Safety Science 151 (2022) 105741

Contents lists available at ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/safety

Integrated management of safety and security in Seveso sites - sociotechnical perspectives

Marja Ylönen [a,*], Alessandro Tugnoli [b], Gabriele Oliva [c], Jouko Heikkilä [d], Minna Nissilä [d], Matteo Iaiani [b], Valerio Cozzani [b], Roberto Setola [c], Giacomo Assenza [c], Dolf van der Beek [e], Wouter Steijn [e], Nadezhda Gotcheva [d], Ernesto Del Prete [f]

[a] University of Stavanger, 4036 Stavanger, P.O. box 8600, Norway
[b] LISES – Department of Civil, Chemical, Environmental and Materials Engineering, Alma Mater Studiorum – University of Bologna, via Terracini 28, 40131 Bologna, Italy
[c] University Campus Bio-Medico of Rome, Via A. del Portillo 21, 00128 Rome, Italy
[d] VTT Technical Research Centre of Finland Ltd, Visiokatu 4, P.O. Box 1300, 33101 Tampere, Finland
[e] TNO, Schipholweg 77, 2316 ZL Leiden, the Netherlands
[f] National Institute for Insurance against Accidents at Work (INAIL), via Roberto Ferruzzi 38/40, 00143 Roma, Italy

ARTICLE INFO

Keywords:
Safety
Security
Cybersecurity
Integrated management
Sociotechnical
Seveso

ABSTRACT

The call for integrated management of safety and security (IMSS) derives from intensification of digitalisation development and the increased reliance on information communication technologies (ICT) in high-risk industries, such as the chemical and process industry. This development means tightened interconnectedness between industrial automation and control and information technology systems. As a result, the risk landscape is changed towards a stronger interconnectedness of safety, physical and (cyber)security risks, which may lead to major accidents. The objective of this paper is to examine the motivations for IMSS, the current state of IMSS, the cybersecurity-induced risks, including the actualisation of interconnected risks and some sociotechnical tools for IMSS in Seveso plants. They are plants where certain quantities of dangerous substances are present, which are subject to the requirements of the Seveso III Directive (2012/18/EU). The data considered is open source and related to cyber and physical security-induced accidents; interviews with the representatives of Seveso sites and regulators; and literature. The method is qualitative content analysis. The results show that, despite the ongoing development in IMSS at the Seveso sites, IMSS is still in its infancy. Indeed, cybersecurity is often handled in a separate IT department, and the communication with process-safety experts is often inadequate. Furthermore, safety and security risk identification and assessment are essentially undertaken separately. To achieve a real IMSS, we argue that the co-existence of technical and organisational, including structural, functional and cultural development is a fundamental aspect. The combination of such complementary aspects represents the main novelty of this study.

1. Introduction

This paper is motivated by the changing risk landscape, which refers to a convergence of cybersecurity risks, physical security risks and safety risks (referring to process-safety, and holistically plant safety risks) in the process-industry, such as in Seveso plants, which may lead to major accidents. Convergence of risks relates to an increasing interconnectedness between information and communication technologies (ICT) and industrial automation and control systems (IACS), which are part of operational technology systems (OT). There are several mechanisms through which this interconnectedness between ICT and OT can occur; for instance, process-industry companies are interested in obtaining real-time data from their industrial processes by using monitoring sensors, willing to use smart tools, e.g., AI tools to analyse big

* Corresponding author.
E-mail addresses: marja.k.ylonen@uis.no (M. Ylönen), a.tugnoli@unibo.it (A. Tugnoli), g.oliva@unicampus.it (G. Oliva), Jouko.Heikkila@vtt.fi (J. Heikkilä), minna.nissila@vtt.fi (M. Nissilä), matteo.iaiani@unibo.it (M. Iaiani), valerio.cozzani@unibo.it (V. Cozzani), r.setola@unicampus.it (R. Setola), giacomo.assenza@unicampus.it (G. Assenza), Dolf.vanderbeek@tno.nl (D. van der Beek), Wouter.steijn@tno.nl (W. Steijn), nadezhda.gotcheva@vtt.fi (N. Gotcheva), e.delprete@inail.it (E. Del Prete).

https://doi.org/10.1016/j.ssci.2022.105741
Received 13 January 2022; Received in revised form 20 February 2022; Accepted 8 March 2022
Available online 16 March 2022
0925-7535/© 2022 The Author(s). Published by Elsevier Ltd. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

data derived from sensors, or planning/forced to use remote-control (e.g., due to travel limitations during COVID19 pandemic) (Kaspersky and ARC Advisory Group 2020). The aforementioned features and activities connect IACS/OT to public networks (ICT) and render IACS/OT more vulnerable and susceptible to cybersecurity interferences (Boyes et al. 2018).

Historically, IACS/OT have been separated from ICT systems. However, there is an increasing pressure from companies' business departments to obtain real-time data from the production processes to be able to better manage them (Brunt and Unal 2019; Boyes et al. 2018). Furthermore, obtaining real-time data from the industrial processes has often been justified by process-safety engineers for safety reasons. In fact, receiving real-time data from the processes enables timely interventions when some disturbances occur. However, when IACS/OT systems are connected to ICT systems, borders between these systems get blurred, and the vulnerability of IACS/OT increases due to increasing potential of cybersecurity breaches.

The tendency of ICT and IACS/OT's expanding interconnectedness has continued for the decades but nowadays it is escalating due to increasing digitalisation, automation, and the use of smart AI tools in high-risk industries, such as Seveso plants. This trend creates a demand for IMSS. Notably, most Seveso plants have indeed improved their management of safety and security, and many developments are still ongoing. Yet, we argue that much remains to be done from a holistic approach and in raising awareness regarding the IMSS.

A review of 369 security incidents (both physical- and cyber-related) in the process industry carried out by Iaiani et al. (2021a) testifies that their number of occurrence has significantly increased after the year 2000, making the security of chemical and process facilities as an issue of major concern. In the last 20 years, about 27% of recorded security incidents had cyber-related causes and, except for a peak between 2000 and 2004, they showed an almost constant time trend, stressing the ongoing nature of the issue despite the increasing awareness of cyber-risks.

Physical and cyber security attacks (e.g., terroristic attacks) on chemical and process plants may generate major events, such as releases of hazardous materials, fires, or explosions with consequences comparable to those of safety-related events, e.g., equipment failure and natural events (NaTech events, floods, earthquakes) (Landucci and Reniers 2019). In fact, damage to workers, local population (injury or fatality), the environment and property were recorded (Iaiani et al. 2021a) as final outcomes suffered by the facilities affected by intentional malicious attacks.

The aim of the paper is thus to participate in the discussion of changing the risk landscape and increasing the awareness of socio-technical, inter-organisational and organisational aspects that must be considered when discussing IMSS in process-industries. In this view, the paper aims to examine the motivations for and current state of IMSS in Seveso plants; cybersecurity related risks and actualisation of interconnected risks; as well as some sociotechnical tools to enhance the current state of IMSS in the process-industries.

This paper is based on the research project SAF€RA 4STER (https://projects.safera.eu/project/21), which is related to the Integrated Management of Safety and Security in Seveso plants, supported by the SAF€RA consortium. This two-year research project was carried out in 2019–2021 as a collaboration among the Technical Research Centre of Finland, VTT, the University of Bologna, the University Campus Bio-Medico of Rome, Italy, and the Netherlands Organization for applied scientific research, TNO (Ylönen et al. 2021).

The research questions regarding this paper are as follows:

- What kind of motivations are there to integrate the management of safety and security (IMSS)?
- What is the current state of IMSS?
- What type of cyber risks related scenarios can be found?
- What kinds of sociotechnical tools can be used to enhance the current state of IMSS?

The data used in the paper consists of a literature review regarding the existing (integrated) management of safety and security, as well as concepts of safety and security. Furthermore, 23 interviews were conducted with the Seveso regulators in Finland and the Netherlands, in addition to security and safety experts in Seveso plants in Finland and Italy. The method of analysis is qualitative content analysis (Krippendorff 2013).

The structure of this article is as follows: The next section describes the core concepts and theoretical framework; the third section deals with the data and method; the fourth section focuses on the analysis of the main motivations for and current state of IMSS, the management system and any practical measures for the IMSS in a multi-plant context; the fifth section deals with findings regarding past incident analysis and sociotechnical tools for the identification and assessment of cyber risks related scenarios and tools to enhance IMSS; and the sixth section provides discussion and a conclusion.

2. Sociotechnical perspective and core concepts: safety, (cyber) security, risk assessment, integrated management

This section provides a conceptual orientation for the study. We start with definitions of the study's core concepts and then move on to present the theoretical framework within which we orientate to IMSS.

2.1. Safety, security, cybersecurity, risk assessment, integrated management

- **Safety:** without unacceptable risks, when those risks derive from the biophysical world, technical failures, human and organisational factors, or safety as antonym of risk (the safety level is linked to the risk level; a high safety means a low risk and vice versa) (see SRA Glossary, 2018)
- **Security:** without unacceptable risks, when those risks derive from malicious human intent, or security as antonym of risk (the security level is linked to the risk level; a high security level means a low risk and vice versa) (see SRA Glossary 2018)
- **Security in this study includes both physical security and cybersecurity**
- **Cybersecurity** is defined "*as the preservation of confidentiality, integrity and availability of information in the Cyberspace* (ISO/IEC 2012, 27032 Cyber Security)
- **Major event:** an event that results in the loss of an asset, whether it is a loss of capability, life, property, or equipment (Center of Chemical Process Safety 2003)
- **Risk assessment:** a systematic process to comprehend the nature of risk, and express and evaluate it, with the available knowledge (SRA Glossary 2018)
- **Integrated management of safety and security** refers here to an organisational function, procedures and practices that ensure that safety, physical security and cybersecurity risks are (co) identified, (co)analysed (co)assessed, prevented and mitigated. Integration of management can occur at structural, functional and cultural levels in an organisation (Jørgensen et al. 2006)

Integrated management refers to three different ways to link safety and security management. *The structural integration* refers to the increased compatibility of systems elements, such as using the similarities of the standards, or creating company level policies that integrate safety and security. *The functional integration* refers to the integration of core functions or coordination of generic processes, such as safety- and security management systems. The deepest level of integration is *cultural integration*, which refers to the embeddedness of an integrated management of safety and security in a culture of learning and continuous improvements (Jørgensen et al. 2006).

There are different approaches to safety; for instance, Eric Hollnagel has pointed to the paradox of safety, namely that reference to it as a positive phenomenon is often approached via its negation, that is, risks and accidents (Hollnagel et al. 2006; Hollnagel 2014). As an alternative, Hollnagel suggests that safety should be approached by looking at factors that contribute to things going well. These factors would include aspects that strengthen organisations resilience, i.e., their capacity to recover from the expected and unexpected events and maintain their core functions despite the crisis (Hollnagel 2014; 2011). We acknowledge the need to look at both positive (such as safety and security culture) and negative aspects, such as safety and security risk aspects, as without understanding the risks and vulnerabilities of a system it would be impossible to create resilience and IMSS.

