Safety Science 166 (2023) 106236

Contents lists available at ScienceDirect

Safety Science

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

Integrated management of safety and security (IMSS) in the nuclear industry – Organizational culture perspective

Marja Ylönen [a], Kim Björkman [b]

[a] University of Stavanger, 4036 Stavanger, P.O. Box 8600, Norway
[b] VTT Technical Research Centre of Finland Ltd., P.O. Box 1000, FI-02044 VTT, Finland

ARTICLE INFO

Keywords:
Safety
Security
Integrated management
Risk
Organizational culture

ABSTRACT

The study is inspired by the change in the risk landscape caused by the development of digitalization and automation in the high-risk industry. The increasing convergence of process-safety, physical security, and cybersecurity risks can lead to major accidents. Integrated management of safety and security (IMSS) is a necessary means of preventing and preparing for accidents. The objective of this paper is to get new insights into the current state of IMSS and related challenges in the nuclear industry. The data includes the International Atomic Energy Agency (IAEA) and World Institute for Nuclear Security (WINS) reports, articles on digitalization, IMSS, and interviews with safety and security experts from two power companies and the Radiation and Nuclear Safety Authority in Finland. The paper compares the results with those in Seveso installations. The methods are thematic and qualitative content analysis. Theoretical framework consists of organizational culture and management perspectives. The paper provides new meanings to the ways in which IMSS is currently implemented. The paper shows the IAEA structural support to IMSS, differences in IMSS implementation in the nuclear industry, and organizational cultural aspects that constrain the IMSS. The latter include the subordination of security to safety, the assumption that organizational culture automatically integrates safety and security, the lack of co-identification and co-assessment of safety and security risks, which prevents a better understanding of systemic risks. The conclusion is that the current state of IMSS is not adequate to address converging, systemic risks, and coordination of safety and security aspects requires more attention.

1. Introduction

The motivation to study integrated management of safety and security (IMSS) (and safeguards) in the nuclear context derives from the advancement of technologies such as digitalization and automation, and the use of artificial intelligence (AI) tools to analyse big data, e.g., deriving from sensors that monitor industrial processes. In high-risk industry contexts, the development of digitalization and automation has led to increasingly blurred boundaries between information technology (IT) and instrumentation and control (I&C) systems, and this makes I&C systems more vulnerable to cyberattacks (Boyes et al. 2018). Due to this development the risk landscape has also changed, and that means that physical security, cybersecurity, and plant safety risks can converge and lead to major accidents (Ylönen et al. 2022; Boyes et al. 2018; Brunt and Unal 2019). An example is a malware installed in the nuclear facility's I&C system during the maintenance. This malware compromises the sensory information and provides incorrect data to the I&C system and/or personnel. Because of the incorrect data, the I&C system can wrongly control the plant towards a dangerous state causing e.g., a transient (i.e., an event when the state of a plant progresses from normal to abnormal).

Instrumentation and control systems play a crucial role in the safe operation of nuclear facilities (IAEA 2018b). The I&C system architecture has three primary functions: 1) to provide the sensory (e.g., measurement and surveillance) capabilities to support functions such as monitoring or control and to enable plant personnel to assess the plant status, 2) to provide automatic control, both of the main plant and of many auxiliary systems, 3) to protect the plant from the consequences of any malfunction or deficiency of plant systems or human errors (IAEA, 2011). Even though, digital I&C systems include many benefits compared to older analogue based solutions, such as improved operational efficiency, improved equipment monitoring, and I&C self-monitoring they also pose challenges such as preserving independence to support in depth defence, limiting the potential effects of postulated common cause failures, ensuring sufficient cybersecurity, and avoiding unnecessary complexity (IAEA 2018a).

E-mail addresses: marja.k.ylonen@uis.no (M. Ylönen), Kim.bjorkman@vtt.fi (K. Björkman).

https://doi.org/10.1016/j.ssci.2023.106236
Received 19 October 2022; Received in revised form 22 May 2023; Accepted 14 June 2023
Available online 3 July 2023

Despite the rare news of cybersecurity challenges and attacks on nuclear power plants (NPPs), there are some cases that have revealed cybersecurity risks. In 2014 in the Japanese Monju NPP a piece of computer malware was found in the control room computer. The malware derived from a programme update. In the contaminated computer there were over 42,000 emails and training reports. The malware sent the information to servers in another country. The computer was an ordinary office PC, so in this case it did not have impacts on nuclear safety. However, if the system would have included information about nuclear fuel transfer, this would have been a serious threat to nuclear safety and security. In another case in the Hatch NPP in the US, a software update led to a reactor shutdown. The worker of an external maintenance service company had made a software update to a computer that was connected to the office network. The computer was used to collect diagnostic data from the NPP's process control system. The update was supposed to synchronize data in the process control system and business system. Instead, the computer reset the all the data of the process control system in the context of restarting the NPP. The protection system caused a reduction of cooling water levels that led to a reactor shutdown. From the information security viewpoint, uncontrollable changes are seen as a high source of risks (Holappa and Valkama 2017). For instance, the Chatham house report expresses concerns that NPPs do not adequately consider cybersecurity risks and that the nuclear industry's awareness of cybersecurity risks is not adequate (see Baylon et al. 2015; Brunt and Unal 2019). Thus, to efficiently use I&C and to be better prepared for I&C-related risks and the convergence of IT and I&C risks, better integration of safety and security is needed.

