A Risk and Threat Assessment Approaches Overview in Autonomous Systems of Systems

Aida Čaušević
Mälardalen University
Västerås, Sweden
Email: aida.causevic@mdh.se

***Abstract*—Systems of systems (SoS) have been introduced in early 1990s in air traffic control domain, defense and information technologies. Systems like this contain a set of components, being systems itself, with constituent components retaining operational independence. The definition and configuration of SoS have evolutionary nature and emergent behavior is one of the many important characteristics to be mentioned.**

Over the past ten years fast technological and industrial advances in the domain of autonomous and cooperating systems started to occur, which created new opportunities to use the benefits of SoS. In the near future, fully autonomous and cooperating systems are expected to become our reality and increase the production efficiency, while decreasing the human effort in harmful environments. There exist the need to make sure that critical properties of SoS, such as safety and security are guaranteed as a joint effort, since it is not sufficient anymore to address these properties independently in the development process. In this paper an overview of the most common approaches and methods used to provide reasoning about joint safety and security is provided, as well as a check of the latest updates in standards related to these properties.

I. Introduction

We are facing new trends in system development that create a shift from the traditional system development, towards systems consisting of a number of components being systems itself, independently developed and deployed, able to communicate and collaborate in order to provide a set of enhanced and improved services. These systems are referred as Systems of Systems (SoS). While all SoS are systems, not all complex systems are SoS where the main difference is that parts of SoS act as autonomous systems itself, are able to form their own connections and variety in their diversity, can lead to enhanced functionality, and contribute in fulfillment of capability demands coming from a SoS itself [1].

SoS are connected to public or semi-public networks, involve multiple stakeholders, have dynamic system reconfigurations, and unpredictable operating environments. Assuming these systems to be autonomous, one needs to carry in mind that supporting technology is still under the development and it will take some time to come up with new methods and techniques needed for understanding and analyzing such systems. Additionally, a range of technologies including hardware, software and infrastructure are utilized without clear understanding of possible security implications [2]. Let us assume that a component used in a larger control system comes with vulnerability not known to anyone in the chain of responsibility at the time of deployment. This might result in system exposure to the vulnerability and create an opportunity for adversary to easily enter and make harm to the system. It is often the case to outsource many activities including design and development of components used in the system. In these situations manufacturers are working in isolation and their work is contract defined, meaning that they will not add any additional security measure beyond those already existing in the contract, and in this way they might create additional safety hazards for the future SoS.

Figure 1 depicts a Volvo's vision of future autonomous SoS. The quarry example is operated in two shifts. In the morning, crushed rock is loaded by an excavator into dump trucks. In the afternoon shift, the morning operation continues, but additional rock is stockpiled, ensuring that loads are both ready to be loaded the next day, preventing potential unplanned stops. They take into the consideration the fact that the work place (i.e., a quarry) is changing constantly (e.g., with each blast more space is created), and to approach to the resulting rocks one can either move the rocks to the crusher, or a crusher can be moved to the rock, which can be both time consuming and costly. To make the work more efficient they have introduced battery-powered autonomous electric load carriers. A fleet of these unmanned carriers are expected to be able to move the same amount of load as one large haul truck. Also in case one of these carriers goes down, it will be a much smaller loss to a quarry's production compared to the large haul truck. However, since the vehicles are expected to be fully autonomous all possible processes and scenarios need to be documented and analyzed taking into consideration all new critical situations. Due to the emergent behavior, functionalities usually not provided by single systems become available. It is expected to use different types of communication (e.g., GPS, machine to server communication, machine to machine communication, etc.) and therefore one has to be also prepared to deal with possible threats, coming from the security domain, to safety of the whole SoS.