2.2. The sociotechnical perspective and expertise

The sociotechnical perspective is a relevant framework when talking about complex interconnected ICT systems, process-automation systems and organisations, and the surprising effects deriving from the convergence of different subsystems and related risks. Sociotechnical refers here to the interconnectedness and complexity of social (including organisational) and technical systems (Kleiner et al. 2015; Leveson 2012).

The sociotechnical perspective emphasises multidimensional (human, organisational and technical) interactions between different subsystems (such as ICT, physical security and process-safety), as well as multilevel interactions pointing to the individual, an organisation and an organisation's external environment. Regarding the latter one can think of political, regulatory, technological, economic and cultural sub-environments, which create pressures to which an organisation needs to respond and adapt to survive (Harvey and Stanton 2014). Complexity is an inherent feature of sociotechnical systems, meaning that the performance of a system as a whole (e.g., a Seveso plant) cannot be predicted by knowing the states of the individual elements (Dekker et al. 2011). Consequently, the process-safety cannot be predicted solely from the point of view of process-safety, but the associated cybersecurity and physical security risks must be taken into account, as both can have negative effects on process-safety.

Furthermore, because of these complex interactions, surprises, such as accidents, may emerge. Moreover, it becomes difficult to find causes for surprises and accidents by analysing them via root-cause analysis. The key is that sociotechnical systems are in a continuous process of change, and linear analysis is not a sufficient tool to enhance understanding the complexity of these interactions and any resulting incidents and accidents (Dekker et al. 2011).

Since the sociotechnical perspective has been developed as an outcome of discussions by several disciplines, it has addressed relevant aspects. For instance, the sociotechnical perspective has indicated the limitations of traditional risk assessment approaches, particularly regarding the inability of linear risk assessment models to consider intricate interactions arising from complex systems that promote or hinder safety in high-risk industries like the nuclear or oil and gas industry (Aven and Ylönen 2019; Dekker et al. 2011). Furthermore, the conventional risk approaches with probabilities are inadequate to consider and reflect various aspects of risk and uncertainties in the context of sociotechnical systems (Aven and Ylönen 2019).

The sociotechnical perspective calls for an understanding of the system as a whole (such as a Seveso plant). It is within this holistic perspective that safety, security and cybersecurity have to be considered. This perspective provides a conceptual framework but also a motivation for applying IMSS. These motivational features will be examined in the analysis section.

2.2.1. Expertise related aspects in the risk, safety, and security context

Social and cultural approaches to safety are not integrated with technical risk assessment and related management, and these different schools do not communicate properly with each other (Wynne 1988, Jasanoff 1993; Aven and Ylönen 2019; 2021). The same goes for the safety and security domains, which are often separated from each other (De Maggio 2019). This relates broadly to an increasing specialisation of expertise in society (Giddens 1991; 1994). That means that expertise is becoming deeper and more specialised but at the same time narrower in scope, decreasing the capacity of experts to see beyond their own area of expertise and limiting their ability to understand and communicate with other experts (Giddens 1991, 1994; Jasanoff 1993). There are fewer generalists who have competences in different areas. Top IT experts are laypeople in the process-safety domain, and similarly, process-engineers are laypeople in the cybersecurity domain. Due to this specialisation of expertise, safety and security easily become boundary objects (Star 2010), referring here to a topic that is shared by various experts but at the same time understood in various ways, depending on the experts' disciplines and frameworks being used, as well as how the concepts are defined. As a result, as mentioned earlier, communication between different experts becomes challenging and misunderstandings may arise (Jasanoff 1993; Wynne 1996). However, the exchange of information and collaboration between experts would, in practice, be necessary for better management of the safety and security interface (e.g., Harvey and Stanton 2014; Gilligan 2021).

2.3. Analytical framework

The sociotechnical perspective functions here as a loose framework within which it is possible to address the relevant aspects, such as multilevel interactions, boundaries between the systems (safety and security management), communication, knowledge, and cultures, as well as the technological aspects (see Fig. 1) that need to be considered when improving the IMSS in an organisational context. In addition, inter-organisational aspects are relevant, as the performance of other companies located in the same industrial area, or vendors and suppliers, have effects on the safety and security of the site (Reniers et al. 2014). Moreover, the use of different risk assessment tools, as well as new technologies such as AI tools, represent sociotechnical aspects, per excellence, by including human and organisational competencies and technologies.

The sociotechnical perspective helps us to see the connections between organizations (management, competences, roles, responsibilities) and technical aspects (risk assessment methods and related software). For instance, cybersecurity has been managed separately from process-safety, although they are closely interrelated as mentioned in the introduction.

Furthermore, the sociotechnical perspective allows for discussion about the external environment as providing an institutional set-up within which IMSS can be developed. We do not focus in this paper on institutional set-up per se, but we complement the sociotechnical framework by including motivational, cognitive and practice aspects, as well as management related structural, functional and cultural aspects into the framework (see Fig. 2). There are several interfaces, and these can be found between the cultural and motivational aspects and functional and practical aspects, etc.

Additionally, there is an increasing need to transfer information from one organisational unit to another as well as a proper coordination of action throughout the relevant units in the organisation when safety, security and cybersecurity come together in terms of converging risks (Harvey and Stanton 2014). The way interfaces and boundaries function between different organisational units becomes an important indication of the success of IMSS.

In addition to the sociotechnical framework above, the examination of the current state of integrated management of safety and security is based on the following three dimensions: structures (e.g., an organisation's structure, strategies, and competences); functions (procedures); and culture (shared attitudes, values, beliefs, understanding and practices) (Jørgensen et al. 2006), see Fig. 2.

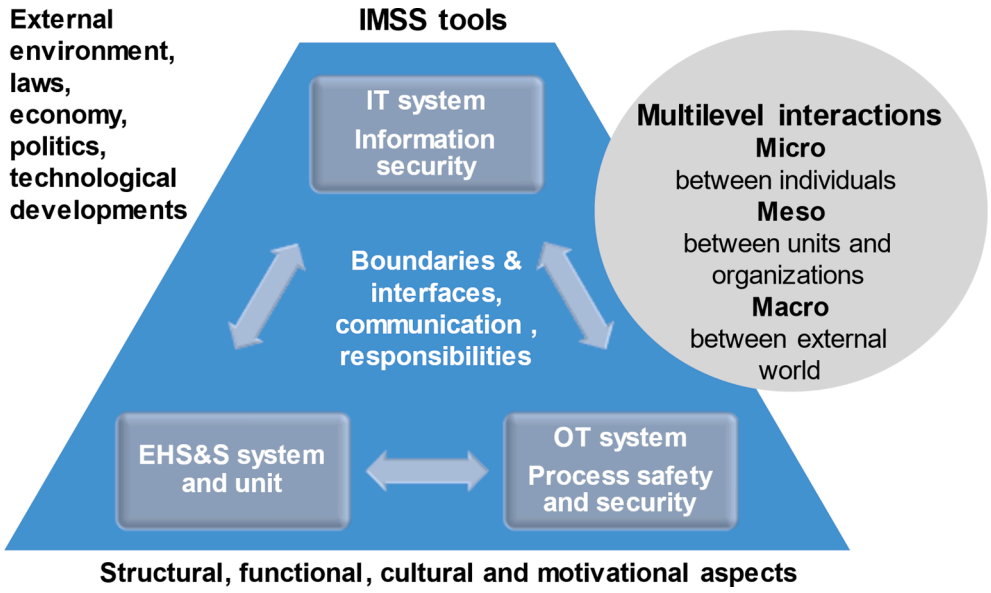

Fig. 1. The sociotechnical perspective on IMSS.

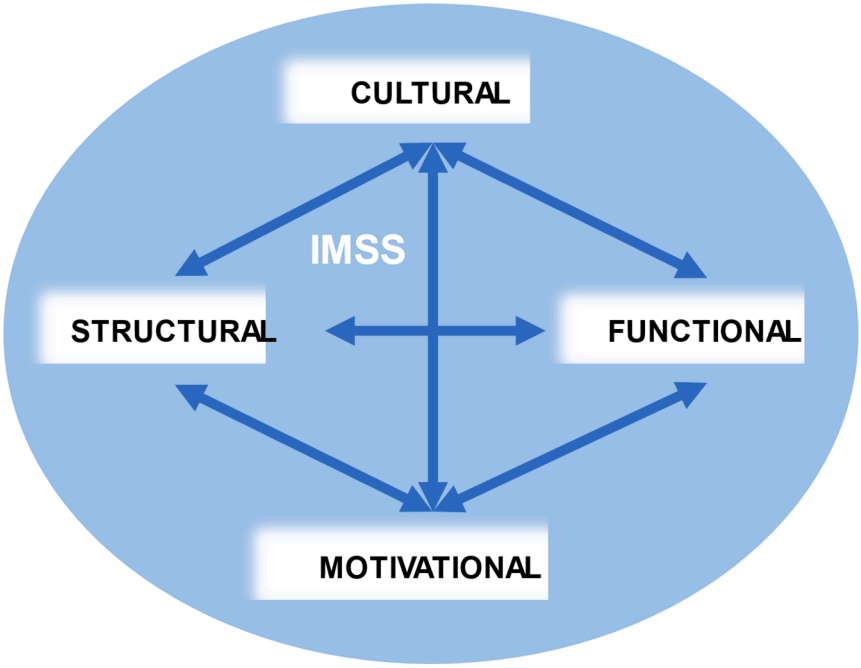

Fig. 2. Framework for analysing IMSS.

In the overall picture, motivation linked to understanding and knowledge about IMSS, communicating information and coordinating the action and boundaries of organisational units, as well as using technological tools, play a relevant role in the successful implementation of IMSS.

3. Data and method of analysis

The data of this study consist of a literature review on safety and security concepts and (integrated) management. The literature review includes 31 articles; four reports in the nuclear context regarding cybersecurity, computer security, as well as security culture; and four books. The key words "safety and security" were used in the search for articles. In addition, we browsed journals by looking at articles on integrated management and the Internet of Things in an industry context.

In the 10-year period from 2009 to 2019, 31 articles were selected for review. The articles were from Safety Science (9), Reliability Engineering and System Safety (8), the Journal of Loss Prevention in the Process Industries (5) and Process Safety Progress (3). These papers covered safety and security aspects, such as the identification and assessment of safety and security risks in the process industry; however, only a minority dealt with the integrated management of safety and security. In addition, we selected articles from Security Journal (1), the Journal of Integrated Security Science (2), Computers in Industry (1) and Cleaner Production (2) for review. In addition to these articles, we reviewed nuclear industry reports regarding cybersecurity, computer security, and security culture (Brunt and Unal, 2018; IAEA 2017; IAEA

2011; IAEA 2008). These reports provided points for comparison in terms of articles on safety and security cultures or cybersecurity. We also reviewed books on security science; the coupling of safety and security; and risk, crisis and security management (Bieder et al. 2020; Nolan 2015; Smith and Brooks 2012; Borodzicz 2005).

