incident likelihood, and a categorization model for ramifications of incidents.	Based on the qualitative interpretation of likelihood (i.e., probability ranges) and takes the oddness of events into account.	Method is demonstrated step-by-step with an illustrative example, i.e., a well drilling system of an oil & gas ICS that is infected with a wiper malware.

Table 1: Overview of existing quantitative security risk assessment methods that have been applied and evaluated in the ICS domain.

means to identify risks that have its roots in the plant design (e.g., PLC has an unprotected USB socket), an augmentation of quantitative attributes that could be fed into probabilistic models is lacking. As a consequence, quantitative methods may be of no avail, given that information required for performing PRA cannot be directly retrieved from security models, even though relevant data may implicitly exist in engineering artifacts to some extent (e.g., cost of components, sources of PD, digital assets).

A Poor Understanding of Potential Consequences The estimation of physical and economic effects caused by potential attacks against ICSs is essential for performing quantitative security risk assessments. Due to the fact that consequences of cyber attacks can be diverse and affect both tangible and intangible assets, estimating potential consequences represents a challenging endeavor [13]. However, it has been argued that assessing the impact of cyber incidents affecting the OT infrastructure tends be easier than those occurring in the IT, since the disruption of plant operation, caused by (accidental) failures, is generally well understood [119]. Yet, identifying and, in further consequence, quantitatively assessing potential consequences of cyber attacks against ICSs is a continuing concern, as there seems to be a general lack of research in this area. As already mentioned in Section 3.2, only a few scholars ([51, 50, 84]) have studied quantitative methods for assessing the impact of cyber-physical attacks thus far. Motivated by the need to improve the understanding of direct and indirect consequences, novel methods that source potential economic losses and physical impacts from engineering artifacts, including plant models, are required. Furthermore, it is worth noting that this research issue is also associated with the lack of integration of security modeling languages in PSE, since (i) they must support the representation of information indicative of incident severity, and (ii) they should fit naturally into PSE, allowing to easily draw on engineering data.

The Need for Automated Modeling of Sophisticated Cyber-Physical Attacks Another research opportunity in the context of risk identification is the automation of threat modeling activities. Enumerating possible threats can be a challenging endeavor, especially if the target of inspection is characterized by high complexity, as is the case with ICSs. Thus, threat modeling ought to be automated to a great extent, allowing security professionals to concentrate on subsequent (sub)processes of risk management. Considering the increasing amount of works that have been published on automated threat modeling and analysis in the past few years, it seems that this research area has been gaining traction recently. However, as suggested in a survey paper on model-driven security risk assessments published by Rocchetto et al. [95], previous work on automated threat modeling has not dealt with identifying cyber-physical attack chains. As Rocchetto et al. [95] correctly point out, an interconnection between vulnerabilities may exist, meaning that the exploitation of one weakness could lower the cost for an attacker to exploit several others. The past has shown that cyber attacks against ICSs often qualify as Advanced Persistent Threats (APTs), comprising multiple attack vectors and stages, involving numerous target hosts that attackers may compromise in order to pivot to the ICS's control level (cf., for instance, Stuxnet [69, 33]). These attacks targeting ICSs can also be considered as high-impact, low-frequency (HILF) events [21], in extreme cases often referred to as "black swans". Due to the criticality of such events, methods for automated threat modeling have to be equipped with new capabilities that support the identification of relationships between potential security weaknesses and possibly also between OT components. We consider the work by Puys et al. [91] as an initial step in this direction, since they propose an approach that automatically identifies possible attack scenarios considering that an attacker already gained a foothold in the ICS.

The Lack of Dynamic Risk Analysis Methods for ICSs Due to the fact that the threat landscape, as well as the ICSs themselves, change throughout their lifecycle, cyber risks cannot be considered as static.

As indicated in this literature review and reported in the survey paper [18], security researchers started to show interest in dynamic risk analysis methods, which alleviate this problem. Since dynamic risk analysis methods appear to be more prevalent in the safety and reliability domain, already established concepts that originate from safety engineering may also be adaptable to fit the needs of performing security risk analyses (e.g., dynamic fault trees, BDMP) [63]. Thus far, only a few researchers (e.g., Kriaa et al. [65]) have investigated dynamic risk analysis methods in the context of ICSs. As a result, we argue that adequate dynamic security risk analysis methods, which are tailored to the characteristics of ICSs and take the cyber-physical cross-domain properties into account, are in need of further investigation. This is in line with the findings of Cherdantseva et al. [18], who indicated that the insufficient level of detail in analyzing risks pertaining to ICSs and the missing holistic perspective poses a research challenge worth addressing. Moreover, we identified a notable lack of approaches that incorporate real-time data gained from security monitoring systems or threat intelligence services, which, in further consequence, could also impede risk response. While some encouraging initial results on leveraging data obtained from technical components for quantitative, dynamic security risk assessments have already been reported (e.g., in [5]), considerably more work needs to be done to implement an ICS-specific real-time data pipeline and the underlying probabilistic models.

Dealing with the Paucity of Historical Data In [21, 18] the authors determine the need for reliable sources of historical data on cyber attacks against ICSs, as the absence of data represents a key research challenge for the application of PRA methods. Both survey papers [21, 18] suggest that this issue may be overcome by utilizing testbeds (e.g., as attempted in [24]) or simulation platforms to launch controlled attacks against replicas of the real ICSs; thereby, generating valuable data that can be used for PRA methods. We support the idea of employing simulation platforms for this purpose and confirm that this problem still remains unresolved. In particular, there are two challenges that deserve attention: First, methods to efficiently realize simulation platforms for risk assessments, which are neither bound to specific scenarios nor require extensive manual adaptation to fit the industrial setup at hand, are needed. Second, it is unknown at present how synthetic data, which is both representative and reliable, can be obtained from simulated attack scenarios. Moreover, from the literature reviewed and the findings reported in [21, 18], it becomes evident that existing cyber risk quantification approaches predominantly resort to subjective information (e.g., expert opinion). In this context, future work is required to investigate the representation of expert judgment in engineering knowledge bases as well as the efficient extraction thereof. Another way of dealing with the lack of historical data is to source relevant information directly from the ICSs, assuming that it is already in operation. Building upon existing research conducted by Allodi and Massacci [5], data could be leveraged from the IT/OT infrastructure to feed (dynamic) cyber risk models. More research in this area is definitely required to determine the limitations of this approach.