To summarize, for autonomous SoS in general one can assume the following: i) emergent behaviors given that they enable continuous evolution of the overall system during its operation; ii) large and often distributed physical systems with complex dynamics; iii) dynamic reconfiguration of the overall system on different time-scales; iv) partial or full autonomy of the subsystems; v) deployment in safety-, and mission-

Fig. 1. A system of systems as envisioned by Volvo - The Electric Site quarry [3]

critical systems, where the shortest interruption of service might introduce hazardous and life-threatening events; vi) systems no longer vulnerable only to unintentional threats (i.e., "foreseeable misuse"), but also to intentional threats posing challenges to the system security.

Bearing in mind above described characteristics, and given that it is challenging to define system boundaries, it becomes a tedious task to enable quality assurance, especially satisfying level of safety and security assurance. In dynamic and distributed systems, such as SoS, ensuring the safety in isolation without taking into consideration security threats is no longer sufficient.

For many years now, safety and security properties have been treated as two distinctive system qualities, and addressed by two separate communities each focusing on their own methodologies, analysis techniques and tools. However, already in 1990s researchers have brought up the commonalities between safety and security and possible need of addressing these properties as a joint effort and developing new ways to reason about them together [4], [5], [6], [7], [8]. In the following years, the research community has focused on existing techniques, identifying similarities, as well as differences, and presenting perspectives how these two can be harmonized under the same roof.

In this paper we provide a discussion on SoS from a perspective of safety and security assurance. In II we briefly describe SoS. We describe the most common safety and security interdependencies in SoS in Section III, followed by overview on the most relevant academic approaches, presented in Section IV. Section V provides an overview on some published industrial work in this area. In Section VI we review some of the relevant safety and security standards. Finally, in Section VII we conclude the paper with discussion on gathered information and provide some insights into our future work.

II. What is a System of Systems?

In order to enable an analysis of a given system one needs to define system borders and have a clear picture on what is included in a system definition. It is a prerequisite for any type of analysis, since it defines the scope and the flow of the analysis. For example, in terms of safety, the risk analysis starts from a system definition and identifies all hazards that can lead to accidents or any other type of damage to the system, people, and environment. It is a similar situation with security. With a well documented system definition it becomes easier to focus on sources of possible threats and recognize security risks most likely to appear in such a system and influence new hazards to appear. Therefore, in this section we overview and discuss some of the existing SoS definitions.

Term SoS does not have one widely recognized definition, yet. However, the notion is generally known and accepted in both research community and industry. One of the early SoS definitions has been provided by Kotov [9]. He argues that SoS are large-scale concurrent and distributed system, whose components are complex systems themselves. As examples of SoS systems he uses multiprocessor servers and clusters and distributed control systems. Periorellis and Dobson stress the importance of cooperation between autonomous component system as the key feature of SoS [10]. The purpose of SoS is to enable enhanced or improved emergent services, based on capabilities of the participating components in the SoS.

According to Maier, SoS are collaborative systems, formed as a collection of components that fulfill valid purposes in their own right and continue to operate in the same pace when disassembled from the rest of the system [11]. His definition is one of the first steps towards distinguishing SoS from large traditional systems, by introducing the notion of component independence. Additionally, he introduces terms evolutionary nature and emergent behavior as a product of such systems. Hall-May et al. define SoS as "*systems whose constituent*

components are sufficiently complex and autonomous to be considered as systems in their own right and which operate collectively with a shared purpose" [12]. They observe that the interactions between component systems are not restricted by physical design.

Rae et al. argue that SoS are a well established concept, but the circumstances under which they are used are not well defined [13]. As the main characteristic of SoS, they assume fluid configuration and fragmented management. They stress the importance of detaching the definition of SoS from the traditional monolithic systems. They introduce terms of *SoS Concept*, *SoS Configuration* and *SoS Instance* to help in understanding and defining the SoS. According to them *SoS Concept* is given by a set of configurations, where SoS are assumed to have a fluid configuration, meaning that many configurations may appear and become instances of the same SoS. As an example they use wireless networks, whose configuration changes whenever a new device registers to the network. A physical system becomes a part of an *SoS Instance* by joining the configuration. A vehicle that is joining to the end of a convoy, where the set of vehicles may be a valid *configuration* of the convoy, an *SoS Concept*.