The analysis of this material involved a qualitative content analysis (Krippendorff 2013). When reviewing the articles, the initial criteria we used were the following: what is the industry specificity; does the article included a definition of safety; does the article included a definition of security; what specific features of safety and security were described (ontological differences); what are the interfaces between safety and security; and are there any possibilities to integrate the management of safety and security. A further analysis was made after the first review. This was based on the following criteria: different motivations for integration of safety and security, the main differences and similarities between safety and security concepts and management, and different tools to integrate the management.

With regard to interviews, a total of 23 Interviews were conducted with representatives of the chemical industry and Seveso sites (11), a security service company (2) and the regulatory bodies (7), as well as confederations of organisations in the chemical industry and oil and gas industry (3). Interviews were carried out in Finland, Italy and the Netherlands. The interviews were semi-structured thematic interviews that lasted around 1– 1.5 h. Themes covered interfaces between safety, security and cybersecurity and IMSS. The consent of interviewees was requested for their participation in the interviews and for recording them. During the interviews, notes were taken, and after the interviews, the recordings were transcribed. According to the General Data Protection Regulation (GDPR) interviewees and their companies were anonymised so that they could not be identified. The method of analysis is qualitative content analysis (Krippendorff 2013). In the analysis of interviews different levels of integration were used as an analytical framework (Jørgensen et al. 2006).

Except for one, the companies interviewed represent multinational companies headquartered in the USA and Europe. They have several sites in different countries in Europe and follow similar procedures for the management of safety and security. Thus, it can be argued that the study provides at least indicative results regarding the current situation of the IMSS in Europe.

4. Findings regarding motivations and current state of IMSS

This section summarises the main findings regarding motivations for and current state of IMSS. In addition, the management system and practical measures for dealing with IMSS in the multi-plant context are discussed.

4.1. Motivations for IMSS

We identified four interrelated motivations for IMSS (see Table 1). A strong motive and justification for IMSS derives from the fact that 1) safety and security have mutual interactions and influences (e.g., Song et al. 2019; Kriaa et al. 2015; Pièrre-Cambacédès et al. 2013). An example would be an insider (security) threat, such as an embittered employee, who intentionally operates valves incorrectly, thus compromising process-integrity and the safety of the site. Another example would be an external cyber-attack against the Seveso plant's operating system that could have severe process-integrity consequences and, in the worst case, health and environmental consequences. Recognition of the mutual interactions and influences of safety and security risks provides the motivation to manage them in a coordinated way.

Table 1
Motivations for integration.

Safety and security have mutual interactions and influences
Avoiding conflicts arising from competing goals and logics and related contradictions
Economic reasons: cost-efficiency
Risks: pure safety or pure security approaches cannot identify systemic risks and risks to the IACS

This first motivational category is the broadest one, and other categories add different perspectives and specifications to the first one. Another motive and justification for IMSS 2) relates to avoiding conflicts arising from competing logics and related contradictions regarding safety and security. An example of contradictory logics between safety and security management is that management of safety relies on openness and transparency, whereas the management of security requires the concealment of data and sharing it only between the trusted community of security experts. Reconciling these contradictory aspects requires coordination. It is of paramount importance not to improve safety at the cost of security and vice versa. An example of contradictory requirements of safety and security can be taken from the nuclear industry context, where during the outages, safety critical components should be marked clearly to ensure nobody mistakenly touches them. From the security perspective, however, this practice is not supported, as it would expediate a potential perpetrator's recognition of the relevant targets. Thus, promoting safety and security in a high-risk industry requires understanding the contradictory logics of safety and security, and this calls for IMSS.

Still another incentive for IMSS 3) relates to economic reasons, namely cost-efficiency measures, such as a reduction of administration and audit costs when combining management of safety and security. In addition, cost benefits are achieved, e.g., when investing in protection measures that are suitable for both safety and security domains (Kriaa et al. 2015; Reniers et al. 2011: Reniers and Amyotte 2012). For instance, using cameras to observe both safety and physical security risks is an example of cost-benefits and synergies obtained from the IMSS.

Furthermore, a strong justification for IMSS is the fact that 4) pure safety or pure security approaches cannot identify and mitigate systemic risks or risks to the industrial automation and control systems (Boyes et al. 2018; Schulman 2020; Young and Leveson 2014; Kriaa et al. 2015; Reniers et al. 2014). Similarly, traditional safety and reliability approaches have not included cybersecurity risks. Therefore, IMSS is required to identify, assess, and mitigate the convergence of different safety and security risks.

Identified motivations act as drivers and incentives for IMSS. However, the relationship between motivation and action or practice is not straightforward. but mediated by cultural factors, which include attitudinal and cognitive components, and material aspects, such as competences and available resources. Therefore, in addition to an examination of the motivations, the current state and practices regarding the IMSS is also good worth reflecting on.

4.2. The current state of IMSS in Seveso sites

We examined the current state of IMSS based on the structural, functional and cultural aspects of integration (Jørgensen et al. 2006). The Responsible Care code – an initiative for the global chemical industry to enhance continuous improvement in safe chemicals management (International Council of Chemicals Associations (ICCA)) – represents structural aspects and was adopted by companies participating in interviews. The Responsible Care code and the Environment, Health, Safety, and Security (EHS&S) management system represent structural integration in the sense that they integrate elements from different environment, safety, and security standards (Fig. 3). In addition, Seveso establishments also have special organisational units or teams focused on EHS&S, which represent functional integration. EHS&S provides a procedure and framework for evaluation and measurement of safety and security management. Furthermore, incident report systems that combine both safety and security incidents into the same system represent functional integration.

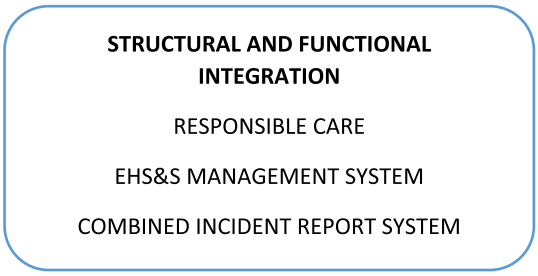

Fig. 3. Indications of structural and functional integration.

Structural integration is deficient in the sense that cybersecurity is handled by a separate IT unit, and as is sometimes the case for multinational corporations, the IT unit may be located at headquarters abroad. These kinds of organisational structures easily create silos, which hamper the efficient flow of information between the organisational units. Furthermore, security threat analysis and process-safety analysis are often undertaken independently, which prevents obtainment of an adequate understanding of systemic risks, let alone the possibility to address such systemic risks.

With regard to the exchange of information, some promising developments were mentioned. For instance, in Seveso establishments, IT experts are involved in discussions about process-safety and process-automation issues. Even though some form of cooperation thus exists among the process-safety, IT, and EHS&S units, the question remains whether this is sufficient in terms of duration and frequency to address systemic risks and build and co-construct knowledge of the safety-security interface.

Although the interviews did not provide us with an adequate information about the status of cultural integration, which is the deepest level of integration, signifying a shared understanding and values regarding the relevance of IMSS in organisations, our interpretation is that an adequate structural and functional integration requires embeddedness in cultural values and beliefs. Thus, the different levels of integrated management (structural, functional, and cultural) are intertwined.

In addition, there were separate developments, such as the development of methods for security vulnerability analysis and separate audits for process-safety. These separate developments are also essential, as a special understanding of safety and security domains needs to be maintained and developed, even in the context of integration.

4.2.1. Lack of institutional standards for IMSS

The institutional framework of IMSS is lacking both in terms of international standards and the Seveso directive. The latter requires that Seveso establishments, of which there are over 12 000 in the European Union, will take measures to prevent major accidents from happening (Seveso III Directive). However, the Seveso Directive does not explicitly demand IMSS. Nevertheless, one could argue whether this is necessary since there is a generic requirement in the Sevoso III Directive to identify and mitigate risks by using a safety management system and making a safety (study) report that must include cybersecurity risks since they present a potential danger (Annex III art. 12 and 15; Sevoso III:2012/18/EU). Moreover, as can be observed with new EU legislation proposals like the Artificial Intelligence Act and the Machine Regulation, legislators could suffice by simply referring to the NIS Directive for assessment and mitigation of cybersecurity risks and/ or existing best practice standards in this area, such as 'IEC 62443: Cyber security for Industrial Automation and Control Systems' to comply with the target requirements (goal prescriptions) formulated in the legislation. This still does not, however, solve the issue of how exactly to integrate both disciplines in practice.

Currently there are no management standards that would require the integration of process-safety, physical security, and cyber-security management. The lack of structural and institutional support for IMSS at the international and national level means that development of IMSS will be on the shoulders of companies themselves, and therefore the progress of IMSS can be slow and uneven. Thus, although the IMSS has currently taken steps forward, it seems to be still in its infancy.

Next, we will look at the possible sociotechnical tools that could enhance both the practical implementation of the coordinated management of safety and security as well as better communication between these domains.

4.3. Management system for the IMSS

From the structural integration perspective, the management system constitutes a key tool for IMSS. A management system signifies the way in which organisations control the interrelated parts of its business in order to gain its objectives, such as process-safety, cybersecurity and physical security. The International Organization for Standardization (ISO) has exploited a common high-level structure to enable the integration of different management standards. The ISO high-level structure provides a useful tool for designing and implementing IMSS. The covered aspects of the management system include a) recognition of the context of organisation; b) leadership; c) planning; d) support; e) operation; f) performance evaluation and g) improvement. The aforementioned implements the classical performance management cycle of plan-act-monitor-review, aiming at a continuous improvement process.

The goal for integration is to *connect, coordinate, and combine safety and security management activities in order to exploit synergies and to resolve conflicts between them.* Tools refer also to the functional level, i.e., how different functions of safety and security management could be combined. Examples include risk identification, risk assessment, incident reporting and emergency management. Furthermore, practical guidelines regarding IMSS were created during this study (Heikkilä et al. 2021). For instance, the following aspects regarding integration were suggested: Allocate resources equally for safety and security; utilise synergies; allocate resources also for tasks required to establish integration; ensure required safety and security competence; improve cross-disciplinary understanding between different safety and security actors, etc. (Heikkilä et al. 2021). Below, we open up some practical measures in terms of IMSS in a multi-plant context and then deal with some integrated risk identification and risk assessment tools.

4.4. Practical measures for integrated management in a multi-plant context

Seveso plants are located in large industrial areas, such as industrial parks, with several other plants nearby. In many cases, they share joint utilities (e.g., electricity, steam water, gases), the import or export of raw materials, and products. The possibility of convergent safety and security risks grow because of this, thus IMSS becomes a more urgent topic to be considered (Reniers et al. 2014). Similarly, an increase in outsourcing, and consequent growth, in the many-tier supply-chain makes IMSS crucial between the Seveso companies and their vendors and suppliers. At the same time, IMSS is more challenging in a multi-plant context, due to the different goals, strategies, and cultures the companies have, not to mention the challenges regarding sharing costs (Reniers et al. 2014). Based on the interviews and literature, we identified some practical measures that could be taken to promote IMSS in a multi-plant context.