Nuclear safety and security share a common objective, to protect individuals, the public and the environment from harmful effects of ionizing radiation (IAEA 2021a). There can be both synergies and conflicts between safety and security. Strengthening one can have a positive or negative impact on the other. An example of a positive impact is the strengthening of cybersecurity to hinder the modification of, e.g., sensor data to prevent I&C systems from performing their safety functions (e.g., reactor trip i.e., automatic or manual emergency shutdown of the plant). Thus, strengthening cybersecurity contributes to I&C systems safety. An example of a negative impact is adding a new physical security barrier to prevent an intruder's access, e.g., to an area where safety systems' components are located. However, the access, when demanded, to a safety critical equipment can be delayed (WINS 2019a). Thus, it is crucial to establish a well-coordinated approach to managing the interface between nuclear safety and nuclear security. WINS (2019a) lists typical benefits using and issues for not using an integrated approach for safety and security management.

IMSS has been seen as a necessary step towards better safety and security in the high-risk industry (Reniers and Khakzad 2017; Schulman 2020; Iaiani et al. 2021a; Iaiani et al. 2021b; Ylönen et al. 2022). The need for integration is triggered by 1) fundamental changes in the risk landscape referring to an increasing convergence of safety, physical and cybersecurity risks, which may lead to major accidents, 2) systemic, emergent risks, which cannot be understood simply by identifying the risks separately for each safety and security domains and then combining them, instead, the co-construction of risk identification is necessary.

By integration we refer to 3 dimensions of integration: structural (e.g., an organization's strategies), functional (an organization's safety and security management) and cultural (e.g., safety and security cultures, and a culture of learning from accidents) (Jørgensen et al.2006). These will be discussed more in the theoretical framework and concepts section of this paper.

The SAF€RA 4STER research project (2019–2020) on IMSS in Seveso plants serves as a reference point for this study (Ylönen et al. 2022). Seveso plants (e.g., refineries, petrochemical sites, chemicals industries) produce, store, or use large quantities of hazardous chemicals and are subject to the requirements of the Seveso III Directive (2012/18/EU). The goal of the directive is to control major accident hazards involving dangerous substances, and it contributes to the technological disaster risk reduction effort. In the SAF€RA 4STER research project, the current state of IMSS (based on interviews with the safety and security experts in the industries as well as representatives of regulators) as well as the cybersecurity and physical security induced incidents and accidents were studied. An analysis of past accidents showed that 1) the integrated management of safety and security would need to pay attention to following cybersecurity-related events: i) an attack on IT systems and compromising sensitive data/information, ii) an attack on the I&C system leading to loss of production (e.g., a production shutdown), iii) an attack infecting the I&C system aimed at generating a major event. The study also showed that 2) the identification of process-safety, physical security and cybersecurity risks are conducted separately, and managed by separate units, and therefore understanding convergent risks remains thin. Separate safety and security risk analyses easily create silos and hamper possibilities to address and manage systemic risks efficiently. 3) Often used risk identification techniques in safety domains cannot be used to identify the potential major events, e.g., a Hazard and Operability Analysis (HAZOP) does not consider external or non-random causes or sources of risks, or multiple failures (Ylönen et al. 2022; Iaiani et al. 2021b).

The contribution of this study to the safety and security in the nuclear field is that it combines the current knowledge on digitalization, safety-security interfaces, IAEA technical guidance documents, the Finnish regulatory framework, as well as the current practices and challenges regarding the implementation of the framework and safety-security synergies. The objective of this paper is to evoke discussions regarding the relationship between safety and security, current practice, organizational boundaries, and needs for improvement in safety-security interfaces in NPPs.

The research questions are the following:

1) What is the current state of integration of safety and security management in NPPs?
2) What are the needs and challenges regarding integration?

The data consists of IAEA and WINS reports on nuclear safety and nuclear security (IAEA 2021a; IAEA 2016; IAEA 2010; WINS 2019a; WINS 2019b; IAEA 2017, IAEA 2008) and a report on Finnish national regulatory framework regarding safety-security interface (Johansson et al. 2018). In addition, the data include interviews with safety and security experts in the nuclear industry and the Radiation and Nuclear Safety Authority (STUK) in Finland. Furthermore, the review of the literature related to digitalization and IMSS (e.g., Reniers et al. 2014; Song et al. 2019; Boyes et al. 2018) carried out in the SAF€RA study (Ylönen et al. 2021) is used as secondary data in the study.