It is obvious that one common definition, applicable and operational in all SoS environments, cannot be established. However, one has to notice that most of the authors mentioned above agree on some common properties, such as *emergent behavior*, *independent component* of the system, *complexity* of SoS, *collective operation with a shared purpose*, etc., that can be seen as the basis for further understanding of SoS, be it autonomous or not.

III. Safety and Security interdependencies in SoS

In systems like this, one has to be able to guarantee fulfillment of system properties of interest. In this paper the focus is on functional safety and security properties that might affect safety in complex autonomous SoS. Safety can be described as the avoidance of catastrophic consequences on the environment or harm to human lives, while security should provide confidentiality, integrity, and continuity of operation. So far, these dependability properties have been traditionally addressed by two different communities and usually isolated one from the another. However, with technological advances, it became clear that looking into safety, and not taking into account security aspect does not make sense anymore. Especially, if we consider type of systems such as SoS that are nowadays used in areas where safety-, or security-related failures could have severe consequences, such as transportation, health care, defense, rail systems, consumer products, media, energy supply systems, etc.

In recent years, the research community has put some effort into studying safety and security properties, identifying similarities and differences, and moreover looking into ways to bring the reasoning around them together. This has resulted in a number of solutions that advocate ways how to integrate and harmonize methods and techniques in order to put them under the same roof [14].

In early 1990s, Burns et al. have identified a need to make clear distinctions between terms safety and security in order to produce better analysis techniques to reason about them [8]. Their definition is based on the differences on the casual structure, introducing terms of relative harm caused by security-critical systems and absolute harm caused by safety-critical systems. The discussion is illustrated by an analysis of a number of cases of system failure where the safety and security issues seem, at least at first sight, to be difficult to distinguish.

Eames et al. made an observation already in 1999, where they claimed that it is acceptable to extend the definition of either safety or security to include both concepts, but they argued as well that it is inappropriate to attempt to unify safety and security analysis techniques [15]. They have grounded their claims on the fact that specialized approaches and techniques related for any of these properties, have been developed with purpose to provide a detailed analysis of the property. However, a process of unification could involve some compromise, which could lead to incomplete analysis, making some security threats and safety risks to remain unforeseen.

In [16] authors report on results achieved within the SafSec project, where the aim has been to investigate possibilities for common safety and security argumentation, while performing combined analysis. They have focused on integrated modular avionics domain and come with a new approach to the certification of highly modular safe or secure systems, based on the construction of safety and security arguments and the collection of evidence supporting those arguments.

An interesting approach has been presented in [17], where authors have showed how a security breaches in a system can bring the system at harm, making safety properties no longer satisfied. The paper is presented from the adversary point of view proving that these two properties can no longer be separated and that there is need to have a one analysis that will take into account both safety and security, as well as their interdependencies.

Pietre-Cambacedes et al. talk about four types of interdependencies between safety and security [18]. They define: i) *conditional dependency*, where fulfillment of security requirements conditions safety or vice-versa; ii) *mutual reinforcement*, where safety requirements or measures contribute to security, or vice-versa. Mutual reinforcement enable resources optimization and cost reduction; iii) *antagonism*, where safety and security requirements or measures lead, when considered together, to conflicting situations; and iv) *independence* define situations without existing interaction between these two properties. In this research the most interest is into conditional dependencies, especially the case where failing to satisfy security requirements produces new safety risks to the system.

Kriaa et al. propose an approach to model safety and security interdependencies using Boolean logic Driven Markov Processes formalism and apply it on an industrial case study taking into consideration the system architecture [19]. Moreover, they provide a discussion on the convergence of security and safety issues in industrial control systems and their possi-

ble interdependencies focusing on already mentioned types of interdependencies, i.e., mutual reinforcement and conditional dependency.

What is clear today is that security provides a significant impact on safety in open and complex systems as autonomous SoS are, and in case of not being treated within the common approach and analyzed by methods capable to take into account both of these properties, one could expect catastrophic hazards and accidents to occur.