4.2 Future Research Directions

Based on the described shortcomings of existing works and the open research issues, we provide suggestions that may serve as a starting point for future research. In the following, we describe three research directions that we consider particularly promising.

Risk Identification Based on Engineering Data Researchers have not yet examined how threats and potential consequences of cyber attacks against ICSs can be automatically identified based on engineering information in order to perform a quantitative security risk analysis. Unlike previous works that leverage AML artifacts (e.g., [41]) to spot potential security weaknesses, a special emphasis may be placed on the automated extraction of relevant information from similar sources of engineering knowledge for the purpose of feeding probabilistic models, thereby setting the stage for quantitative risk anal-

yses. In particular, researchers may aim at designing these methods in a way that they can be embedded into PSE; thus, allowing to reuse a considerable amount of know-how, which systems integrators maintain about the plant to be built, for risk identification. Based on this, the developed methods should have automated threat modeling and analysis capabilities, including the identification of potential consequences and a consideration of the involved costs both from the attacker's and defender's perspective (e.g., time-to-compromise, cost models for PD/MD and BI). Moreover, these methods need to support the identification of complex cyber-physical attack scenarios, as insights into possible paths that attackers might take as well as the interconnections of potential vulnerabilities are essential.

Dynamic Risk Analysis Methods for ICSs Further research is needed to develop security risk analysis methods that provide a sufficient level of detail by gearing them to the specificities of ICSs while ensuring that they are still able to cope with the complexity of these systems. Particular attention should be paid to their dynamic characteristic, which has to be reflected both in their underlying stochastic model and the way how probabilities are updated. The developed cyber risk model should provide the means to create holistic risk profiles spanning over multiple phases of the ICS's lifecycle and account for the dynamic aspects of information security, rather than providing a merely static perspective. Furthermore, the knowledge required to update probabilities in real-time may be sourced from security monitoring components (e.g., intrusion detection systems) and relevant threat intelligence sources (e.g., feeds, honeypots).

Digital Twins to Support Quantitative Security Risk Assessments As already mentioned, the problem of efficiently creating virtual ICS environments in order to simulate attack scenarios and thereby generate valuable data that can be used for security risk assessments remains unresolved thus far. Addressing this issue requires innovative methods concerning the development of simulation platforms that lend themselves well for assessing security risks. In this context, it may be worthwhile to make use of the concept of digital twins. A digital twin virtually replicates its physical counterpart, such as an ICS, and can be employed for security-improving use cases [28]. It has been shown in [27, 25, 26] that engineering-related data (e.g., the specification of ICSs) allows to create such digital twins in an efficient manner and exploit them for the purpose of intrusion detection. As we also indicate in [28], it would be interesting to further explore how attacks against digital twins can be executed. The results of these virtual attack simulations could then be factored into cyber risk models. Although there are scientific works on the subject of ICS attack simulation for the purpose of assessing the impact (e.g., [17, 14, 67]), no research has been found that deals with simulation-based approaches for attack likelihood estimation. Thus, it would be interesting to investigate whether digital twins, which may even run in parallel to their physical counterparts during the operation of the ICS, can remedy the issue of probabilistic data scarcity.

5 Conclusion

In this article, we have briefly reviewed the state of the art in the area of quantitative security risk assessment, specifically in the context of complex industrial systems, and including a consideration of cyber insurance aspects. Furthermore, we have identified research gaps and have made suggestions for future research. In essence, this article informs researchers and practitioners about the fundamental issues and opportunities pertaining to the identification, quantitative analysis, and evaluation of ICS cyber risks, aiming to stimulate joint efforts in this interdisciplinary field. Figure 1 summarizes the identified research issues, research directions, and relevant scientific works that readers can use as a foundation for their future research.