The paper is structured as follows: after the introduction the second section introduces IT and I&C at nuclear facilities. The third section deals with the theoretical framework and core concepts, while the fourth section deals with the data and method of analysis. The fifth section presents the findings of the study based on the analysis of reports, interviews, and the literature review. The sixth section consists of discussion and conclusion.

2. IT & I&C at nuclear facilities

Digital technologies are being included more frequently in I&C systems at nuclear facilities. New nuclear facilities and modern nuclear facility designs utilize digital I&C systems, and during the modernization of existing facilities digital technologies are introduced to the I&C systems. Digital I&C systems make it possible to efficiently handle large amounts of process data while requiring less human interaction than previous I&C systems. However, digital I&C are also more vulnerable to cybersecurity threats. Cyber-attacks can endanger the safety and security of nuclear facilities leading, e.g., to loss of process control or radiological consequences.

At nuclear facilities the IT and I&C systems consist of the following levels and components (WINS 2019b):

- Level 4 (IT): Enterprise Resource Planning (ERP).
- Level 3 (IT): Manufacturing Execution System (MES).
- Level 2 Supervisory Control And Data Acquisition (SCADA) system (I&C): Supplies the information collected from the PLCs and DCSs to control room operators, enabling them to manage an entire process or plant.
- Level 1: Programmable Logic Controllers (PLC)/Distributed Control Systems (DCS) (I&C): PLCs and DCSs are used in local computers to collect information, e.g., sensor data from different parts of the facility. They also control various processes, e.g., opening and closing of valves.
- Level 0 (I&C): Sensors and actuators.

Levels 4 and 3 represents the IT part and levels 2–0 the I&C part. To provide the required information for plant and business applications, there may be some level of connectivity or communications between IT and I&C (WINS 2019b).

IT and I&C systems are prone to cyber threats from different sources, such as external threats, internal threats and technical development threats (internal changes to the infrastructure that controls and manages nuclear processes). External threats include threats such as the Stuxnet computer worm (Collins and McCombie, 2012). Insider threats may be deliberate or unintentional, e.g., an email attachment infected with a malware program is opened. I&C systems may use standard IT components making them prone to the same malware that threatens the office automation field.

In addition to the individual I&C systems, the design of the overall I&C architecture in nuclear facilities can contribute to cybersecurity by mitigating the effects of intentional or accidental malfunctioning (IAEA 2018b). The overall I&C architecture is the organization of the complete set of I&C systems which are important to safety, including systems identification, classification and segmentation, system and subsystem communication pathways, overall system and subsystem functions and signal handling (IAEA 2018a). Of the five attributes generally concerned with cybersecurity the most important in I&C systems are integrity, availability, and authentication and authorization (confidentiality, and non-repudiation are the other two attributes) (IAEA 2018b). Typically, availability issues are addressed by defence-in-depth levels and approaches. Integrity issues can be addressed by managing the information flow. As far is reasonably possible, information should move from security zones of higher integrity to security zones of lower integrity and not vice versa.

In (WINS 2019b), four building blocks for a robust security infrastructure are presented. These include risk assessment, design principles, lifecycle management and a security culture. Risk assessment should form the basis for selecting security measures allowing the organization to focus efforts on the areas that provide the highest impact. The design principles building block considers topics such as zoning and compartmentalization, defence-in-depth, and integrating physical and cybersecurity. These principles should be applied regardless of risk assessment results. Cybersecurity needs to be explicitly considered during all life cycle phases (IAEA 2018b). Security should be designed into the systems from the beginning (WINS 2019b). Since humans are a crucial part of security, it is important that the security culture includes IT, I&C, and physical security. In (IAEA 2021b), a security culture has been defined as: “The assembly of characteristics, attitudes and behaviour of individuals, organizations and institutions which serves as a means to support, enhance and sustain nuclear security”. Training is an effective way to advance a security culture (WINS 2019b). According to the IAEA (2008), a nuclear security culture and nuclear safety culture build on the organization culture, i.e., shared values, attitudes, beliefs, and norms in the organization.

Many cybersecurity standards and guidance frameworks have been developed for industrial control systems. Many of the standards have been reviewed in (Linnosmaa et al. 2021) from the Finnish nuclear I&C perspective. The review considered the most significant standards to be the IEC 62443 series (Industrial communication networks—IT security for networks and systems), ISO 27000 series (Information technology—Security techniques—Information security management systems), IEC 62645 (Nuclear Power Plants—Instrumentation, control and electrical power systems—Cybersecurity requirements), IEC 62859 (Nuclear Power Plants—Instrumentation and control systems—Requirements for coordinating safety and cybersecurity) and IAEA’s NSS 17 (Computer Security at Nuclear Facilities).

3. Theoretical frameworks and core concepts: Organizational culture, integrated management, safety, security, cybersecurity

The theoretical framework described here consists of Edgar Schein’s model of organizational culture (1992, 2010) and the concept and layers of integrated management (Jørgensen et al. 2006), see Fig. 1. In addition, to examine safety and security, including physical security and cybersecurity and related risks and interfaces, we define these main concepts in Table 1, in the Appendix A.