The list of measures is not exhausted. Some items from the list are already in use in industrial areas or industrial parks, but there is also room for improvement. In the multi-plant context, it is important to understand the risks that other chemical installations in the same area may cause, as installations can be linked in terms of the danger and threat they pose to each other. Often a small fracture of events may cause dramatic impacts. This is called power-law distribution (Reniers et al. 2014). Without knowing the power-law distribution, it is not possible to deal with systemic risks. The list of synergies below provides

ideas concerning potential ways of collaborating in a multi-plant context.

IMSS in a multi-plant context

- Common guarding
- Common emergency exercises
- Common fire brigade
- Common incident reporting system
- Integrated incident analysis
- Integrated risk identification and assessment
- Common safety and security culture
- Common understanding of risks and possible impacts that neighbouring
- organisations may have on your company and vice versa
- Inspectors from different safety and security domains could carry out inspections jointly

IMSS could be realised in a multi-plant context by integrating safety and security risk identifications and assessments, as one of the most relevant things would be to gain a common understanding of the risks and possible impacts that the other organisations in the same area may have on the company. In addition, a common incident reporting system could be created, and incident analysis could be conducted in an integrated way. This could also contribute to a better understanding of mutual implications. Furthermore, emergency plans and exercises could be designed to encompass both safety and security aspects. Furthermore, a shared safety and security culture could be enhanced. In addition, inspectors could also enhance IMSS by organising joint inspections and feedback meetings with the companies located in the same area. Based on our interviews, common guarding and emergency exercises were already in use in Seveso plants, but integrated risk identification was not commonly used.

5. Findings regarding past incident analysis and tools for identifying and assessing risks

This section deals with the main findings regarding past incident analysis and integrated risk identification and assessment. Both factors were identified in section 4.3 as key elements in IMSS. Different risk identification and risk assessment tools suitable for contributing to IMSS will be examined, as the risk assessment and risk management will be the functions of the organisations that play a core role in handling convergent risks. Finally, some countermeasures for convergent risks are discussed.

5.1. Past incident analysis and the main risk scenarios

Past incident analysis focused on 82 cyber-security induced events in the chemical industry and similar sectors occurring worldwide over the last 50 years (Iaiani et al. 2021b). Cyber-attacks have most frequently targeted cyber-systems with common consequence such as data theft, system blockage, malfunctions, etc. However, cyber-attacks to the Basic Process Control System (BPCS) and the Safety Instrumented System (SIS) of process facilities have the potential for major consequences on humans, assets, and the environment, which are comparable to those caused by safety-related causes (Landucci and Reniers 2019). The analysis provided historical evidence of these cases concerning the pipeline transport of hydrocarbons; however, the dynamics of these events (induced system pressurisation, deactivation of alarms, etc.) is also deemed credible in process plants (Iaiani et al. 2021b). The results (Fig. 4) evidenced that petrochemical installations are the most affected by cyber-attacks, with at least 15 incidents that affected the OT system of the facility.

Past incident analysis (Fig. 4) shows that cyber-security risk management and IMSS would need to pay attention to three main classes of cybersecurity-related events: a) an attack on the IT system and compromising sensitive data/information; b) an attack on the OT system leading to loss of production (e.g., production shutdown or product out of specification); c) an attack infecting the OT system aimed at generating a major event. The historical evidence of OT infections leads to major events and further stresses the need for the integration of safety and security [as pointed out in section 4.1 the literature review (i.e., "Safety and security have mutual interactions and influences").

Attacks on the IT system aimed at compromising sensitive data/information concern the "traditional" object of cyber-security management, which is common to any computer network, regardless of whether it belongs to a Seveso installation. These aspects of cyber-security are usually managed with the best practices of information security management, such as those provided by the ISO/IEC 27000 series of standards (International Organization for Standardization (ISO),

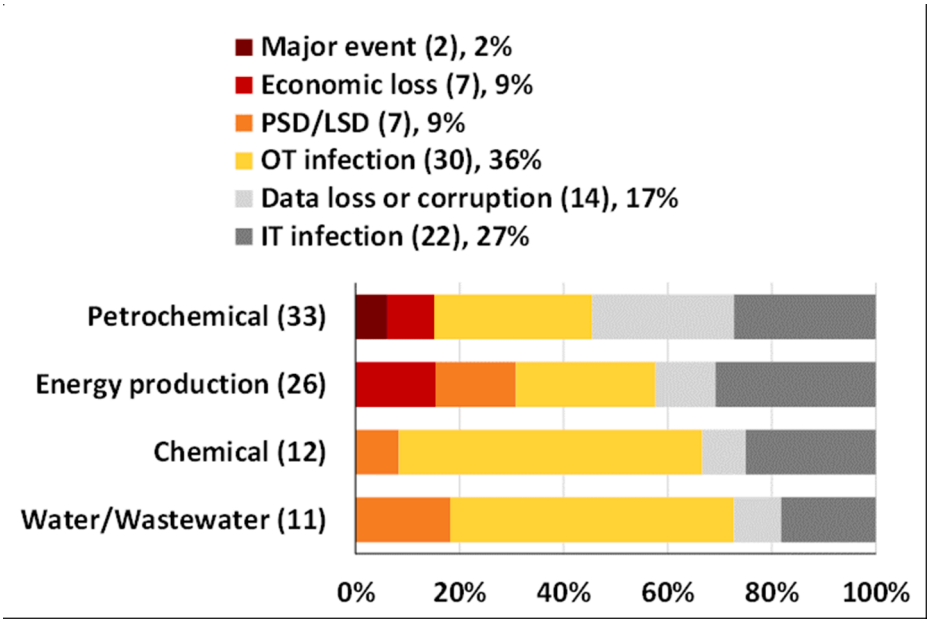

Fig. 4. Results from past incident analysis: share of impacts concerning recorded cybersecurity-related incidents vs. the industrial sectors. adapted from Iaiani et al. 2021b

International Electrotechnical Commission (IEC), 2018).

Attacks on the OT system aimed at loss of production require an assessment specific to the OT system, such as the one addressed by the ISA/IEC 62443 series of standards for Industrial Automation and Control Systems (IACS) (International Society of Automation (ISA), International Electrotechnical Commission (IEC), 2018). In particular, these standards require the evaluation of all the impacts (including those on the physical process plant) that can result from intentionally malicious attacks on the OT system in order to evaluate a facility's actual level of cyber risk and implement proper cybersecurity countermeasures for its reduction. These standards are quite scant in providing support to the identification of adverse outcomes. Literature examples of methods that support this assessment usually rely on semi-quantitative matrix or scoring approaches [ISA/IEC 62443]. More sophisticated approaches include cyber Bow-Tie approaches (Abdo et al. 2018), cyber Process Hazard Analysis approaches (Cusimano and Rostick 2018), HAZOP-like approaches for attacks to BPCS and SIS (Iaiani et al. 2021d), and cause-effect matrix approaches (Hashimoto et al. 2013).

OT infections leading to major events are the ones for which the greater benefit is expected from integration of management systems. Major events characterisation and modelling traditionally belong to the expertise area of safety management (Mannan 2012). Methods and tools used for the prediction of expected consequences (i.e., physical effect modelling for major accident scenarios, damage models, calculation of risk indexes) developed in the context of safety risk analysis are directly applicable to the major events induced by malicious attacks. However, the identification of the potential major events (i.e., characterisation of the accident scenario in terms of mode of loss of containment, operating conditions before release, inventory released, etc.) cannot be achieved with identification techniques as normally used in the safety domain (e.g., HAZOP, Process Hazard Analysis, PHA, Failure Modes, Effects and Criticality Analysis, FMECA, Fault Tree Analysis, FTA, Human Error Identification Techniques, HEI, etc.), since they focus on events originating from random failures or human error.

5.2. Integrated risk identification and assessment tools

As pointed out in previous sections, IMSS requires an increased share of knowledge among the disciplines, especially in terms of the identification of risks, which is a starting point for any risk management system (International Organization for Standardization (ISO), 2018). However, the weakness is that the major scenario identification falls outside of the current practice of Security and Cyber-Risk Assessment (Matteini et al. 2019). As a result, simplified assumptions are frequently adopted, e.g., considering, in the security risk assessment, the worst-case consequences from the safety assessments, even though the cyber-attacks have the potential for consequences different from those considered in the safety study (e.g., some abnormal states of the plant cannot be induced through the BPCS and the SIS).

Past event analysis, although important to pinpointing the credibility of potential scenarios, is not suitable for the evaluation of expected scenarios originating in specific plants, as the low number of recorded events does not allow one to correlate them with all the relevant factors describing real situations (e.g., system design, materials and operating conditions, interdependencies in the physical and cyber system).

For the identification of various process-safety, physical security, and cybersecurity risks in an integrated way, the structured approaches, such as Hazard and Operability Analysis (HAZOP), can be used as a reference (see Chockalingam et al. 2016). Basic implementation would require that both a physical- and cyber security expert shall be included in the HAZOP team to ensure that the security-related inputs are integrated into the same HAZOP analysis. While the HAZOP technique is qualitative and aims to stimulate the imagination of participants to identify potential hazards and operability problems, the inclusion of security aspects is unsupported by commonly used guidewords. Nevertheless, promising examples about the security applications of HAZOP (Wei et al. 2016) and other process hazard analysis methods (Marszal and McGlone, 2019) are available.

The main criticism of the direct use of HAZOP may originate from the current practice of its application, which does not take into account external and non-random causes or sources of risks. Moreover, HAZOP and process hazard risk analysis (PHR), usually disregard multiple failures (i.e., several dangerous events occurring at once) (CCPS 2008), although this is possible with respect to cyber-attacks or physical attacks.

Joint risk assessments for safety and security could include shared identification of both security threats and major accident scenarios, joint risk evaluation including both aspects, and means of prevention and preparedness affecting both safety and security. Only minor changes for traditional ways of working may be required.

There are several examples combining safety and security risk assessments (Chockalingam et al. 2017; Kavallieratos et al. 2020; Langner 2013). In addition, specific dynamic and systemic risk assessment methods for the integration of safety and security risks have been developed. These include, for example, STPA-SEC (System-Theoretic Process Analysis for Security), which is a top-down safety hazard analysis method, based on systems theory, especially aimed at safety–critical cyber-physical systems. STPA-SEC has also been extended to include security analyses (Schmittner et al. 2016; Friedberg et al. 2017; Pereira et al. 2017; Sabaliauskaite et al. 2018). These extended STPA methods have been applied especially to cyber-security issues.

Whether the practical application of some tools that combine safety and security risk assessment leads to simultaneous or sequential identification (e.g., first security risks are independently identified and then they are used as inputs to safety risk identifications (see Chockalingam et al. 2017)) is still an open question. Sequential identification has the potential to miss cross-impacts of safety risks on security risks and the other way around.

HSE has published guidelines in an Operational Guidance (HSE OG86) for Inspection Cyber Security for Industrial Automation and Control Systems on major accidents in the workplaces. Self-assessment checklists to address the major cyber-attack avenues for protecting ICS are also available. These aid in identifying the most common potential threat scenarios and known countermeasures.