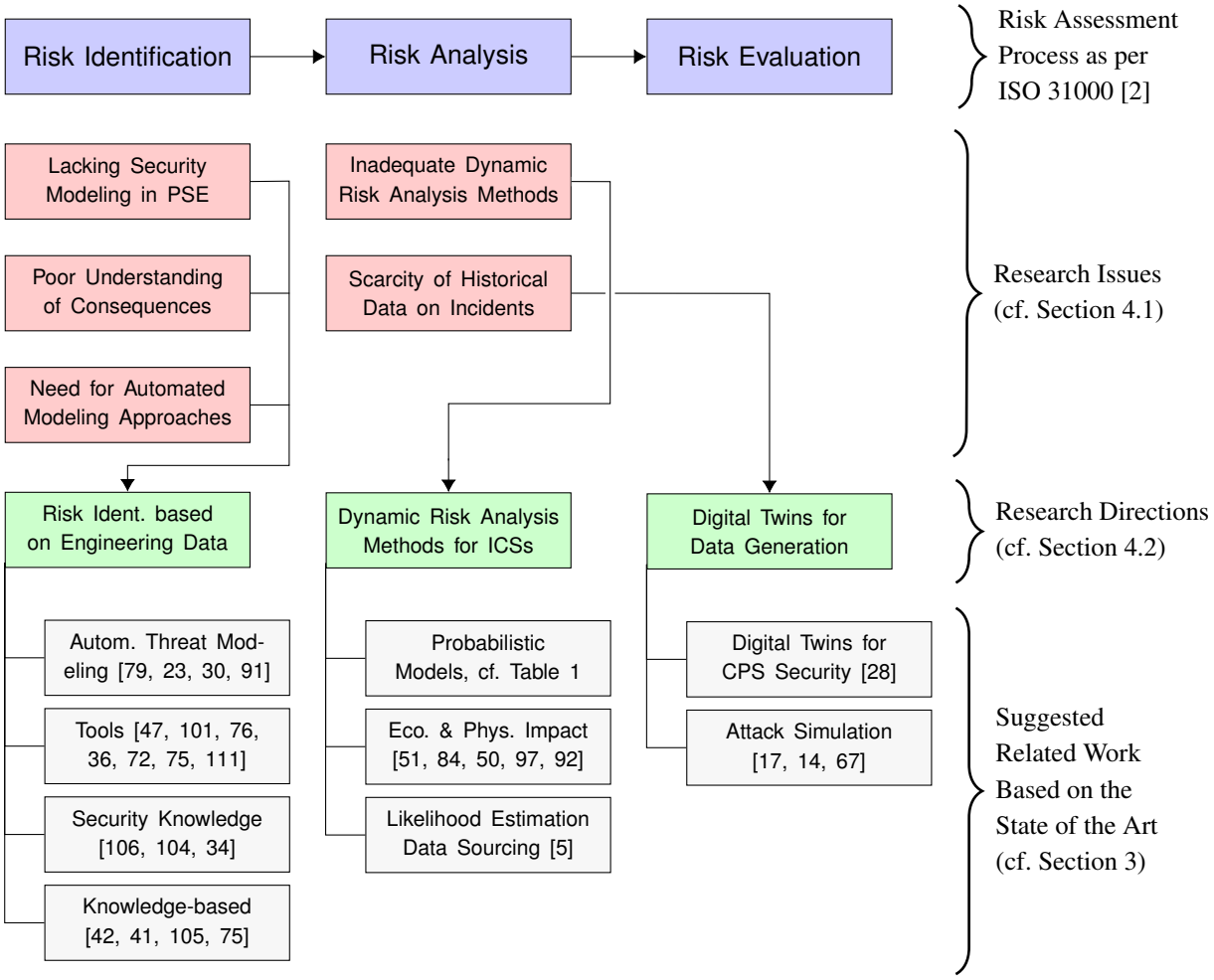


Figure 1: Overview of identified research issues and opportunities in the area of quantitative security risk assessment for ICSs, including a broad classification of literature that may be used as a starting point for future research.

Qualitative risk assessment methods still have a strong presence in ICS security standards and guidelines (e.g., IEC 62443, VDI/VDE 2182), yet, questions have been raised about their usefulness. We advocate quantitative methods and argue that the cost-effective risk reduction and cyber insurance underwriting make their application necessary. However, several problems arise when seeking to apply them for analyzing ICS security risks, creating barriers that hinder their adoption. In particular, the continuously evolving and complex threat environment in which ICSs function, the impediments concerning the sharing of security-relevant information among parties, the paucity of historical data on security incidents, and accumulating cyber risks are issues that deserve attention. Thus far, researchers have already taken the first steps in addressing these issues, but numerous challenges remain to be tackled.

The findings from this work lead to the conclusion that quantitatively assessing ICS security risks is still in its infancy. Research in this area is driven by the anticipated benefit of reducing uncertainty concerning cyber risks for decision support. Although it appears that quantitative methods are slowly gaining traction, little effort has been made so far to test the validity of proposed approaches and examine their limitations in detail. Thus, we expect that they need to gain more scientific credibility until companies in the industrial automation sector will make the shift toward a more quantitative security risk

assessment process.

Acknowledgments

The COMET center SBA Research (SBA-K1) is funded within the framework of COMET — Competence Centers for Excellent Technologies by BMVIT, BMDW, and the federal state of Vienna, managed by the FFG. This research was further funded by the FFG under the industrial PhD program (grant no. 874644). Moreover, the financial support by the Christian Doppler Research Association, the Austrian Federal Ministry for Digital and Economic Affairs and the National Foundation for Research, Technology and Development is gratefully acknowledged.

References

[1] Industrial communication networks – network and system security – part 1-1: Terminology, concepts and models. 2009. IEC 62443-1-1.

[2] Risk management – Principles and guidelines. `https://www.iso.org/standard/43170.html`, [Online; Accessed on August 2, 2019], November 2009. ISO 31000:2009.

[3] Industrial communication networks – network and system security – part 3-3: System security requirements and security levels. 2013. IEC 62443-3-3.

[4] Enterprise-control system integration – part 3: Activity models of manufacturing operations management. `https://www.iso.org/standard/67480.html`, [Online; Accessed on August 2, 2019], 2016. IEC 62264-3.

[5] L. Allodi and F. Massacci. Security events and vulnerability data for cybersecurity risk estimation. *Risk Analysis*, 37(8):1606–1627, August 2017.

[6] L. Apvrille and Y. Roudier. SysML-sec: A SysML environment for the design and development of secure embedded systems. In *Proc. of the 2013 Asia-Pacific Council on Systems Engineering (APCOSEC'13), Yokohama, Japan*. EURECOM, September 2013.

[7] L. Apvrille and Y. Roudier. Designing safe and secure embedded and cyber-physical systems with SysML-Sec. In *Proc. of the 3rd International Conference on Model-Driven Engineering and Software Development (MODELSWARD'15), Angers, France*, pages 293–308. Springer International Publishing, February 2015.

[8] L. Ayala. *Cyber-Physical Attack Recovery Procedures: A Step-by-Step Preparation and Response Guide*. Apress, June 2016.

[9] F. Baiardi, F. Corò, F. Tonelli, and D. Sgandurra. Automating the assessment of ICT risk. *Journal of Information Security and Applications*, 19(3):182–193, July 2014.

[10] F. Baiardi, F. Corò, F. Tonelli, A. Bertolini, R. Bertolotti, and L. Guidi. Security stress: Evaluating ICT robustness through a monte carlo method. In *Proc. of the 9th International Conference on Critical Information Infrastructures Security (CRITIS'14), Limassol, Cyprus*, volume 8985 of *Lecture Notes in Computer Science*, pages 222–227. Springer, Cham, October 2016.