Theories and studies on organizational culture and management provide relevant lenses to approach the research questions on the integration of safety and security, and related challenges (Schein 2010; Guldenmund 2000; Henriqson et al. 2014; Reiman et al. 2015; Glesner et al. 2020; Jørgensen et al. 2006; Stacey 2012). The choice of the approach also affects the data collection and analysis as well as interpretation of the findings, not to mention the application of the results.

By organizational culture we refer to shared beliefs, values, norms, practices and structures in the organization (Guldenmund 2000; Pidgeon 1991; Schein 2004; Henriqson et al. 2014). Organizational culture is a collective-level phenomenon, although individuals are the carriers of organizational culture. There are two opposite understandings regarding the concept of culture: anthropological and instrumental. The anthropological understanding emphasizes that culture is an emergent phenomenon that is formed as a result of interactions between an organization’s members and therefore it cannot be steered or managed, but it may be influenced (Grøte 2012; Haukelid 2008). Instead, the instrumental understanding stresses that culture can be managed and steered, e.g., by allocating resources, structuring the organization’s activities and affecting processes in ways that are beneficial to safety (Swartz 2000; Schein 2004; Haukelid 2008; Silbey 2009; Aven and Ylönen 2021). Both anthropological and instrumental understanding provide valuable perspectives on organizational culture (Edwards et al. 2013).

Why the organizational culture should be affected is, e.g., an effort to reduce the frequency of safety deviations and the severity of possible accidents or the desire to create common understanding of the importance of safety and security in the company’s operations. In addition, an important reason why organizational culture should be affected is the understanding that the organizational culture is a key factor in other organizational changes, e.g., the introduction of new technologies (Alvesson and Sveningsson 2015). The way in which the organizational culture (e.g., values and beliefs) can be influenced is, e.g., the good example of senior managers, training, and continuous implementation of safety values etc.

Edgar Schein’s three-level model of organizational culture is used here as a framework for considering and analysing the relationship between safety and security (Schein 1992, 2004). Schein distinguishes between three layers of culture. The most visible layer are artifacts and consist of visible behaviour, e.g., how safety and security experts or senior managers communicate in organization. The second layer embraces espoused values, and these values can manifest themselves in rules, standards or prohibitions. The third layer consists of basic underlying assumptions. These are often unconscious, non-reflected assumptions, that can be made visible, for example, by an external analyst,

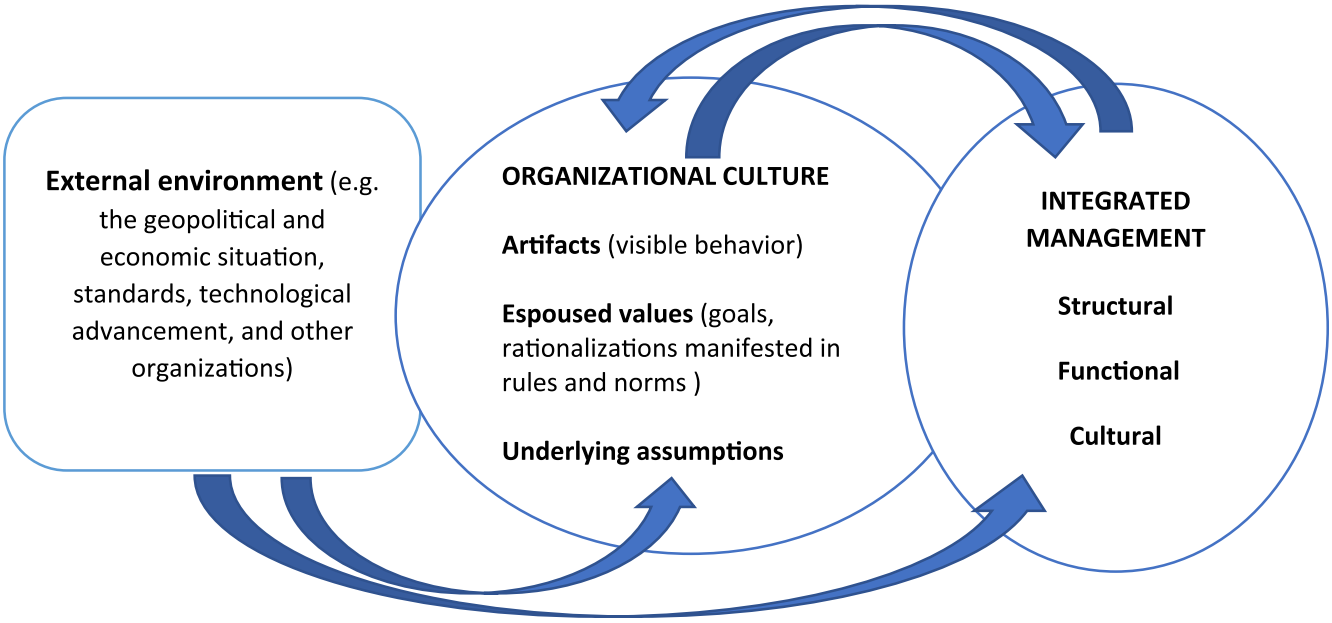

Fig. 1. Analytical framework consisting of 3 levels of organizational culture (Schein 2004) and 3 levels of integration of management (Jørgensen et al. 2006), that influence each other, and are also influenced by the organization's external environment.