5.3. PHAROS methodology

A systematic and formally rigorous methodology, PHAROS (Process Hazard Analysis of Remote manipulations through the cOntrol System), was developed within the framework of the SAF€RA 4STER project (Iaiani et al., 2021c) in order to identify scenarios that can potentially originate from malicious manipulations, which may lead to major events. PHAROS exploits a HAZOP-like approach. The analysis is carried out by a team of experts (process experts, plant system experts, control experts, loss prevention system experts, security experts). The method supports identification of i) the specific set of manipulations of the BPCS and the SIS, which may lead to major events; ii) the protection requirements for the safeguards in place; iii) and the design of the network system segmentation (division into zones and conduits) as suggested by ISA/IEC 62443. Application of PHAROS consists of nine steps presented in Fig. 5 and discussed by Iaiani et al. 2021c.

Within PHAROS, attackers aiming to generate a Security Event (SE, e.g., release or other major event) are assumed to exploit a physical Mechanism of Actions within the plant (MAs, e.g., cause internal overpressure). The cyber-attacker can cause MAs only by Remote Manipulations (RMs, e.g., setpoint change) of the Manipulative Elements connected to the OT system (MEs, e.g., controllers and their logics). These RMs result in Local Consequences (LCs, e.g., closing/opening) on the Remotely Manipulable Components (RMCs, e.g., automatic valves, pumps, compressors) of the physical plant, which together originate the MA. The procedure goes through the systematic identification, based on a review of process documentation, of the chain leading from remote

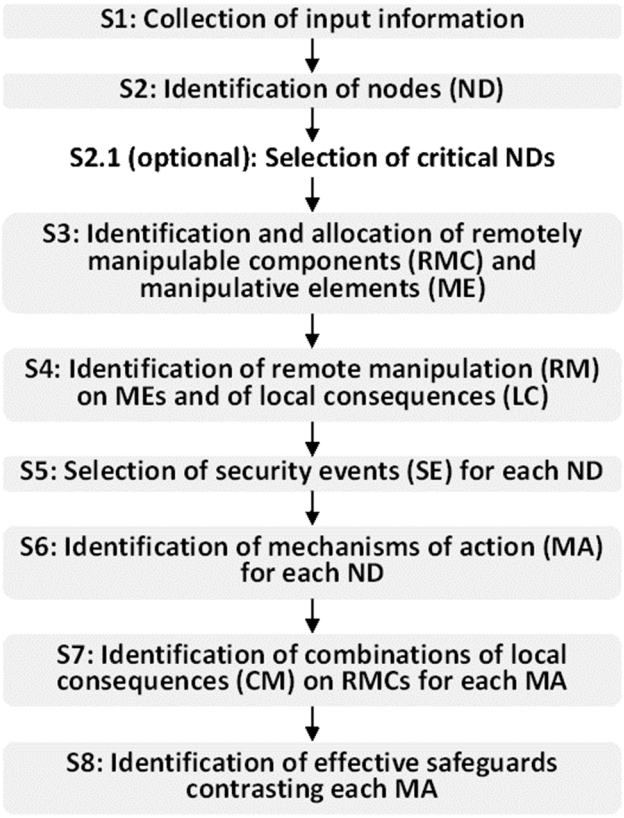

Fig. 5. Flowchart of PHAROS.

manipulations to the security event for each node in the process. Inherent/Passive safeguards (IPSs, e.g., PSVs) and the Active/Procedural (APSs, e.g., PSD activation logics) safeguards present in the system for safety purposes play a role in the possibility to generate MAs and therefore must be identified and carefully taken into consideration. This may help to identify better design specifications for the barriers (e.g., matching the requirements from physical scenarios deriving from the attack).

The PHAROS procedure is an example of the integration of safety and security expertise in the management of risk, as it applies a systematic risk identification procedure typical of safety (i.e., HAZOP-like analysis) to the domain of cyber-security threats to physical process systems. The use of a similar approach in the field of security and safety promotes the diffusion of a "common language" between the two disciplines, establishing an effective interdisciplinary communication and understanding and yielding a more integrated management of safety and security risks. Shared understandings and effective communication provide the necessary common ground for jointly asking and answering questions across disciplinary boundaries (Gilligan 2021). This is of particular relevance, since potential conflicts or inconsistences between requirements defined in isolation by the safety and security assessment are avoided, and since it may allow the recognition of risks which could otherwise be overlooked (e.g., those deemed unlikely in the safety assessment or out of the scope in the security assessment) (Ji et al. 2021; Leveson 1995; Pietre-Cambacedes and Bouissou 2013; Sørby 2003).

5.4. Countermeasures

This subsection investigates possible countermeasures applied to deal with cyber-attacks in the context of Seveso plants. In the literature, there are some countermeasures developed to deal with cyber-attacks to OT systems and detecting anomalies. However, these tools are currently not in common practice in the Seveso plants. They are meant to complement and further advance the current best practice in the protection of IT/OT networks, based on countermeasures like network segmentation, firewalls, authentication systems, patch management, etc. Nevertheless, these countermeasures are worth of presenting and reflecting on, as they provide relevant sociotechnical tools to deal with the challenges that digitalisation and the safety-security interfaces may create. In line with this view, the following countermeasures can ideally contribute to raising the resilience in IMSS.

5.4.1. Agent-based impact simulation

In the context of critical infrastructure protection (CIP) the effect of a malfunction can be evaluated via *domino effect models*, either with a high level of abstraction (Haimes et al. 2005; Yu et al. 2020), a fine-grained analysis (De Porcellinis et al. 2008; Rosato et al. 2008; Marti et al. 2008; Yang and Marti 2022) or a combination of the two (Oliva et al. 2010) in order to provide meaningful insights on the near-future situation affecting neighbouring infrastructures in a reasonable time and with an adjustable level of detail.

These approaches could be mimicked from the CIP domain for the evaluation/quantification of the impact of a cyber-attack on workers' safety. For instance, an agent-based simulation model featuring the main components and subsystems of a plant, as well as the workers and neighbouring infrastructures, could be set up to assess the near future effect of a successful cyber-attack able to affect the physical processes (e.g., releasing refrigeration ammonia into the environment). In addition, knowledge of the impact scenarios could help in devising adequate and specific mitigation actions.

5.4.2. Machine learning approaches to detecting traffic anomalies tailored to the OT case

The most well-established approaches to actively enforcing security from a cyber point of view include Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) (Ding et al. 2018). Recently, approaches based on artificial intelligence and machine learning have proved their effectiveness in detecting attacks (Ghosh and Sampalli 2019; Kunal and Dua 2019; Almseidin et al. 2017; Vinayakumar et al. 2019; Anton et al. 2018).

Notably, to effectively detect cyber anomalies, such algorithms require the availability of training datasets. Although most of such datasets are not specific to the OT domain (Özgür and Erdem 2016; Tavallaee et al. 2009; Moustafa and Slay 2015; Garcia et al. 2014), datasets including actual traffic for OT and ICS systems have been developed and released in recent years (Goh et al. 2017; Laso et al. 2017; Faramondi et al. 2021).

5.4.3. Leveraging on the process dynamics

Cyber anomalies are typically detected by looking at anomalous traffic in a communication network, without inspecting the message payload (i.e., the information content). However, the actual readings from sensors and the commands sent to actuators, together with knowledge of the dynamics of the process, can be exploited to spot anomalies that entail the physical process, even when no apparent cyber anomaly can be identified. The main idea of such methods is that, since the process often has a known dynamic, formally correct messages could still be unexpected or anomalous, based on the expected or foreseen working condition of the plant. For instance, if a tank is emptying, a raise in the water level (or too slow a decrease) can be flagged as suspect even if the message received is well formed and appears legitimate from the cyber point of view. This class of methodologies typically rely on a *digital twin* of the process (Tao et al. 2018), i.e., a piece of software able to simulate the expected dynamics of the process, and on decision techniques borrowed from the domain of fault detection (Miciolino et al. 2017; Nicolaou et al. 2018), where an alarm is raised if the discrepancy between the sensorial measurements and the ones expected based on the digital twin are too large.

6. Discussion and conclusion

The novelty of this research is the collective, multidisciplinary findings that illuminate the current state of IMSS from complementary perspectives. These include i) motivations for IMSS, ii) the current practices of IMSS in a single plant and multi-plant context, iii) institutional support for IMSS, iv) past incident analysis showing what types of cyber-security induced events Seveso sites should pay attention to, v) some risk identification and assessment tools, and their suitability for identifying systemic risks, vi) new Pharos method for the identification of scenarios originating from malicious manipulations of the BPCS and the SIS and vii) countermeasures to deal with the cyber-attacks on OT systems. Table 2 summarises the main results of the study and our interpretations of the industry responses and the current state of IMSS.

The sociotechnical approach in this study refers to the interconnectedness and complexity of social (including organisational) and technical systems. It allows us to get a more comprehensive picture of IMSS and to see the links between the external environment (institutional support to IMSS), the organizational (management, expertise, practices), and the technical (available risk assessment tools) aspects. The sociotechnical approach was complemented by an integrated management perspective that incorporates structural, functional and cultural dimensions.

The relevance of IMSS has been addressed by several safety, security and risk studies (Chen et al. 2022; Reniers and Khakzad 2017; Reniers et al. 2014; Harvey and Stanton 2014). Furthermore, the literature on

Table 2
Summary of the main results of the study.