IV. State-of-the-art methods

In this section a review on solutions related to combined safety and security reasoning is provided.

Most of the publications related to safety and security considerations in SoS are position statement publications that typically discuss challenges to be addressed in the future [20], [21], [22], [17]. On the other side, there is a number of publications related to joint safety and security reasoning, but not specifically to SoS [23], [24]. In most cases, related solutions focus either on safety engineering and existing safety approaches with security aspects or improving security engineering with safety techniques. The first group of approaches is highly related to our work, since we aim at enhancing safety work with notions of security, and our intention is to focus only to those security threats that might endanger system safety. We describe some of them in the following.

Macher et al. propose a combined analysis of safety and security properties called SAHARA (security-aware hazard analysis and risk assessment) that is a merge of Hazard Analysis and Risk Assessment (HARA) approach coming from automotive domain with STRIDE coming from the security domain [25]. The proposed approach is in line with automotive safety standard ISO 26262 for road vehicles. They include a classification scheme for probability of security threats, useful when determining appropriate counter measurements. They also provide an analysis of the impact of identified security threats on the safety analysis of automotive systems.

Ponsard et al. illustrate the challenges of safety and security co-engineering to the growing connectivity and new trends towards autonomous vehicles [26]. They recognize the need of continuous maintenance of security related data in order to enable required level of safety. The main challenge, is on how to preserve the same level of safety while updating security data. They propose requirements engineering based approach using goal-oriented requirements engineering that has shown good capabilities for modeling requirements and reasoning about them and is able to provide decomposition while preserving global properties.

Winther et al. have looked into problems related to security that could reflect onto safety, and with respect to that, they have developed HAZOP specially suited to identify security threats [27]. They have established modifications on already existing method by introducing new guide words, attributes, and templates for combined analysis of these properties. In addition, they have demonstrated the approach on the safety related system.

Similar to the previous approach, in [28] authors propose the use of the HAZOP approach to analyze the security issues in today's complex systems that are operating in high-risk environments. The main advantage of the approach is the fact that it provides a rigorous security analysis, and it can supplement and integrate with other forms of analysis. It does not cover all security issues, but it provides useful information and systematic analysis. They provide a e-commerce case study to demonstrate the power of the approach.

A framework, based on probability as a measure of uncertainty, that aims for risk analysis, focusing on both safety and security has been presented in [29]. Authors take into account that risk is a combination of possible consequences and associated uncertainties.

Young et al. provide a new system thinking approach for safety and security assurance [30]. Systems-Theoretic Process Analysis for Security (STPA-Sec) augments traditional security approaches and introduces a top-down analysis process designed to help a multidisciplinary team consisting of security, operations, and domain experts identify and constrain the system from entering vulnerable states that lead to losses. The approach allows to focus on vulnerable states in order to avoid threats to exploit them and create disruptions, and eventual losses.

Studying the mutual relationships between safety and security in cyber-physical systems (CPS), Kornecki et al. [31] realized that this interaction can be seen both as a synergy or conflict depending on the circumstances in which a system operates. They have proposed an approach based on Bayesian Belief Networks to evaluate factors related to safety and security of CPS, assumed to be randomly distributed. The approach is evaluated in an oil pipeline control to observe safety and security violations. The main goal of this approach has been to prove that approaches like this can complement other techniques dealing with joint assessment of safety and security.

Simpson et al. present their findings on the already noted relation between safety and security, where they aim at using existing theory of non-interference (well-known in research focusing on security) when describing safety-critical systems [32]. They use event-based description of systems to show different notations of safety. The approach is based on division of the system into components that can be later on reasoned about. A simple example is presented to illustrate the application of this technique to different classes of a safety property.

V. State-of-the-practice

Despite the academic efforts towards proposing combined approaches for safety and security analysis, there is still a lack of integration between safety and security practices in the industrial context. One of the reasons for this is due to the existence of separate standards and independent safety and security assurance processes, often addressed by different organizational teams, and under the certification of different standards.