Table 1
The core concepts and their definitions.

Concepts	Definitions
Safety	Without unacceptable risks, when the risks derive from unintentional acts or accidents, or the biophysical world, technical failures, human and organizational factors (see SRA Glossary 2018).
Security	Without unacceptable risks, when the risks derive from human malicious intents (SRA Glossary 2018).
Safety-security interface	Interactions between nuclear safety and nuclear security functions of technical systems, organizational and administrative measures including plant procedures in an NPP in operation and within or between regulatory authorities (WENRA 2019).
Cybersecurity	the protection of privacy, integrity, and accessibility of data information in cyberspace (ISO/IEC 27032:2012).
Integrated management of safety and security	An organizational function, as well as procedures and practices that ensure that safety, physical security and cybersecurity risks are (co)identified, (co)analysed (co)assessed, prevented and mitigated. The integration of management can occur at structural, functional and cultural levels in an organization (Jørgensen et al. 2006).
Risk assessment	A systematic process to comprehend the nature of risks and to express and evaluate risks with the available knowledge (Aven 2020, 270).
Risk management	activities to deal with risk, including prevention, mitigation, adaptation or sharing risks (Aven 2019, 271).

so that organizational culture can be improved.

Organizational culture is the basis which the safety culture builds upon. The safety culture concept was launched by the expert group of the IAEA in the aftermath of the Chernobyl nuclear power accident. A safety culture in the nuclear context can be defined as an "*assembly of characteristics and attitudes in organizations and individuals which establish that as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance*" (IAEA, 1991, p. 4). A safety culture is a well-acknowledged concept in the nuclear field and many high-risk industry sectors. In contrast, a security culture is a much newer term, and less used. A security culture as defined in section 2 is located within the organizational culture and implies that the safety culture and security culture can be integrated (IAEA 2008; IAEA 2021b).

By management we refer to the responsibility for and control of a company or organization and their activities. Management includes setting goals, implementing strategies, designing systems, coordinating, and solving problems. Management is closely connected to leadership and refers to developing fresh approaches, exploring new issues, formulating visions and inspiring others to follow a leader (Stacey 2012). Safety management for instance is an organizational function that ensures that safety risks have been identified, prevented, and mitigated. The goal of safety management is to protect from injury, losses, and accidents. Safety management applies a set of principles, processes and measures to fulfil its tasks. Furthermore, in the current complex sociotechnical environment, where several organizational functions, such as management functions, and technical systems such as IT and I&C are interconnected, there are needs to create adaptive responses to new emerging challenges and to strive for a balance between many contradictory demands that the safety and security domains create (e.g., Cameron and Quinn 2011; Dekker et. al. 2011; Harvey and Stanton 2014; Reiman et al. 2015; Aven and Ylönen 2018; Glesner et al. 2020).

The relationship between the organizational culture and safety management can be seen as reciprocal. On the one hand, an organizational culture provides a broad framework within which safety management is established, implemented, and developed. On the other hand, safety management also affects the organizational culture, for example by providing resources and intervening in developments that can be negative in terms of safety (Grote and Künzler 2000; Guldenmund 2010).

By integration we refer to three ways to link safety and security management. These levels include structural, functional and cultural integration. Structural integration refers to the increased compatibility of system elements, such as using the similarities of the standards or creating a company-level policy that integrates safety and security. Functional integration refers to combining core functions or coordination generic processes, such as safety management and security management systems. The deepest level of integration is cultural integration and this refers to the embeddedness of the integrated management of safety and security in a culture of learning and continuous improvement (Jørgensen et al. 2006).

Often, structural integration is the easiest to achieve, whilst cultural

integration requires internalization of the values and understanding of the relevance of integrated management of safety and security among the organization's members. These different levels can also be present simultaneously.

The potential advantages of integration can be characterized as providing synergies, reducing administrative burden and costs, providing coordination and balance between potentially different ways to implement safety and security improvements (Song et al. 2019).

Our analytical framework, Fig. 1, visualizes two mutually complementary frameworks: in the middle, there are 3 layers of organizational culture: i) artifacts, i.e., visible behaviour, ii) espoused values, such as, goals and rationalisations, manifested in rules and norms, and iii) underlying assumptions (Schein, 2004). We approach the IMSS from the perspective of these three layers. In addition, on the right, there are 3 levels of integrated management (Jørgensen et al. 2006) of safety and security, which provide a complementary perspective to IMSS. The cultural dimension includes the adoption of IMSS into the organization's everyday practices, which requires both motivation and an understanding of the importance of integration. Functional dimensions entail that IMSS is shown in the functions and procedures in the organization, and that relates to artifact (visible behaviour) and espoused values (e.g., rationalisation). Similarly, the structural dimensions embracing strategies and structures of organisations relate partly to espoused values and artifacts. In addition, structural dimensions, also partially go beyond the organizational culture framework. An example is laws and regulations that enforce and support IMSS at the structural level. Similarly, recommendations and examples of other companies and industries provide support to changes at the organizations' structural level.