Main results of the study	Related comments
Motivations for developing IMSS based on literature review • Safety and security have mutual interactions and influences • Avoiding conflicts arising from competing goals and logics and related contradictions • Economic reasons: cost-efficiency • Risks: pure safety or pure security approaches cannot identify systemic risks and risks to the IACS	The motivations for developing IMSS are closely related to the understanding of systemic risks. Interviews showed that the current risk identification practices do not help in understanding systemic risks. Thus, the motivations for the IMSS are also underdeveloped in Seveso companies.
Current practices of IMSS based on interviews • Cybersecurity is handled by a separate IT unit • Security threat analysis and process-safety analysis are often undertaken independently • Responsible Care & EHS Management system • Combined Incident Report System • Common Emergency Exercises	The structural and functional arrangements of the Seveso companies (separate IT unit, separate risk analyses in safety and security domains) easily create silos and make it difficult to identify and manage systemic risks efficiently.However, positive developments are under way, such as the combined incident report system and joint emergency exercises combining safety, cyber-security and physical security risks.
IMSS in a multi-plant context • Common guarding • Common emergency exercises • Common fire brigade • Common incident reporting system • Inspectors from different safety and security domains carry out inspections jointly • Common understanding of risks and possible impacts that neighbouring organisations may have on your company and vice versa • Integrated incident analysis • Integrated risk identification and assessment • Common safety and security culture	Common guarding, joint emergency exercises, common fire brigade, joint inspections carried out by different inspectors are in use in industrial parks. In addition, efforts are made to reach an understanding of the potential risks and impacts that neighbouring organisations may have on each other. At present, however, risk identification and assessment practices are not adequately integrated in the context of a single company or multi-plants.
Past incident analysis shows that IMSS would need to pay attention to the following cybersecurity-related events: a) an attack on the IT system and compromising sensitive data/information; b) an attack on the OT system leading to loss of production (e.g., production shutdown); c) an attack infecting the OT system aimed at generating a major event	Often used risk identification techniques in safety domains (HAZOP, Process Hazard Analysis, PHA, Failure Modes, Effects and Criticality Analysis, FMECA, Fault Tree Analysis, FTA) are insufficient to identify attacks on the OT system. The above mentioned techniques focus on events caused by random failures or human error, not events caused by intentional acts.
Integrated risk identification and assessment tools There are several examples combining safety and security risk assessments. (Chockalingam et al. 2017; Kavallieratos et al. 2020; Langner 2013). In addition, specific dynamic and systemic risk assessment methods for the integration of safety and security risks have been developed, such as STPA-SEC (System-Theoretic Process Analysis for Security). It is a top-down safety hazard analysis method, based on systems theory, especially aimed at safety–critical cyber-physical systems.	Seveso companies often rely on separate tools to identify cyber-security, process-safety and physical security risks. The major scenario identification falls outside of the current practice of Security and Cyber-Risk Assessment (Matteini et al. 2019). As a result, simplified assumptions are frequently adopted, e.g., considering, in the security risk assessment, the worst-case consequences from the safety assessments, even though the cyber-attacks have the potential for consequences different from those considered in the safety study.
PHAROS (Process Hazard Analysis of Remote manipulations through the cOntrol System) was developed in the project to identify scenarios that can potentially originate from malicious manipulations of the BPCS and the SIS, which may lead to major events (Iaiani et al., 2021c). PHAROS exploits a HAZOP-like approach. The analysis is carried out by a team of experts (process experts, plant system experts, control experts, loss prevention system experts, security experts).	PHAROS method was developed during this study and has not yet been tested in practice. PHAROS is a promising method, as it promotes the diffusion of a "common language" between the two disciplines, establishing an effective interdisciplinary communication and understanding and yielding a more integrated management of safety and security risks.
Countermeasures developed to deal with cyber-attacks to OT systems and detecting anomalies. Agent-based impact simulation (*domino effect models),* Machine learning approaches to detecting traffic anomalies tailored to the OT case (*Intrusion Detection Systems, Intrusion Prevention Systems (IPS)),* Leveraging on the process dynamics. Sensors can be exploited to spot anomalies that entail the physical process, even when no apparent cyber anomaly can be identified. methodologies typically rely on a *digital twin* of the process.	These tools are not currently widely used at Seveso plants.
Institutional support for IMSS is weak. IMSS is not required or supported by laws or the Seveso Directive.	Weak institutional support means that the development of IMSS is up to the Seveso companies themselves. This leads to uneven development between the Seveso companies and EU-countries.

safety, security and risks provides several motivations to apply IMSS, such as better understanding and identification of systemic risks (regarding the mutual interactions and influences between safety and security), since pure safety or pure security approaches are not sufficient to identify or mitigate them. Other motivations for integration are avoidance of conflicts related to competing goals of separate safety and security management approaches and establishing better cost efficiency.

The motivations for developing IMSS are closely linked to the understanding of systemic risks. Motivations were not asked directly in the interviews. Nevertheless, the interviews of Seveso companies showed that the current risk identification practices do not help in understanding systemic risks. From this perspective, the motivations for IMSS are underdeveloped in Seveso companies.

The positive aspects that our study showed were some examples of current practices that are in line with the IMSS, e.g., a design of common emergency exercises that include cyber-security and process-safety aspects, or an incident report system that integrates both safety and security incidents into the same system. In addition, in a multi-plant context, common guarding/fire brigade and joint inspections by different safety and security inspectors were rather common. In contrast, the interviews did not provide any indication of the creation of a common safety and security culture in which the IMSS could be rooted. In addition, the EHS management system in Seveso sites provides a model for integration of different safety and security areas. However, it does not automatically support IMSS by including process-safety, physical security and cyber-security aspects into the same management system.

Regarding current IMSS practices, our interviews with the safety and security experts at Seveso plants revealed two clear deficiencies. Firstly, there is an evident gap, especially between cybersecurity management and process-safety management. Cybersecurity is often managed by a separate IT unit that can even be located in another country. This makes it difficult to obtain an adequate collaboration and co-construction of knowledge about process-safety and cybersecurity interfaces. Another deficiency refers to that security threat analysis and process-safety analysis are often undertaken independently. Even though there are several examples combining safety and security risk assessments (Chockalingam et al. 2017; Kavallieratos et al. 2020; Langner 2013), such as STPA-SEC (System-Theoretic Process Analysis for Security), Seveso companies rely often on separate cyber-security, process-safety and physical security risk identification tools. Separate risk identifications and analyses in the safety and security domains easily create silos and hamper possibilities to address and manage systemic risks.

Our study of past incident analysis shows that IMSS would need to pay attention to three main classes of cybersecurity-related events: a) an attack on the IT system, compromising sensitive data/information; b) an attack on the OT system leading to loss of production (e.g., production shutdown or product out of specification); and c) an attack infecting the OT system aimed at generating a major event. However, often used risk identification techniques in safety domains (HAZOP, Process Hazard Analysis, PHA, Failure Modes, Effects and Criticality Analysis, FMECA, Fault Tree Analysis, etc.) are not suitable to identify the potential major events or attacks on the OT system. The aforementioned techniques focus on events originating from random failures or human error, but not events originating from intentional acts.

In addition, the major scenario identification falls outside of the current practice of Security and Cyber-Risk Assessment (Matteini et al. 2019). As a result, simplified assumptions are frequently adopted, e.g., considering, in the security risk assessment, the worst-case consequences from the safety assessments, even though the cyber-attacks have the potential for consequences different from those considered in the safety study.

In terms of organizational factors, not only the distance between the organisational units hinders the internal collaboration within Seveso plants, but also the influence of different subcultures between process-safety, EHS&S, and cybersecurity units. In addition, there are different experts (safety and cyber-security) with different disciplines (technical and social science expertise) and differing concepts that may make the exchange of information and flow of communication between the experts and units challenging. These experts can use similar terms, which may have different connotations in their respective fields, or different terms and definitions that others do not understand. These differences in disciplinary background and conceptual frameworks create challenges with regard to the efficient exchange of information and flow of communication.

Becoming familiar with each other's terminology and thinking as well as establishing trustworthy relationships between different experts would require time and permanent forums. In this context, the **PHAROS** (Process Hazard Analysis of Remote manipulations through the cOntrol System) method represents an ideal, sociotechnical tool. PHAROS was developed in this project to identify scenarios that can potentially originate from malicious manipulations, which may lead to major events (Iaiani et al., 2021c). PHAROS exploits a HAZOP-like approach. The analysis is carried out by a team of experts (process experts, plant system experts, control experts, loss prevention system experts, security experts). In this sense PHAROS contributes to IMSS, as it supports collaboration between different safety and security experts. Furthermore, PHAROS allows for the recognition of risks that could otherwise be disregarded, e.g., risks that could be deemed unlikely in the safety assessment or out of its scope. As Pharos is a new method, it has not yet been used or tested in practice.

There are also promising techniques and countermeasures (e.g., Critical Infrastructure Protection) developed to handle cyber-attacks to OT systems that could be adapted to IMSS; for instance, agent-based impact simulation or machine learning approaches to detecting traffic anomalies tailored to the OT case. However, the path for a concrete adoption of these techniques in the context of IMSS is still underway.

An important element in supporting the development of IMSS is an institutional set-up, which, however, is missing. There are no international standards that require and adequately support IMSS. Moreover, not even the Seveso III Directive demands IMSS. This means that the development of IMSS rests on the shoulders of single Seveso companies for now, and therefore the progress of IMSS can be slow and uneven between companies and EU countries.

Based on our analysis, we argue that IMSS is still in its infancy at Seveso sites, although there are indications that IMSS is evolving. This study revealed sociotechnical factors and gaps in the understanding and motivations of IMSS, inadequate risk identification and analysis tools and practices related to systemic risks, and a lack of institutional support for IMSS. Together, these factors constrain the development of IMSS.

Thus, the development of IMSS at Seveso sites should be further improved. This would require the introduction of new risk identification methods, better integration of the identification of process-safety, cybersecurity and physical security risks and the co-assessment of these risks. In addition, one should think beyond the current disciplinary boundaries. This would require permanent forums where different experts can communicate together and co-construct a better understanding of convergent risks (Heikkilä et al. 2021). Furthermore, the use of tools developed, such as PHAROS, which supports collaboration between different experts, would be crucial for IMSS. In addition, organisational roles and responsibilities would require new definitions. New jobs and tasks could be defined as requiring several areas of expertise. This would be a way to enhance expert collaboration. Only in this way will a better understanding of the emerging risks and the motivation for IMSS be obtained. In addition, institutional support for the IMSS would be necessary.

This study is not a final word regarding the IMSS, but it provides relevant insights. The future research on IMSS could include studies on:

- integrated safety and security risk identification using new methodologies (STPA-SEC) or adapting existing ones like HAZOP;

- adoption of the Pharos method as developed in the current study and its effects on the exchange of information and knowledge between different safety and security experts in Seveso sites;
- the integrated management of safety and security cultures
- evolving institutional set-up regarding IMSS
- the relationships between motivation, understanding and practices in terms of IMSS
- comparative study of IMSS in multi-plant contexts
- organizational boundaries, roles and responsibilities contributing to or constraining of IMSS

In addition, comparative studies between the countries and companies in terms of the state of IMSS would be relevant.

CRediT authorship contribution statement

Marja Ylönen: Conceptualization, Writing – original draft. **Alessandro Tugnoli:** Writing – original draft. **Gabriele Oliva:** Writing – original draft. **Jouko Heikkilä:** Writing – review & editing, Writing – original draft, Visualization. **Minna Nissilä:** Writing – review & editing. **Matteo Iaiani:** Writing – original draft. **Valerio Cozzani:** Writing – review & editing. **Roberto Setola:** Writing – review & editing. **Giacomo Assenza:** Investigation. **Dolf van der Beek:** Writing – review & editing. **Wouter Steijn:** Writing – review & editing. **Nadezhda Gotcheva:** Writing – review & editing. **Ernesto Del Prete:** Writing – review & editing.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

We are grateful for valuable comments and suggestions from three reviewers.

This research has been made possible thanks to the support of the SAF€RA, which is a partnership between 16 research funding organisations from 12 European countries who collaborate on research programming and launch joint calls in the field of industrial safety. More information about this project can be found here: Integrated Management of Safety and Security Synergies in Seveso Plants (SAF€RA 4STER) | SAF€RA (safera.eu)

We are grateful for the support of the Finnish Chemicals and Safety Agency (TUKES), the Finnish Working Environment Fund (FWEF), the National Institute for Insurance against Accidents at Work, Italy (INAIL), and the Ministry of Social Affairs and Employment (SZW) in the Netherlands.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

This research was supported by the Finnish Working Environment Fund (FWEF), the Finnish Chemicals and Safety Agency (TUKES), the National Institute for Insurance against Accidents at Work, Italy (INAIL) and the Dutch Ministry of Social Affairs and Employment (SZW) [Occupational Safety Research Program 2019/2020].