[11] F. Baiardi and D. Sgandurra. Assessing ICT risk through a monte carlo method. *Environment Systems and Decisions*, 33(4):486–499, December 2013.

[12] F. Baiardi, F. Tonelli, and A. Bertolini. CyVar: Extending var-at-risk to ICT. In *Risk Assessment and Risk-Driven Testing*, volume 9488 of *Lecture Notes in Computer Science*, pages 49–62. Springer, Cham, 2015.

[13] R. Bojanc and B. Jerman-Blažič. An economic modelling approach to information security risk management. *International Journal of Information Management*, 28(5):413 – 422, October 2008.

[14] A. Bracho, C. Saygin, H. Wan, Y. Lee, and A. Zarreh. A simulation-based platform for assessing the impact of cyber-threats on smart manufacturing systems. *Procedia Manufacturing*, 26:1116 – 1127, 2018.

[15] E. J. Byres, M. Franz, and D. Miller. The use of attack trees in assessing vulnerabilities in SCADA systems. In *Proc. of the 2004 IEEE International Infrastructure Survivability Workshop (IISW'04), Lisbon, Portugal*, pages 1–9. IEEE, December 2004.

[16] M. Caselli, E. Zambon, and F. Kargl. Sequence-aware intrusion detection in industrial control systems. In *Proc. of the 1st ACM Workshop on Cyber-Physical System Security (CPSS'15), Singapore*, pages 13–24. ACM, April 2015.

[17] R. Chabukswar, B. Sinopoli, G. Karsai, A. Giani, H. Neema, and A. Davis. Simulation of network attacks on SCADA systems. In *Proc. of the 1st Workshop on Secure Control Systems, Cyber Physical Systems Week 2010*. TRUST, April 2010.

[18] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart. A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, 56:1 – 27, February 2016.

[19] A. Coburn, E. Leverett, and G. Woo. *Solving Cyber Risk: Protecting Your Company and Society*. John Wiley & Sons, December 2018.

[20] D. Codetta-Raiteri and L. Portinale. Decision networks for security risk assessment of critical infrastructures. *ACM Transaction on Internet Technology*, 18(3):29:1–29:22, May 2017.

[21] A. Cook, R. Smith, L. Maglaras, and H. Janicke. Measuring the risk of cyber attack in industrial control systems. In *Proc. of the 4th International Symposium for ICS & SCADA Cyber Security Research 2016 (ICS-CSR'16), Belfast, UK*, pages 1–11. BCS Learning & Development Ltd., August 2016.

[22] A. Couce-Vieira, S. H. Houmb, and D. Ríos-Insua. Csira: A method for analysing the risk of cybersecurity incidents. In *Proc. of the 4th International Workshop on Graphical Models for Security (GraMSec'17), Santa Barbara, California, USA*, volume 10744 of *Lecture Notes in Computer Science*, pages 57–74. Springer, Cham, August 2018.

[23] W. Depamelaere, L. Lemaire, J. Vossaert, and V. Naessens. CPS security assessment using automatically generated attack trees. In *Proc. of the 5th International Symposium for ICS & SCADA Cyber Security Research 2018 (ICS-CSR'18), Hamburg, Germany*, pages 1–10. British Computer Society (BCS), 2018.

[24] G. Dondossola, F. Garrone, and J. Szanto. Supporting cyber risk assessment of power control systems with experimental data. In *Proc. of the 2009 IEEE/PES Power Systems Conference and Exposition (PSCE'09), Seattle, Washington, USA*, pages 1–3. IEEE, March 2009.

[25] M. Eckhart and A. Ekelhart. Securing cyber-physical systems through digital twins. *ERCIM News*, 2018(115), October 2018.

[26] M. Eckhart and A. Ekelhart. A specification-based state replication approach for digital twins. In *Proc. of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy (CPS-SPC'18), Toronto, Ontario, Canada*, pages 36–47. ACM, October 2018.

[27] M. Eckhart and A. Ekelhart. Towards security-aware virtual environments for digital twins. In *Proc. of the 4th ACM Workshop on Cyber-Physical System Security (CPSS'18), Incheon, Republic of Korea*, pages 61–72. ACM, June 2018.

[28] M. Eckhart and A. Ekelhart. *Digital Twins for Cyber-Physical Systems Security: State of the Art and Outlook*. Springer, 2019.

[29] M. Eckhart, A. Ekelhart, A. Lüder, S. Biffl, and E. Weippl. Security development lifecycle for cyber-physical production systems. In *Proc. of the 45th Annual Conference of the IEEE Industrial Electronics Society (IECON'19), Lisbon, Portugal*. IEEE, October 2019.

[30] M. Eckhart, K. Meixner, D. Winkler, and A. Ekelhart. Securing the testing process for industrial automation software. *Computers & Security*, 85:156–180, August 2019.

[31] A. Ekelhart, S. Fenz, M. Klemen, and E. Weippl. Security ontologies: Improving quantitative risk analysis. In *Proc. of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07), Waikoloa, Hawaii, USA*, pages 156a–156a. IEEE, January 2007.

[32] A. Ekelhart, S. Fenz, M. D. Klemen, and E. R. Weippl. Security ontology: Simulating threats to corporate assets. In *Proc. of the 2nd International Conference on Information Systems Security (ICISS'06), Kolkata, India*, volume 4332 of *Lecture Notes in Computer Science*, pages 249–259. Springer Berlin Heidelberg, December 2006.

[33] N. Falliere, L. O. Murchu, and E. Chien. W32. stuxnet dossier. Technical Report 6, Symantec Corporation,

February 2011.

[34] S. Fenz and A. Ekelhart. Formalizing information security knowledge. In *Proc. of the 4th International Symposium on Information, Computer, and Communications Security (ASIACCS'09), Sydney, Australia*, pages 183–194. ACM, March 2009.