The relationship between integrated management and the organizational culture can be seen in that organizational culture embraces management, and thus has effects on integrated management. However, as mentioned earlier, the integrated management also affects the organizational culture, for example by exerting new demands for collaboration between different experts and organizational units, as well as new definitions and delegation of responsibilities from the integrated management of safety and security perspective.

Both organizational culture and management are influenced by the organization's external environment, such as the geopolitical and economic situation, standards, advancement of technologies, regulatory requirements, as well as by the performance of other organizations such as vendors and suppliers, which organization needs to respond to via its management system. We included external environment in the framework, although we do not use it in the analysis of data. It is important to consider the external environment as a framework condition for organizational culture and integrated management. We provide some examples of external environment in the discussion and conclusions section.

4. Data and methods

This study represents a qualitative study typical of the social sciences. It is characterized by theoretical framework, data (documents and interviews), qualitative research methods, systematic analysis of documents and interviews, and creation of meanings regarding the IMSS (Leavy 2020; Krippendorff 2013; Vaismoradi 2016; Hänninen 2016).

The data consists of a systematic review of IAEA and WINS reports on nuclear safety and nuclear security and their interface (IAEA 2021a; IAEA 2016; IAEA 2010; WINS 2019a; WINS 2019b; IAEA 2017; IAEA 2008) and the report on Finnish national framework on safety-security interface (Johansson et al. 2018). In addition, the data include six interviews with safety and security experts from two power companies and the Radiation and Safety Authority (STUK). Furthermore, as secondary data, the study uses the systematic review of IMSS in high-risk industries conducted in the context of the SAF€RA 4STER study on the IMSS in Seveso plants (Ylönen et al. 2022).

The reports review on interface of nuclear safety and nuclear security was conducted by using the key words "safety security interface", "safety security I&C" and "integrated management of safety and security". The review was restricted to work performed within the International Atomic Energy Agency (IAEA) and the World Institute for Nuclear Security (WINS). Related to IAEA we searched the IAEA's scientific and technical publications. The searches returned 17 hits in total. Publications focusing on e.g., research facilities or transportation of radioactive material were excluded because the focus of this study is on nuclear power plants. In addition, during the review process we excluded superseded publications. The final number of documents was seven. We performed the same searches also in the WINS knowledge center. These searches returned two relevant publications for review.

The interviewees were selected based on their management position and expertise in the safety or security fields in the nuclear industry (Appendix B). In addition, the authors' 10 years' experience from the nuclear safety research, meant foreknowledge of the industry and the research theme, which made it easier to contact interviewees, gain trust and conduct fruitful interviews. The interviews were organized around themes, which were based on the SAF€RA study and the SAF€RA literature review. The themes included e.g. the relationship between safety culture and security culture (e.g., whether or not a separate security culture is essential and rationale for it); the ways in which the safety and security are managed in the company (e.g., integrated or by separate departments; collaboration between safety and security experts; concrete ways to coordinate safety and security; challenges in managing safety and security in an integrated way); the management of IT-I&C and cybersecurity; changes in the risk landscape (Appendix B). The interviews lasted 1–1.5 h each. They were not recorded, but notes were taken during the interviews. In three cases, notes were sent to the interviewees who checked that the facts were written correctly.

In addition, as secondary data, the study uses the systematic review of IMSS in high-risk industries conducted in the context of the SAF€RA 4STER study on the IMSS in Seveso plants. The key words "safety and security" and "integrated management" were used in the search for articles in the 10-year period from 2009 to 2019 from the journals that are presented in the end of this paragraph. After several hits, the number of reviewed articles were reduced based on evaluation of their relevance in terms of IMSS and the concepts of safety and security. (Appendix C). In the SAF€RA study 31 articles on the concepts and management of safety and security in high-risk industries were reviewed (Ylönen et al. 2021). The selected 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) (Ylönen et al. 2022).

The review of IAEA and WINS reports sheds light on IMSS in the nuclear industry, whilst the secondary literature review collected from the SAF€RA study illuminates the motivations for integration and differences and similarities between the safety and security, which are relevant to understanding integration. Furthermore, the whole SAF€RA study provides us with good insight into the current state of digitalization, and the IMSS in high-risk industries, as well as related challenges and opportunities. The literature review was systematic but not exhaustive.

The method of analysis used is a qualitative content analysis in report reviews and literature reviews and a thematic analysis in the interviews (Krippendorff 2013; Vaismoradi et al. 2016). There are similarities between the qualitative content analysis and the thematic analysis. These include systematic coding, examining of meanings, and creation of interpretations, through which it is possible to describe the studied phenomenon, and to create a story that provides new information, develops understanding and that is culturally inspiring (Vaismoradi et al. 2016).