Through the project we run at our department, CloSS [1] we have had an opportunity to meet some of the companies in Sweden and talk about these issues with them. In context of complex, software-intensive systems all of the companies we have met have realized the need to treat safety and security properties within one unified process, as early as possible. In most cases they have already developed processes to support assurance of these properties, usually within complementary processes. The major challenge is the lack of suitable standards to guide them in this process. In general, security is not covered in any detail in safety standards that makes software-intensive and successfully safety-certified systems, still open for security threats. In general, it is evident that there is a lack on industrial case study or any strong evidence related to this topic. However, we have been able to identify work of Maysz et al. [33] as highly relevant in this area. In their technical report provide a guidance for risk-driven approach within marine cyber-security taking into account Rolls-Royce perspective. They find complex interaction between safety and security within maritime domain as a challenging engineering task, especially when taking into account chains of events such as malware being accidentally introduced and compromises the safety. They argue that existing system engineering techniques are mature enough to deal with multiple qualities, however iterative nature of risk-based systems engineering might introduce high system cost since the two quality factors interact and potentially increase the number of design iterations.

VI. Safety and Security Standards

A. Safety standards

To the best of our knowledge, there is no either safety or security standard that directly addresses these properties in context of complex SoS. The closest to joint safety and security assessment is SAE j3061 [34], guidebook on cyber-security, that covers vehicular domain. However, this document cannot be seen as standard itself, since it provides only a guide on how to include cyber-security when developing complex systems. There is no details on which methods, and techniques are the most applicable and should be used. In the following we overview some of the existing and well known safety and security standards, relevant to SoS.

IEC 61508 [35] is an international standard focusing on functional safety of electrical, electronic, and programmable electronic safety-related systems, applied in industry. It provides a definition of a functional safety as a part of the overall safety related to "part of the overall safety relating to the EUC (Equipment Under Control) and the EUC control system which depends on the correct functioning of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities." It defines safety integrity level (SIL) as a discrete level, ranging from SIL 1 as the lowest and SIL 4 as the highest level of safety. The standard has its origin in process control industry and covers the whole safety life-cycle.

[1] http://www.es.mdh.se/projects/472-Software_Center_Closing_the_safety_security_gap_in_software_intensive_systems

ISO 13849 [36] is an international standard on safety of machinery, and safety-related parts of control systems. It focuses on providing requirements and guidance on the principles for the design and integration of safety-related parts of control systems, including software design. It specifies the performance level required for enabling safety functions.

ISO 26262 [37] is an international standard that addresses functional safety related to road vehicles. All parts of the development process are covered starting from the specification, through the implementation, integration, verification, validation and finally product release. ISO 26262 defines functional safety for automotive equipment applicable throughout the life-cycle of all automotive electronic and electrical safety-related systems.

B. Security standards

The ISO/IEC 27000-series of Information Security Management System is a joint work of the International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC).The aim of these two series is to provide recommendations on information security management, risks and controls within information security management system domain. It covers a broad scope including, privacy, confidentiality and IT security issues. These standards expect organizations to assess their information security risks, implement appropriate steps for information security assurance using the provided guidance and suggestions. Additionally, a continuous feedback and improvement activities are required throughout a "plan-do-check-act". The series include ISO/IEC 217001 addressing requirements for information security systems management, ISO/IEC 27032 related to guidelines for cyber-security, and SO/IEC 27002 addressing the code of practice for information security controls.

ISA/IEC 62443 standard defines procedures for implementing electronically secure Industrial Automation and Control Systems [38]. It is a complete security life-cycle program, with best practices for developing and deploying policy and technology solutions to address security issues in control systems and mitigate possible cyber-security threats.