[35] E. B. Fernandez. Threat modeling in cyber-physical systems. In *Proc. of the 2016 IEEE 14th International Conference on Dependable, Autonomic and Secure Computing, 14th International Conference on Pervasive Intelligence and Computing, 2nd International Conference on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech'16), Auckland, New Zealand*, pages 448–453. IEEE, August 2016.

[36] M. D. Ford, K. Keefe, E. LeMay, W. H. Sanders, and C. Muehrcke. Implementing the ADVISE security modeling formalism in möbius. In *Proc. of the 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'13), Budapest, Hungary*, pages 1–8. IEEE, June 2013.

[37] I. N. Fovino, A. Carcano, T. D. L. Murel, A. Trombetta, and M. Masera. Modbus/DNP3 state-based intrusion detection system. In *Proc. of the 24th IEEE International Conference on Advanced Information Networking and Applications (AINA'10), Perth, Western Australia, Australia*, pages 729–736. IEEE, April 2010.

[38] J. Freund and J. Jones. *Measuring and Managing Information Risk: A FAIR Approach*. Butterworth-Heinemann, September 2014.

[39] D. Geer, K. S. Hoo, and A. Jaquith. Information security: why the future belongs to the quants. *IEEE Security Privacy*, 99(4):24–32, July 2003.

[40] L. Getoor, N. Friedman, D. Koller, A. Pfeffer, and B. Taskar. *Probabilistic Relational Models*. MIT Press, 2007.

[41] M. Glawe and A. Fay. Wissensbasiertes Engineering automatisierter Anlagen unter Verwendung von AutomationML und OWL. *at-Automatisierungstechnik*, 64(3):186–198, March 2016.

[42] M. Glawe, C. Tebbe, A. Fay, and K.-H. Niemann. Knowledge-based engineering of automation systems using ontologies and engineering data. In *Proc. of the 2015 International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management (IC3K'15), Lisbon, Portugal*, pages 291–300. SCITEPRESS - Science and Technology Publications, Lda, November 2015.

[43] J. Guan, J. H. Graham, and J. L. Hieb. A digraph model for risk identification and mangement in SCADA systems. In *Proc. of the 2011 IEEE International Conference on Intelligence and Security Informatics (ISI'11), Beijing, China*, pages 150–155. IEEE, July 2011.

[44] A. Hahn. *Operational Technology and Information Technology in Industrial Control Systems*, pages 51–68. Springer, Cham, August 2016.

[45] A. Herzog, N. Shahmehri, and C. Duma. An Ontology of Information Security. *International Journal of Information Security and Privacy*, 1(4):1–23, October 2007.

[46] H. Holm, K. Shahzad, M. Buschle, and M. Ekstedt. P^2CySeMoL: Predictive, probabilistic cyber security modeling language. *IEEE Transactions on Dependable and Secure Computing*, 12(6):626–639, November 2015.

[47] H. Holm, T. Sommestad, M. Ekstedt, and L. Nordström. CySeMoL: A tool for cyber security analysis of enterprises. In *Proc. of the 22nd International Conference and Exhibition on Electricity Distribution (CIRED'13), Stockholm, Sweden*, pages 1–4. IET, June 2013.

[48] R. A. Howard. Microrisks for medical decision analysis. *International Journal of Technology Assessment in Health Care*, 5(3):357–370, 1989.

[49] K. Huang, C. Zhou, Y. Tian, W. Tu, and Y. Peng. Application of bayesian network to data-driven cybersecurity risk assessment in SCADA networks. In *Proc. of the 27th International Telecommunication Networks and Applications Conference (ITNAC'17), Melbourne, Victoria, Australia*, pages 1–6. IEEE, November 2017.

[50] K. Huang, C. Zhou, Y. Tian, S. Yang, and Y. Qin. Assessing the physical impact of cyberattacks on industrial cyber-physical systems. *IEEE Transactions on Industrial Electronics*, 65(10):8153–8162, October 2018.

[51] Y.-L. Huang, A. A. Cárdenas, S. Amin, Z.-S. Lin, H.-Y. Tsai, and S. Sastry. Understanding the physical and economic consequences of attacks on control systems. *International Journal of Critical Infrastructure Protection*, 2(3):73–83, October 2009.

[52] D. W. Hubbard and R. Seiersen. *How to Measure Anything in Cybersecurity Risk*. John Wiley & Sons Inc, 2016.

[53] J. C. Hull. *Options, Futures and Other Derivatives*. Pearson Education, January 2018.

[54] V. Jacobs, J. Bulters, and M. van Wieren. Modeling the impact of cyber risk for major dutch organizations. In *Proc. of the 15th European Conference on Cyber Warfare and Security (ECCWS'16), Munich, Germany*. ACPIL, July 2016.

[55] P. Johnson, A. Vernotte, D. Gorton, M. Ekstedt, and R. Lagerström. Quantitative information security risk estimation using probabilistic attack graphs. In *Proc. of the 4th International Workshop on Risk Assessment and Risk-Driven Testing (RISK'16), Graz, Austria*, volume 10224 of *Lecture Notes in Computer Science*, pages 37–52. Springer, Cham, October 2016.

[56] P. Jorion. *Value at Risk: The New Benchmark for Managing Financial Risk*. McGraw-Hill Professional, 3rd edition, November 2006.

[57] H. Kagermann, J. Helbig, A. Hellinger, and W. Wahlster. Recommendations for implementing the strategic initiative INDUSTRIE 4.0 – securing the future of german manufacturing industry. Technical report, National Academy of Science and Engineering, April 2013.

[58] S. Kaplan and B. J. Garrick. On the quantitative definition of risk. *Risk Analysis*, 1(1):11–27, 1981.

[59] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer. STRIDE-based threat modeling for cyber-physical systems. In *Proc. of the 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe'17), Torino, Italy*, pages 1–6. IEEE, September 2017.

[60] P. Kieseberg and E. Weippl. Security challenges in cyber-physical production systems. In *Proc. of the 10th International Conference on Software Quality (SWQD'18), Vienna, Austria*, pages 3–16. Springer, Cham, January 2018.