References

Abdo, H., Kaouk, M., Flaus, J.M., Masse, F., 2018. A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie – combining new version of attack tree with bowtie analysis. Computers Security 72, 175–195. https://doi.org/10.1016/j.cose.2017.09.004.

Almseidin,M., Alzubi,M., Kovacs, S., Alkasassbeh, M., 2017. Evaluation of machine learning algorithms for intrusion detection system. In: Proceedings SISY 2017 - IEEE 15th International Symposium on Intelligent Systems and Informatics pp. 000277–000282. https://dx.doi.org/10.1109/SISY.2017.8080566.

Anton, S.D., Kanoor, S., Fraunholz, D., Schotten, H.D., 2018. Evaluation of machine learning-based anomaly detection algorithms on an industrial Modbus/TCP data set. In: ARES 2018: Proceedings of the 13th International Conference on Availability, Reliability and Security, Article No. 41, pp. 1–9. https://doi.org/10.1145/3230833.3232818.

Aven, T., Ylönen, M., 2019. The strong power of standards in the safety and risk fields: A threat to proper developments of these fields? Reliab. Eng. Syst. Saf. 189, 279–286. https://doi.org/10.1016/j.ress.2019.04.035.

Aven, T., Ylönen, M., 2021. How the risk science can help us establish a good safety culture. J. Risk Res. 24 (11), 1349–1367.

Bieder, C., Pettersen Gould, K., 2020. The Coupling of Safety and Security, Springer Briefs in Safety Management. https://doi.org/10.1007/978-3-030-47229-0_9.

Boyes, H., Hallaq, B., Cunningham, J., Watson, T., 2018. The industrial internet of things (IIoT): An analysis framework. Comput. Ind. 101, 1–12. https://doi.org/10.1016/j.compind.2018.04.015.

Borodzicz, E.J., 2005. Risk, Crisis and Security Management. John Wiley & Sons Limited, Chichester, UK.

Brunt, R., Unal, B., 2019. Cybersecurity by Design in Civil Nuclear Power Plants. Chatham House. The Royal Institute of International Affairs. UK.

Center of Chemical Process Safety (CCPS), 2003. Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites. Wiley/AIChE, New York.

Center for Chemical Process Safety (CCPS), 2008. Guidelines for Hazard Evaluation Procedures, 3rd ed. CCPS/AIChE, New York.

Chen, C., Reniers, G., Yang, M., 2022. Integrating Safety and Security Management to Protect Chemical Industrial Areas from Domino Effects. Springer Series in Reliability Engineering. Springer, Cham. https://doi.org/10.1007/978-3-030-88911-1_1.

Chockalingam S., Hadžiosmanović D., Pieters W., Teixeira A., van Gelder P., 2017. Integrated Safety and Security Risk Assessment Methods: A Survey of Key Characteristics and Applications. In: Havarneanu G., Setola R., Nassopoulos H., Wolthusen S. (Eds.) Critical Information Infrastructures Security. CRITIS 2016. Lecture Notes in Computer Science, vol 10242. Springer, Cham. https://doi.org/10.1007/978-3-319-71368-7_5.

Cusimano, J., Rostick, P., 2018. If It Isn't Secure, It Isn't Safe: Incorporating Cybersecurity into Process Safety. In: AIChE Spring Meeting and Global Congress on Process Safety, April 2018.

De Porcellinis, S., Setola, R., Panzieri, S., Ulivi, G., 2008. Simulation of heterogeneous and interdependent critical infrastructures. Int. J. Crit. Infrastruct. 4 (1–2), 110–128. https://doi.org/10.1504/IJCIS.2008.016095".

Dekker, S., Cilliers, P., Hofmeyr, J.H., 2011. The complexity of failure: implications of complexity theory for safety investigations. Saf. Sci. 49 (6), 939–945. https://doi.org/10.1016/j.ssci.2011.01.008.

Ding, D., Han, Q.-L., Xiang, Y., Ge, X., Zhang, X.-M., 2018. A survey on security control and attack detection for industrial cyber-physical systems. Neurocomputing 275, 1674–1683. https://doi.org/10.1016/j.neucom.2017.10.009.

Faramondi, L., Flammini, F., Guarino, S., Setola, R., 2021. A Hardware-in-the-Loop Water Distribution Testbed Dataset for Cyber-Physical Security Testing. IEEE Access 9, 122385–122396. https://doi.org/10.1109/ACCESS.2021.3109465.

Friedberg, I., McLaughlin, K., Smith, P., Laverty, D., Sezer, S., 2017. STPASafeSec: Safety and security analysis for cyber-physical systems. J. Information Security Applications 34, 183–196. https://doi.org/10.1016/j.jisa.2016.05.008.

Garcia, M., Grill, J., Stiborek, J., Zunino, A., 2014. An empirical comparison of botnet detection methods. Computers Security 45, 100–123. https://doi.org/10.1016/j.cose.2014.05.011.

Ghosh, S., Sampalli, S., 2019. A survey of security in SCADA networks: Current issues and future challenges. IEEE Access 7, 135812–135831. https://doi.org/10.1109/ACCESS.2019.2926441.

Giddens, A., 1991. The Consequences of Modernity. Cambridge: Polity Press.

Giddens, A., 1994. Living in a post-traditional society. In: Beck, U., Giddens, A., Lash,S. (Eds.). Reflexive Modernization. Politics, Tradition and Aestheticsin the Modern Social Order. Cambridge: Polity Press, 56–109.

Gilligan, J.M., 2021. Expertise Across Disciplines: Establishing Common Ground in Interdisciplinary Disaster Research Teams. Risk Anal. 41 (7), 1171–1177.

Goh, J., Adepu, S., Junejo, K.N., Mathur, A., 2017. A Dataset to Support Research in the Design of Secure Water Treatment Systems. In: Havarneanu G., Setola R., Nassopoulos H., Wolthusen S. (Eds.) Critical Information Infrastructures Security. CRITIS 2016. Lecture Notes in Computer Science, vol 10242. Springer, Cham. https://doi.org/10.1007/978-3-319-71368-7_8.

Haimes, Y.Y., Horowitz, B.M., Lambert, J.H., Santos, J.R., Lian, C., Crowther, K.G., 2005. Inoperability input-output model for interdependent infrastructure sectors. I: Theory and methodology. J. Infrastruct. Syst. 11 (2), 67–79. https://doi.org/10.1061/(ASCE)1076-0342(2005)11:2(67).

Harvey, C., Stanton, N.A., 2014. Safety in System-of-Systems: Ten key challenges. Saf. Sci. 70, 358–366. https://doi.org/10.1016/j.ssci.2014.07.009.

Hashimoto, Y., Toyoshima, T., Yogo, S., Koike, M., Hamaguchi, T., Jing, S., Koshijima, I., 2013. Safety securing approach against cyber-attacks for process control system. Comput. Chem. Eng. 57, 181–186. https://doi.org/10.1016/j.compchemeng.2013.04.019.

Heikkilä, J., Nissilä, M., Ylönen, M., Gotcheva, N., Tugnoli, A., Iaiani, M., Cozzani, V., Oliva, G., Setola, R., Assenza, G., van der Beek, D., Steijn, W., Young, H., Roelofs, M., 2021. Guidelines: Integrated Management of Safety and Security Synergies in Seveso