VII. Discussion

This paper provides an overview on the current trends on joint safety and security work, related to the risk analysis in the domain of autonomous SoS. The domain of autonomous SoS is relatively new and there are still issues to be addressed. So far, safety and security have been topics of interest in two separate communities, but it is evident that with current trends, where systems are built as complex SoS, one has to think about new solutions that will take both properties into account through one unified approach and analyze their impact on each other. It is evident that the industry faces with new challenges when developing software-intensive safety-, and security-critical systems established over a communication environment. We have observed that some supporting methods, techniques and tool for system development existing in specific domains are inadequate and lack system and process thinking.

On the positive side, safety and security reasoning is gaining an attention from both research and industrial community. Most of the reviewed contributions have started from the already existing approaches from either safety or security domain and extended it towards the other property. These solutions might be suitable at the moment, but for the future we have to think about providing approaches, not only specialized in either safety or security domain, but capable to take both of these properties into account already at early stages of system development. With solutions like this, we will be able to cope with safety and security related questions in advanced systems such as autonomous SoS. At the moment there is a big initiative in many of the mentioned standards to update them towards including security perspective and it is expected to be available soon.

VIII. Conclusions

Through the findings in this paper we have seen that there exist a need for a joint functional safety and security approaches. There is significant effort coming from academic community, in most cases with an industrial support. As future work we plan to focus on developing approaches that will support joint safety and security analysis.

Acknowledgments

This work is funded through PiiA research postdoctoral program and RAASS project, ECSEL JU SafeCop project, CloSS project funded by Software Center Sweden, and The Knowledge Foundation (KKS) funded SAFSEC-CPS project.

References

[1] M. W. Maier and E. Rechtin, *The Art of Systems Architecting*. Boca Raton, FL, USA: CRC Press, Inc., 2000.

[2] M. Warren and W. Hutchinson, "Cyber attacks against supply chain management systems: a short note," *International Journal of Physical Distribution & Logistics Management*, 2000.

[3] M. G. Doyle, "How Volvo CE is engineering a quarry run by electric loaders and haulers for big cuts to costs and emissions," http://www.equipmentworld.com/how-volvo-ce-is-engineering-a-quarry-run-by-electric-loaders-and-haulers-for-big-cuts-to-costs-and-emissions/, 2016, [Online; accessed 31-March-2017].

[4] V. Stavridou and B. Dutertre, "From security to safety and back," in *Computer Security, Dependability and Assurance: From Needs to Solutions*, 1998.

[5] D. P. Eames and J. Moffett, *The Integration of Safety and Security Requirements*. Springer Berlin Heidelberg, 1999.

[6] J. Rushby, "Critical system properties: Survey and taxonomy," Computer Science Laboratory, SRI International, Tech. Rep. SRI-CSL-93-1, 1994.

[7] D. F. C. Brewer, *Applying Security Techniques to Achieving Safety*. London: Springer London, 1993.

[8] A. Burns, J. McDermid, and J. Dobson, "On the meaning of safety and security," *Comput. J.*, April 1992.

[9] V. Kotov, "Systems of systems as communicating structures," 1997.

[10] P. Periorellis, D. P. Periorellis, P. John, and E. Dobson, "Organisational failures in dependable collaborative enterprise systems," *Journal of Object Technology*, 2002.

[11] M. W. Maier, "Architecting principles for systems-of-systems," *Systems Engineering*, 1998.

[12] M. Hall-May and T. Kelly, *Defining and Decomposing Safety Policy for Systems of Systems*. Springer Berlin Heidelberg, 2005.

[13] A. J. Rae and A. Rob, "Is the "system of systems" a useful concept for hazard analysis?" Proceedings of the 29th International System Safety Conference, August, 2011.

[14] C. W. Axelrod, "Applying lessons from safety-critical systems to security-critical software," in *IEEE Systems, Applications and Technology Conference, Long Island*, May 2011.

[15] D. P. Eames and J. Moffett, *The Integration of Safety and Security Requirements*. Springer Berlin Heidelberg, 1999.

[16] S. Lautieri, D. Cooper, and D. Jackson, *SafSec: Commonalities Between Safety and Security Assurance*. Springer London, 2005.