The analysis of the reports was based on manifested contents, and it did not involve interpretations like our analysis of interviews. The thematic analysis of interviews focused both on manifested and latent contents.

The content of the interviews was grouped based on themes. A theme

is here understood as a core component of the interview. Under each theme we added citations from the interviews. Then we typified the citations under each theme and extracted core ideas in terms of the IMSS. These core ideas are presented as findings in section 5. We selected the main findings from the interviews with licensees and the regulators. These are summarized in Table 2. After the described analysis, we exploited Edgar Schein's model of organizational culture as an analytical framework and the three levels of integrated management to interpret the interviewees' experiences. Despite some techniques, there are few practical explanations on how interpretations, i.e., creating meaning and raising to a more abstract level, occurs (Vaismoradi et al. 2016). The results of both interviews and documents will be presented in the next section, summarized in Tables 2 and 3, and further discussed in the discussion section. The representations of the interviewees were interpreted from the perspectives of organizational culture and integrated management. The interpretations represent the findings on a more abstract level.

The empirical quality of the qualitative research can be evaluated based on three dimensions, the number of participants, the abundance of data per person, and depth of the analysis (Hänninen 2016). The number of interviewees is small, but the interviewees were selected based on their experience and expertise in the safety and security fields. This ensured that they were able to provide thorough answers to the interview questions. In addition, the authors' relatively long experience in nuclear safety research provided us with foreknowledge of the subject and made it easier to contact the interviewees and conduct the interviews. This contributed to the fact that we got a lot of data from each interview. Abundant interview data enabled a relatively in-depth analysis, and the theoretical framework supported the interpretations of the IMSS, enabling the creation of new meanings. Together, these factors allowed us to offer new insights into IMSS, and answer research questions.

Validity in this research does not refer to correspondence of the data with the "objective truth", but that the data allows us to produce valid inferences about the reality outside of our data from the perspective of the research questions. (Maxwell 2012).

The limitations of the data include the small number of interviewees in one country, which does not allow generalization in the quantitative sense. However, we argue that it is possible to make qualitative generalisations about the current state of IMSS in the nuclear industry and the challenges and needs of IMSS in high-risk industry based on the analysis of reports, interviews, and the SAF€RA study. The review of the IAEA technical reports and WINS reports provides information about the current state of IMSS and differences in management of safety-security relationships between the nuclear industry companies in different countries. In addition, our interviews and the interviews and results of the SAF€RA study (Ylönen et al. 2022; Appendix C) provide information on the challenges and needs of IMSS in the high-risk industry. Thus, we argue that we can give valid qualitative generalisations about the challenges and needs of IMSS.

5. Results

The results section is divided into three parts following the structure of our theoretical framework. The first part deals with the nuclear power plants' external environment referring here to both the international requirements and experience of the management of the safety-security interface, and the Finnish national regulatory framework for the safety-security interface. The second part focuses on the motivations for the IMSS that reflects general academic understanding of the needs for IMSS. They can inspire IMSS at structural, functional, and cultural levels. Then the third part presents the results from the interviews with safety and security experts from the power companies and the Radiation and Nuclear Safety Authority (STUK) from the perspectives of organizational culture and integrated management.

Table 2
Main findings from the interviews from the organizational culture perspective.

Theme	Artifacts	Espoused values or Underlying assumptions	Impacts on IMSS
Management of security domain	Two contradictory tendencies: making security aspects more commonplace and shared through trainings vs. legitimizing secrecy, i.e., matters belonging to the security domain cannot be discussed	Espoused value (rationality) is that the security management belong to security experts, and many security aspects cannot be discussed. Different management principles in security and safety.	Many employees of NPPs acknowledge that security aspects cannot be openly discussed. This may result in some relevant safety-security interfaces remaining unnoticed, unaddressed, or untouched because security experts may not see all the safety implications.
Safety-security relationship	Talking about security as little brother of safety. Separate risk identifications	Espoused value: Nuclear safety and radiation safety are the priority, and security is subordinate to safety.	Subordination of security to safety and separate risk identifications do not enhance an understanding of systemic and convergent risks.
Safety culture/ security culture	Security subordinated to the safety culture: good security practices are seen as part of good safety culture. In practice safety culture experts do not seem to be closely involved with security.	Underlying assumptions: Safety and security cultures can be developed in parallel within the framework of organizational culture. The organizational culture can automatically support strong performance in security. Separate security culture is not needed.	Security aspects may remain underdeveloped as the security culture is not supported. It may lead to a situation in which the organizational culture is focused more upon safety than security. This will not contribute to understanding the content of security or understanding convergence of safety and security risks. Not clear who is responsible for creating IMSS in an organizational culture. Security aspects and the content may remain unclear. This may hinder the developments of IMSS.
Involvement of safety experts in security related meetings	Security experts involve broad range of safety experts in their meetings. However, safety culture experts do not seem to be closely involved with security.	Espoused value: Collaboration is important.	If safety culture experts rarely participate in security related meetings, understanding of each other's' fields may remain superficial, and therefore also the understanding of systemic safety and security risks remains thin, not to