[61] P. Kocher, J. Horn, A. Fogh, , D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, M. Schwarz, and Y. Yarom. Spectre attacks: Exploiting speculative execution. In *Proc. of the 40th IEEE Symposium on Security and Privacy (S&P'19), San Francisco, California, USA*. IEEE, May 2019.

[62] B. Kordy, S. Mauw, and P. Schweitzer. Quantitative questions on attack–defense trees. In *Proc. of the 15th International Conference on Information Security and Cryptology (ICISC'12), Seoul, Korea*, volume 7839 of *Lecture Notes in Computer Science*, pages 49–64. Springer Berlin Heidelberg, November 2012.

[63] B. Kordy, L. Piètre-Cambacédès, and P. Schweitzer. DAG-based attack and defense modeling: Don't miss the forest for the attack trees. *Computer Science Review*, 13-14:1 – 38, November 2014.

[64] S. Kriaa, M. Bouissou, and Y. Laarouchi. A model based approach for SCADA safety and security joint modelling: S-cube. In *Proc. of the 10th IET System Safety and Cyber-Security Conference (CP'15), Bristol, UK*, pages 1–6. IET, January 2015.

[65] S. Kriaa, M. Bouissou, and L. Piètre-Cambacédès. Modeling the stuxnet attack with BDMP: Towards more formal risk assessments. In *Proc. of the 7th International Conference on Risks and Security of Internet and Systems (CRiSIS'12), Cork, Ireland*, pages 1–8. IEEE, October 2012.

[66] S. Kriaa, L. Pietre-Cambacedes, M. Bouissou, and Y. Halgand. A survey of approaches combining safety and security for industrial control systems. *Reliability Engineering & System Safety*, 139:156–178, July 2015.

[67] M. Krotofil, A. Isakov, A. Winnicki, D. Gollmann, J. Larsen, and P. Gurikov. Rocking the pocket book: Hacking chemical plants for competition and extortion. Technical report, Black Hat, August 2015.

[68] A. Krutov. Clear and present danger: the pressing need to address cyber risk requires its better understanding and adequate quantification. *Financier Worldwide Magazine*, August 2014.

[69] R. Langner. To kill a centrifuge: A technical analysis of what stuxnet's creators tried to achieve. `https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf`, [Online; Accessed on August 2, 2019], 2013.

[70] N. T. Le and D. B. Hoang. Security threat probability computation using markov chain and common vulnerability scoring system. In *Proc. of the 28th International Telecommunication Networks and Applications Conference (ITNAC'18), Sydney, New South Wales, Australia*, pages 1–6. IEEE, November 2018.

[71] A. Ledeczi, M. Maroti, A. Bakay, G. Karsai, J. Garrett, C. Thomason, G. Nordstrom, J. Sprinkle, and P. Volgyesi. The generic modeling environment. In *Proc. of the 2001 IEEE International Workshop on*

Intelligent Signal Processing (WISP'01), Budapest, Hungary. IEEE, May 2001.

[72] L. Lemaire, J. Lapon, B. De Decker, and V. Naessens. A SysML extension for security analysis of industrial control systems. In *Proc. of the 2nd International Symposium on ICS & SCADA Cyber Security Research 2014 (ICS-CSR'14), St Pölten, Austria*, pages 1–9. BCS, September 2014.

[73] L. Lemaire, J. Vossaert, B. De Decker, and V. Naessens. An assessment of security analysis tools for cyber-physical systems. In *Proc. of the 4th International Workshop on Risk Assessment and Risk-Driven Testing (ICTSS'16), Graz, Austria*, volume 10224 of *Lecture Notes in Computer Science*, pages 66–81. Springer, Cham, October 2016.

[74] L. Lemaire, J. Vossaert, B. De Decker, and V. Naessens. Security evaluation of cyber-physical systems using automatically generated attack trees. In *Proc. of the 12th International Conference on Critical Information Infrastructures Security (CRITIS'17), Lucca, Italy*, volume 10707 of *Lecture Notes in Computer Science*, pages 225–228. Springer, Cham, October 2017.

[75] L. Lemaire, J. Vossaert, J. Jansen, and V. Naessens. Extracting vulnerabilities in industrial control systems using a knowledge-based system. In *Proc. of the 3rd International Symposium for ICS & SCADA Cyber Security Research 2015 (ICS-CSR'15), Ingolstadt, Germany*, pages 1–10. BCS Learning & Development Ltd., September 2015.

[76] E. LeMay, M. D. Ford, K. Keefe, W. H. Sanders, and C. Muehrcke. Model-based security metrics using adversary view security evaluation (ADVISE). In *Proc. of the 8th International Conference on Quantitative Evaluation of SysTems (QEST'11), Aachen, Germany*, pages 191–200. IEEE, September 2011.

[77] M. Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas, A. Fogh, J. Horn, S. Mangard, P. Kocher, D. Genkin, Y. Yarom, and M. Hamburg. Meltdown: Reading kernel memory from user space. In *Proc. of the 27th USENIX Conference on Security Symposium (SEC'18), Baltimore, Maryland, USA*, pages 973–990. USENIX, August 2018.

[78] E. Lisova, I. Sljivo, and A. Causevic. Safety and security co-analyses: A systematic literature review. *IEEE Systems Journal*, 13(3):1–12, December 2018.

[79] G. Martins, S. Bhatia, X. Koutsoukos, K. Stouffer, C. Tang, and R. Candell. Towards a systematic threat modeling approach for cyber-physical systems. In *Proc. of the 2015 Resilience Week (RWEEK'15), Philadelphia, Pennsylvania, USA*, pages 1–6. IEEE, August 2015.

[80] M. A. McQueen, W. F. Boyer, M. A. Flynn, and G. A. Beitel. Quantitative cyber risk reduction estimation methodology for a small SCADA control system. In *Proc. of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06), Kauia, Hawaii, USA*, pages 226–226. IEEE, January 2006.

[81] M. A. McQueen, W. F. Boyer, M. A. Flynn, and G. A. Beitel. Time-to-compromise model for cyber risk reduction estimation. 23:49–64, 2006.