plants (SAFeRA 4STER). VTT Technical Research Centre of Finland. VTT Technology No. 385.
Hollnagel, E., Woods, D. D., Leveson, N., 2006. (Eds.). Resilience engineering: Concepts and precepts. Ashgate Publishing.
Hollnagel, E., Pariès, J., Woods, D.D., Wreathall, J., 2011. Resilience Engineering in Practice. Farnham, UK: Ashgate.
Hollnagel, E. 2014. Safety I and Safety II. Past and future of safety management. Farnham: Ashgate.
HSE OG86. Cyber Security for Industrial Automation and Control Systems (IACS).HSE Operational Guidance. https://www.hse.gov.uk/foi/internalops/og/og-0086.pdf.
IAEA, 2008. Nuclear Security Culture. IAEA Nuclear Security series No. 7. Implementing Guide. International Atomic Energy Agency, Vienna.
IAEA, 2011. Computer Security at Nuclear Facilities. Nuclear Security Series No. 17. Technical Guidance. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf.
IAEA, 2017. Self-assessment of nuclear security culture in Facilities and Activities. IAEA Nuclear Security series No 28-T. Technical guidance.
Iaiani, M., Casson Moreno, V., Reniers, G., Tugnoli, A., Cozzani, V., 2021a. Analysis of events involving the intentional release of hazardous substances from industrial facilities. Reliab. Eng. Syst. Saf. 212, 107593. https://doi.org/10.1016/j.ress.2021.107593.
Iaiani, M., Tugnoli, A., Bonvicini, S., Cozzani, V., 2021b. Analysis of Cybersecurity-related Incidents in the Process Industry. Reliab. Eng. Syst. Saf. 209, 107485. https://doi.org/10.1016/j.ress.2021.107485.
Iaiani, M., Tugnoli, A., Bonvicini, S., Cozzani, V., 2021c. Major accidents triggered by malicious manipulations of the control system in process facilities. Saf. Sci. 134, 105043. https://doi.org/10.1016/j.ssci.2020.105043.
Iaiani, M., Tugnoli, A., Macini, P., Cozzani, V., 2021d. Outage and asset damage triggered by malicious manipulation of the control system in process plants. Reliab. Eng. Syst. Saf. 213, 107685. https://doi.org/10.1016/j.ress.2021.107685.
International Council of Chemicals Associations (ICCA). https://icca-chem.org/focus/responsible-care/.
International Organization for Standardization (ISO), 2018. ISO 31000:2018(E) Risk Management - Guidelines.
International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) 2012. ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity.
International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), 2018. ISO/IEC 27000 series of standards: Information technology - Security techniques - Information security management systems.
International Society of Automation (ISA), International Electrotechnical Commission (IEC), 2018. ISA/IEC 62443 Series of Standards: Industrial Automation and Control Systems Security.
Jasanoff, S., 1993. Bridging the two cultures of risk analysis. Risk analysis 13 (2), 123. https://doi.org/10.1111/j.1539-6924.1993.tb01057.x.
Ji, Z., Yang, S.H., Cao, Y., Wang, Y., Zhou, C., Yue, L., Zhang, Y., 2021. Harmonizing safety and security risk analysis and prevention in cyber-physical systems. Process Saf. Environ. Prot. 148, 1279–1291. https://doi.org/10.1016/j.psep.2021.03.004.
Jørgensen, T.H., Remmen, A., Mellado, M.D., 2006. Integrated management systems - three different levels of integration. J. Cleaner Prod. 14 (8), 713–722. https://doi.org/10.1016/j.jclepro.2005.04.005.
Kaspersky and ARC Advisory Group, 2020. The State of Industrial Cybersecurity in the Era of Digitalization. https://ics.kaspersky.com/the-state-of-industrial-cybersecurity-2020/.
Kavallieratos, G., Katsikas, S., Gkioulos, V., 2020. Cybersecurity and Safety Co-Engineering of Cyberphysical Systems—A Comprehensive Survey. Future Internet 12 (65), 65. https://doi.org/10.3390/fi12040065.
Kleiner, B.M., Hettinger, L.J., Dejoy, D.M., Huang, Y.-H., Love, P.E.D., 2015. Sociotechnical Attributes of safe and unsafety work systems. Ergonomics 58 (4), 635–649.
Kriaa, S., Pietre-Cambacedes, L., Bouissou, M., Halgand, Y., 2015. A survey of approaches combining safety and security for industrial control systems. Reliab. Eng. Syst. Saf. 139 (2015), 156–178. https://doi.org/10.1016/j.ress.2015.02.008.
Krippendorff, K. H., 2013. Content analysis: An introduction to its methodology (3rd ed.). California; CA: Sage Publications.
Kunal, Dua, M., 2019. Machine learning approach to IDS: A comprehensive review. In: 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA), pp. 117–121. https://doi.org/10.1109/ICECA.2019.8822120.
Landucci, G., Reniers, G., 2019. Preface to special issue on quantitative security analysis of industrial facilities. Reliab. Eng. Syst. Saf. 191 (2019), 106611 https://doi.org/10.1016/j.ress.2019.106611.
Langner, R., 2013. The RIPE Framework. A Process-Driven Approach towards Effective and Sustainable Industrial Control System Security. Langner Communications Whitepaper. https://www.langner.com/wp-content/uploads/2017/04/The-RIPE-Framework.pdf.
Laso, P.M., Brosset, D., Puentes, J., 2017. Dataset of anomalies and malicious acts in a cyber-physical subsystem. Data in Brief 14, 186–191. https://doi.org/10.1016/j.dib.2017.07.038.
Leveson,N. G., 1995. Safeware: System safety and computers. A guide to preventing accidents and losses caused by technology. Addison-Wesley Professional.
Leveson, N. 2012. Engineering a safer world: systems thinking applied to safety. Cambridge, MA: The MIT Press. https://dx.doi.org/10.7551/mitpress/8179.001.0001.
De Maggio, M.C., Mastrapasqua, M., Tesei, M., Chittaro, A., Setola, R., 2019. How to improve the security awareness in complex organizations. Eur. J. Security Res. 4 (1), 33–49.
Mannan, S., 2012. Lees' Loss Prevention in the Process Industries, 4th ed. Elsevier. https://doi.org/10.1016/C2009-0-24104-3.
Marszal, E.M., McGlone, J., 2019. Security PHA Review for Consequence-Based Cybersecurity. International Society of Automation, 168 pages ISBN: 978-1-64331-000-8.
Martí, J., Ventura, C., Hollman, J., Srivastava, K., Juárez, H., 2008. I2Sim modelling and simulation framework for scenario development, training, and real-time decision support of multiple interdependent critical infrastructures during large emergencies. In: NATO RTO Modelling and Simulation Group Conference, Vancouver, BC, Canada.
Matteini, A., Argenti, F., Salzano, E., Cozzani, V., 2019. A comparative analysis of security risk assessment methodologies for the chemical industry. Reliab. Eng. Syst. Saf. 191, 106083. https://doi.org/10.1016/j.ress.2018.03.001.
Miciolino, E.E., Setola, R., Bernieri, G., Panzieri, S., Pascucci, F., Polycarpou, M.M., 2017. Fault diagnosis and network anomaly detection in water infrastructures. IEEE Des. Test 34 (4), 44–51. https://doi.org/10.1109/MDAT.2017.2682223.
Moustafa, N., Slay, J., 2015. UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In: 2015 Military Communications and Information Systems Conference (MilCIS), Nov. 2015, pp. 1–6. https://dx.doi.org/10.1109/MilCIS.2015.7348942.
Nicolaou, N., Eliades, D. G., Panayiotou, C., Polycarpou, M. M., 2018. Reducing vulnerability to cyber-physical attacks in water distribution networks. In: 2018 international workshop on cyber-physical systems for smart water networks (CySWater), pp. 16-19. https://doi.org/10.1109/CySWater.2018.00011.
Nolan, D.P., 2015. Safety and Security Review for the Process Industries: Application of HAZOP, PHA, What-IF and SVA Reviews, 4th Ed., Elsevier. https://doi.org/10.1016/B978-0-323-32295-9.00015-X.
Oliva, G., Panzieri, S., Setola, R., 2010. Agent-based input–output interdependency model. Int. J. Crit. Infrastruct. Prot. 3 (2), 76–82. https://doi.org/10.1016/j.ijcip.2010.05.001.
Pereira, D., Hirata, C., Pagliares, R., Nadjm-Tehrani, S., 2017. Towards Combined Safety and Security Constraints Analysis. In: Tonetta S., Schoitsch E., Bitsch F. (eds) Computer Safety, Reliability, and Security. SAFECOMP2017. Lecture Notes in Computer Science, vol 10489. Springer, Cham. https://doi.org/10.1007/978-3-319-66284-8_7.
Pièrre-Cambacédès, L., Bouissou, M., 2013. Cross-fertilization between safety and security engineering. Reliab. Eng. Syst. Saf. 110 (2013), 110–126. https://doi.org/10.1016/j.ress.2012.09.011.
Reniers, G.L.L., Cremer, K., Buytaert, J., 2011. Continuously and simultaneously optimizing an organization's safety and security culture and climate: the Improvement Diamond for Excellence Achievement and Leadership in Safety & Security (IDEAL S&S). J. Cleaner Prod. 19, 1239–1249. https://doi.org/10.1016/j.jclepro.2011.03.002.
Reniers, G., Amyotte, P., 2012. Prevention in the chemical and process industries: Future directions. J. Loss Prev. Process Ind. 25 (1), 227–231. https://doi.org/10.1016/j.jlp.2011.06.016.
Reniers, G.L.L., Sörensen, K., Khan, F., Amyotte, P., 2014. Resilience of chemical industrial areas through attenuation-based security. Reliab. Eng. Syst. Saf. 131, 94–101. https://doi.org/10.1016/j.ress.2014.05.005.
Reniers, G., Khakzad, N., 2017. Revolutionizing safety and security in the chemical and process industry: Applying the CHESS concept. J. Integrated Security Sci. 1, 2–15.
Rosato, V., Issacharoff, L., Tiriticco, F., Meloni, S., Porcellinis, S., Setola, R., 2008. Modelling interdependent infrastructures using interacting dynamical models. Int. J. Crit. Infrastruct. 4 (1–2), 63–79. https://doi.org/10.1504/IJCIS.2008.016092.
Sabaliauskaite, G., Liew, L.S., Cui, J., 2018. Integrating autonomous vehicle safety and security analysis using STPA method and the six-step model. Int. J. Adv. Security 11, 160–169.
Schmittner, C., Ma, Z., Puschner, P., 2016. Limitation and Improvement of STPA-Sec for Safety and Security Co-analysis. In: Skavhaug, A., Guiochet, J., Schoitsch, E., Bitsch, F. (eds) Computer Safety, eliability, and Security. SAFECOMP 2016. Lecture Notes in Computer Science, vol 9923. Springer, Cham. https://doi.org/10.1007/978-3-319-45480-1_16.
Schulman, P.R., 2020. Safety and Security: Managerial Tensions and Synergies. In Bieder, C., Pettersen Gould, K. (eds.), The Coupling of Safety and Security, SpringerBriefs in Safety Management, https://doi.org/10.1007/978-3-030-47229-0_9.
Smith, C., Brooks, D.J., 2012. Security Science: The theory and practice of security. Butterworth-Heinemann.
Song, G., Khan, F., Yang, M., 2019. Integrated Risk Management of Hazardous Processing Facilities. Process Saf. Prog. 38 (1), 42–51. https://doi.org/10.1002/prs.11978.
SRA 2018 Glossary Society for Risk Analysis, www.sra.org/resources.
Star, S.L., 2010. This is not a boundary object: reflection on the origin of a concept. Sci. Technol. Human Values 35 (5), 601–617.
Sørby, K., 2003. Relationship between security and safety in a security-safety critical system: Safety consequences of security threats. NTNU, Trondheim, Norway, MSc thesis, 2003.
Tao, F., Zhang, H.e., Liu, A., Nee, A.Y.C., 2019. Digital twin in industry: State-of-the-art. IEEE Trans. Ind. Inf. 15 (4), 2405–2415. https://doi.org/10.1109/TII.2018.2873186.
Tavallaee, M., Bagheri, E., Lu, W., Ghorbani, A. A., 2009. A detailed analysis of the KDD CUP 99 data set. In: 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, pp. 1–6. https://doi.org/10.1109/CISDA.2009.5356528.
Vinayakumar, R., Alazab, M., Soman, K.P., Poornachandran, P., Al-Nemrat, A., Venkatraman, S., 2019. Deep Learning Approach for Intelligent Intrusion Detection System. IEEE Access 7, 41525–41550.

Wei, J., Matsubara, Y., Takada, H., 2016. HAZOP-based Security Analysis for Embedded Systems. https://pdfs.semanticscholar.org/be5f/8ee2e5862d3f85bc9dbff4b444d1bfdd9dbc.pdf.

Wynne, B., 1988. Technology as Cultural Process. In: Baark E., Svedin U. (Eds.) Man, Nature and Technology. Palgrave Macmillan, London. https://doi.org/10.1007/978-1-349-09087-7_5.

Wynne, B. 1996. May the sheep safely graze? A reflexive view of the expert – lay knowledge divide. In: Lash, S., Szerszynski, B., Wynne, B. (Eds.) Risk, environment and modernity: towards a new ecology, Sage Publications, London (1996), pp. 44-83.

Yang, Z., Marti, J.R., 2022. Real-time Resilience Optimization Combining an AI Agent with Online Hard Optimization. IEEE Trans. Power Syst. 37 (1), 508–517. https://doi.org/10.1109/TPWRS.2021.308837.

Ylönen, M., Nissilä, M., Heikkila, J., Gotcheva, N., Tugnoli, A., Iaiani, M., Cozzani, V., Oliva, G., Setola, R., Assenza, G., Van Der Beek, D., Steijn, W., Young, H., Roelofs, M., 2021. Integrated Management of Safety and Security Synergies in Seveso plants (SAFERA 4STER). Final report. VTT Technology 386.

Young, W., Leveson, N.G., 2014. Insider risks: An integrated approach to safety and security based on systems theory. Commun. ACM 57 (2), 31–35. https://doi.org/10.1145/2556938.

Yu, K.D.S., Aviso, K.B., Santos, J.R., Tan, R.R., 2020. The economic impact of lockdowns: A persistent inoperability input-output approach. Economies 8 (4), 109. https://doi.org/10.3390/economies8040109.

Özgür, A., Erdem, H., 2016. A review of KDD99 dataset usage in intrusion detection and machine learning between 2010 and 2015. PeerJ Preprints, vol. 4, Art. no. e1954v1. https://doi.org/10.7287/peerj.preprints.1954v1.