[17] K. Hansen, "Security attack analysis of safety systems," in *IEEE Conference on Emerging Technologies Factory Automation*, Sept 2009.

[18] L. Pitre-Cambacds and M. Bouissou, "Modeling safety and security interdependencies with bdmp (boolean logic driven markov processes)," in *IEEE International Conference on Systems, Man and Cybernetics*, Oct 2010.

[19] S. Kriaa, M. Bouissou, F. Colin, Y. Halgand, and L. Pietre-Cambacedes, *Safety and Security Interactions Modeling Using the BDMP Formalism: Case Study of a Pipeline*. Springer International Publishing, 2014.

[20] P. Allen, A. Ames, C. Belta, M. Campbell, G. Hager, L. Kavraki, H. Kress-Gazit, V. Kumar, M. Mataric, and M. Schwager, "National science foundation workshop on future directions in cyber-physical systems, robotics, and autonomy," USA, Tech. Rep., 2015.

[21] M. Gerla and P. Reiher, "Securing the future autonomous vehicle: A cyber-physical systems approach," in *Securing Cyber-Physical Systems*. CRC Press, 2015.

[22] V. Izosimov, A. Asvestopoulos, O. Blomkvist, and M. Trngren, "Security-aware development of cyber-physical systems illustrated with automotive case study," in *Design, Automation Test in Europe Conference Exhibition*, 2016.

[23] J. Cusimano and E. Byers, "Safety and security: two sides of the same coin," http://www.exida.com/images/uploads/238.pdf/, accessed: 2016-12-13.

[24] R. Winther, *Qualitative and Quantitative Analysis of Security in Safety and Reliability Critical Systems*. Springer London, 2004.

[25] G. Macher, H. Sporer, R. Berlach, E. Armengaud, and C. Kreiner, "Sahara: A security-aware hazard and risk analysis method," in *Design, Automation Test in Europe Conference Exhibition*, March 2015.

[26] C. Ponsard, G. Dallons, and P. Massonet, *Goal-Oriented Co-Engineering of Security and Safety Requirements in Cyber-Physical Systems*. Springer International Publishing, 2016.

[27] R. Winther, O.-A. Johnsen, and B. A. Gran, *Security Assessments of Safety Critical Systems Using HAZOPs*. Springer Berlin Heidelberg, 2001.

[28] T. Srivatanakul, J. A. Clark, and F. Polack, *Effective Security Requirements Analysis: HAZOP and Use Cases*. Springer Berlin Heidelberg, 2004.

[29] T. Aven, "A unified framework for risk and vulnerability analysis covering both safety and security," *Reliability Engineering & System Safety*, 2007.

[30] W. Young and N. Leveson, "Systems thinking for safety and security," in *Proceedings of the 29th Annual Computer Security Applications Conference*. ACM, 2013.

[31] A. J. Kornecki, N. Subramanian, and J. Zalewski, "Studying interrelationships of safety and security for software assurance in cyber-physical systems: Approach based on bayesian belief networks," in *Federated Conference on Computer Science and Information Systems*, Sept 2013.

[32] A. Simpson, J. Woodcock, and J. Davies, "Safety through security," in *Proceedings of the 9th International Workshop on Software Specification and Design, Washington, DC, USA*. IEEE Computer Society, 1998.

[33] V. Malysz, R. Melville, and R. Oates, "Cyber security risk management systems." E&T Cyber Security Hub, 2017.

[34] SAEJ3061, "Cybersecurity guidebook for cyber-physical vehicle systems." SAE International, 2016.

[35] "IEC 61508 -functional safety of electrical/electronic/programmable electronic safety-related systems." 2010.

[36] "ISO 13849 - safety of machinery - safety-related parts of control systems." International Organisation for Standardisation., 2009.

[37] "ISO 26262 - road vehicles - functional safety." International Organisation for Standardisation., 2011.

[38] "ISA/IEC 62443 - industrial network and system security." 2010.