[82] B. Obama. Executive Order 13691 — Promoting Private Sector Cybersecurity Information Sharing. `https://www.dhs.gov/sites/default/files/publications/2015-03714.pdf`, [Online; Accessed on August 2, 2019], February 2015.

[83] A. Oltramari, L. Cranor, R. Walls, and P. McDaniel. Building an ontology of cyber security. *CEUR Workshop Proceedings*, 1304:54–61, 1 2014.

[84] H. Orojloo and M. A. Azgomi. A method for evaluating the consequence propagation of security attacks in cyber-physical systems. *Future Generation Computer Systems*, 67:57–71, February 2017.

[85] M. O'Rourke. The year in risk 2017. *Risk Management*, 64(11):20–25, December 2017.

[86] P. Pandey and E. A. Snekkenes. A performance assessment metric for information security financial instruments. In *Proc. of the 2015 International Conference on Information Society (i-Society'15), London, UK*, pages 138–145. IEEE, November 2015.

[87] Y. Peng, K. Huang, W. Tu, and C. Zhou. A model-data integrated cyber security risk assessment method for industrial control systems. In *Proc. of the 2018 IEEE 7th Data Driven Control and Learning Systems Conference (DDCLS'18), Enshi, China*, pages 344–349. IEEE, May 2018.

[88] L. Piètre-Cambacédès and M. Bouissou. Beyond attack trees: Dynamic security modeling with boolean logic driven markov processes (BDMP). In *Proc. of the 2010 European Dependable Computing Conference (EDCC'10), Valencia, Spain*, pages 199–208. IEEE, April 2010.

[89] N. Poolsappasit, R. Dewri, and I. Ray. Dynamic security risk management using bayesian attack graphs.

IEEE Transactions on Dependable and Secure Computing, 9(1):61–74, Jan 2012.

[90] Prudential Regulation Authority. Cyber insurance underwriting risk. Technical Report Supervisory Statement 4/17, Prudential Regulation Authority, July 2017.

[91] M. Puys, M.-L. Potet, and A. Khaled. Generation of applicative attacks scenarios against industrial systems. In *Proc. of the 10th International Symposium on Foundations and Practice of Security (FPS'17), Nancy, France*, volume 10723 of *Lecture Notes in Computer Science*, pages 127–143. Springer, Cham, October 2018.

[92] P. Radanliev, D. C. D. Roure, R. Nicolescu, M. Huth, R. M. Montalvo, S. Cannady, and P. Burnap. Future developments in cyber risk assessment for the internet of things. *Computers in Industry*, 102:14–22, November 2018.

[93] M. Raugas, J. Ulrich, R. Faux, S. Finkelstein, and C. Cabot. CyberV@R: A cyber security model for value at risk. Technical report, CyberPoint, January 2013.

[94] N. Robinson. Incentives and barriers of the cyber insurance market in europe. Technical report, European Network and Information Security Agency (ENISA), June 2012.

[95] M. Rocchetto, A. Ferrari, and V. Senni. Challenges and opportunities for model-based security risk assessment of cyber-physical systems. In *Resilience of Cyber-Physical Systems*, pages 25–47. Springer, Cham, January 2019.

[96] A. Roy, D. S. Kim, and K. S. Trivedi. Cyber security analysis using attack countermeasure trees. In *Proc. of the 6th Annual Workshop on Cyber Security and Information Intelligence Research (CSIIRW'10), Oak Ridge, Tennessee, USA*, pages 28:1–28:4. ACM, April 2010.

[97] K. Ruan. Introducing cybernomics: A unifying economic framework for measuring cyber risk. *Computers & Security*, 65:77–89, March 2017.

[98] R. Schlegel, S. Obermeier, and J. Schneider. Structured system threat modeling and mitigation analysis for industrial automation systems. In *Proc. of the 2015 IEEE 13th International Conference on Industrial Informatics (INDIN'15), Cambridge, UK*, pages 197–203. IEEE, July 2015.

[99] B. Schneier. Attack trees. *Dr. Dobb's Journal: Software Tools for the Professional Programmer*, 24(12):21–26, 1999.

[100] A. Shostack. *Threat Modeling: Designing for Security*. Wiley Publishing, 2014.

[101] T. Sommestad, M. Ekstedt, and H. Holm. The cyber security modeling language: A tool for assessing the vulnerability of enterprise system architectures. *IEEE Systems Journal*, 7(3):363–373, September 2013.

[102] M. G. Stewart and J. Mueller. Cost-benefit analysis of airport security: Are airports too safe? *Journal of Air Transport Management*, 35:19 – 28, March 2014.

[103] F. Swiderski and W. Snyder. *Threat Modeling*. Microsoft Press, 2004.

[104] C. Tebbe, M. Glawe, K.-H. Niemann, and A. Fay. Informationsbedarf für automatische IT-Sicherheitsanalysen automatisierungstechnischer Anlagen. *at-Automatisierungstechnik*, 65(1):87–97, January 2017.

[105] C. Tebbe, M. Glawe, A. Scholz, K. heinz Niemann, A. Fay, and J. Dittgen. Wissensbasierte Sicherheitsanalyse in der Automation. *atp magazin*, 57(04):56–66, March 2015.

[106] C. Tebbe, K.-H. Niemann, and A. Fay. Ontology and life cycle of knowledge for ICS security assessments. In *Proc. of the 4th International Symposium for ICS & SCADA Cyber Security Research 2016 (ICS-CSR'16), Belfast, UK*, pages 1–10. BCS Learning & Development Ltd., August 2016.

[107] A. Teixeira, K. C. Sou, H. Sandberg, and K. H. Johansson. Secure control systems: A quantitative risk management approach. *IEEE Control Systems Magazine*, 35(1):24–45, February 2015.

[108] C. Ten, C. Liu, and M. Govindarasu. Vulnerability assessment of cybersecurity for SCADA systems using attack trees. In *Proc. of the 2007 IEEE Power Engineering Society General Meeting (PES'07), Tampa, Florida, USA*, pages 1–8. IEEE, June 2007.

[109] VDI/VDE 2182-1. Sheet 1: IT-security for industrial automation - general model. `https://infostore.saiglobal.com/en-au/Standards/VDI-VDE-2182-1-2011-1113701_SAIG_VDI_VDI_2587342/`, [Online; Accessed on August 2, 2019], 2011.

[110] D. Vose. *Risk Analysis: A Quantitative Guide*. John Wiley & Sons, 3rd edition, April 2008.

[111] A. H. Vu, N. O. Tippenhauer, B. Chen, D. M. Nicol, and Z. Kalbarczyk. CyberSAGE: A tool for automatic security assessment of cyber-physical systems. In *Proc. of the 11th International Conference on Quantitative Evaluation of Systems, Florence, Italy*, volume 8657 of *Lecture Notes in Computer Science*, pages 384–387. Springer, Cham, September 2014.

[112] W. Wang, A. Cammi, F. D. Maio, S. Lorenzi, and E. Zio. A monte carlo-based exploration framework for identifying components vulnerable to cyber threats in nuclear power plants. *Reliability Engineering & System Safety*, 175:24–37, July 2018.

[113] E. Weippl and P. Kieseberg. Security in cyber-physical production systems: A roadmap to improving IT-security in the production system lifecycle. In *Proc. of the 2017 AEIT International Annual Conference (AEIT'17), Cagliari, Italy*, pages 1–6. IEEE, September 2017.

[114] World Economic Forum (WEF). Partnering for cyber resilience: Towards the quantification of cyber threats. Technical report, January 2015.

[115] F. Xie, T. Lu, X. Guo, J. Liu, Y. Peng, and Y. Gao. Security analysis on cyber-physical system using attack tree. In *Proc. of the 9th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'13), Beijing, China*, pages 429–432. IEEE, October 2013.

[116] P. Xie, J. H. Li, X. Ou, P. Liu, and R. Levy. Using bayesian networks for cyber security analysis. In *Proc. of the 2010 IEEE/IFIP International Conference on Dependable Systems Networks (DSN'10), Chicago, Illinois, USA*, pages 211–220. IEEE, June 2010.

[117] M. Yampolskiy, P. Horvath, X. D. Koutsoukos, Y. Xue, and J. Sztipanovits. Systematic analysis of cyber-attacks on CPS-evaluating applicability of DFD-based approach. In *Proc. of the 5th International Symposium on Resilient Control Systems (ISRCS'12), Salt Lake City, Utah, USA*, pages 55–62. IEEE, August 2012.

[118] M. Yampolskiy, P. Horvath, X. D. Koutsoukos, Y. Xue, and J. Sztipanovits. Taxonomy for description of cross-domain attacks on CPS. In *Proc. of the 2nd ACM International Conference on High Confidence Networked Systems (HiCoNS'13), Philadelphia, Pennsylvania, USA*, pages 135–142. ACM, April 2013.

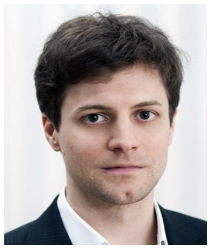
[119] D. Young, J. Lopez, M. Rice, B. Ramsey, and R. McTasney. A framework for incorporating insurance in critical infrastructure cyber risk strategies. *International Journal of Critical Infrastructure Protection*, 14:43–57, September 2016.

[120] J. Zalewski, S. Drager, W. McKeever, and A. J. Kornecki. Threat modeling for security assessment in cyberphysical systems. In *Proc. of the 8th Annual Cyber Security and Information Intelligence Research Workshop (CSIIRW'13), Oak Ridge, Tennessee, USA*, pages 10:1–10:4. ACM, January 2013.

Author Biography

Matthias Eckhart received a bachelor's degree in Internet Technology, a master's degree in IT & Mobile Security, and a master's degree in IT Law & Management from the University of Applied Sciences JOANNEUM. Since 2017, he has been working as a junior researcher at SBA Research in the field of cyber-physical systems security. In 2018, he joined the Christian Doppler Laboratory for Security and Quality Improvement in the Production System Lifecycle (CDL-SQI). His research interests focus on information security risk assessment for industrial control systems, with an emphasis on quantitative methods. He is currently a PhD candidate at TU Wien.

Bernhard Brenner received a BSc in Medical Informatics from TU Wien, Austria, and an MSc from Denmarks Technical University (DTU), Denmark, in Computer Security. Bernhard joined SBA Research in April 2018 and since April 2019, he works at the Christian Doppler Laboratory for Security and Quality Improvement in the Production System Lifecycle (CDL-SQI) at TU Wien, Austria. His research focuses on methods for the protection of information in terms of access control, confidentiality of data and integrity of assets in computer aided CPS Engineering. He is currently a PhD candidate at TU Wien.



Andreas Ekelhart received a master's degree in Business Informatics and a master's degree in Software Engineering & Internet Computing from the TU Wien. He completed his PhD in Computer Science at the Institute of Software Technology and Interactive Systems at the TU Wien, exploring ontologies to formalize information security knowledge. At SBA Research he leads the department for applied research projects, and in 2018, he joined the Christian Doppler Laboratory for Security and Quality Improvement in the Production System Lifecycle (CDL-SQI). He is a member of the International Information Systems Security Certification Consortium (ISC2) and holds various industrial certifications including CISSP, CSSLP, MCPD, and MCSD.

Edgar Weippl is co-founder and Research Director of SBA Research, a Comet research center for information security. Since 2018, he has also been the Head of the Christian Doppler Research Laboratory Security and Quality Improvement in the Production System Lifecycle (CDL-SQI). His research focuses on the development of information security and quality improvement concepts, methods, and mechanisms. He was also the General Chair or PC Chair of major conferences including ACM CCS (2016), ACM SACMAT (2015, 2017) and ESORICS (2015).