(continued on next page)

Table 2 (*continued*)

Theme	Artifacts	Espoused values or Underlying assumptions	Impacts on IMSS
			mention that the contribution to IMSS remains inadequate.
IT- I&C and cybersecurity	Even though I&C is separated from IT, digitalization increases cybersecurity challenges, e.g., how to manage maintenance and configuration.	Espoused value is: Being vigilant in terms of cybersecurity risks and possible insider risks.	Change in the risk landscape enhances the need for IMSS.

Table 3
Summary of findings based on the analytical framework of integrated management.

Integrated management	Supportive features	Constraints
Structure	IAEA's support to safety-security interface. Collaboration with external organizations for situation awareness and IMSS National Nuclear Energy Act that enables STUK to supervise 3S.National regulatory framework with overall integrated management system and organizational culture emphasis.In an NPP, corporate security and safety are integrated in the same department. The line organization and the responsible leader are responsible for IMSS.	No unified international approach. Small organizations' scarce resources to handle both safety and security culture. Safety and security have own management models even though they would be integrated in the same department. In STUK separate units deal with safety, security and safeguards.
Function	Joint meetings between safety and security. STUK has carried out inspections with other regulatory bodies.	Safety and security managed by different experts, units, and principles. No integrated risk identification of risk assessments. Safety culture experts not much involved in security meetings, no separate security culture.
Culture	Safety and security aspects seen as important.	Radiation and nuclear safety are the priority goal. Security is subordinate to safety. Security not embedded as strongly in the organizational culture, as the safety culture is. The embeddedness of security and IMSS in the culture of learning and improvement remains obscure.

5.1. External environment: IAEA and WINS experiences and guidance regarding the IMSS

In the following sections, we discuss experiences of managing the safety-security interface in the context of nuclear power from both an international and a national perspective. In addition, we discuss security integration of IT and I&C systems. The IAEA and WINS experiences and guides, as well as Finnish regulatory framework represent here both external environment for the nuclear power companies and the structural level support for the IMSS. The IAEA and WINS documents have both exemplary and directive effects on nuclear power companies' IMSS.

5.1.1. International experience and guidance regarding the management of safety-security interface

In the international nuclear power context, the necessity to tackle with systemic risks through IMSS is acknowledged and strongly supported by the IAEA. Requirements related to leadership and management for safety in organizations are described in IAEA (2016). Concerning management systems (IAEA, 2016) states: *"The management system shall integrate its elements, including safety, health, environmental, security, quality, human-and-organizational-factor, societal and economic elements, so that safety is not compromised."*.

Already IAEA (2010) states that an integrated management approach is needed to ensure that decisions to advance security or safety does not adversely affect the other. Problems related to safety and security should be assessed on mutually supporting and reinforcing terms. In addition, IAEA (2010) discusses the need for the management to endorse both a safety and a security culture to ensure that both objectives receive pertinent attention. IAEA (2010) identifies also the competing logics and related contradictions regarding safety and security. For example, safety is generally advanced by openness and transparency, whereas the management of security requires confidentiality of security information.

Despite the acknowledgment of IMSS, the international experience shows national differences in the management of systems and nuclear safety and nuclear security culture (IAEA 2021a). These differences relate to the relationship between safety and security culture. In some cases, the security culture has been considered a subset of the safety culture. Whereas, in other cases, there are specific nuclear safety and nuclear security culture groups within their regulatory bodies aiming to understand the culture of their organization and to identify and implement improvements. It has turned out that paying more attention to security culture has created a positive impact on the overall organizational culture.

In addition, in some countries the national legal framework can require that safety, nuclear security and safeguards are implemented in an integrated manner (IAEA 2021a). In such cases, the safety and security culture are typically integrated. In the integrated approach, integrated safety and security departments need to have one vision and to report through the same executive. The commitment and support from different levels of management in relevant organizations is needed to sustain an integrated approach. The integrated approach can be considered from three different levels: the strategic level, the operational level, and the cultural level. To be able to completely promote safety and security cultures and their interface the importance of the management system architecture needs to be stressed.

Challenges identified in (IAEA 2021a) included that the countries with small and medium sized organizations might not have sufficient personnel resources with the necessary qualifications and experience in both nuclear safety and nuclear security. Additionally, safety and security experts may not always have the same appreciation and understanding of their roles and responsibilities in each other's area.

Traditionally, nuclear facility management have integrated the different areas of safety, such as nuclear safety, fire safety and occupational safety. However, the same level of integration has not been applied to the interface between safety and security (WINS 2019a). Achieving integrated safety and security is not a trivial task. It requires (1) hard work and support from the company's board and senior management, (2) resources and knowledge about how nuclear safety and nuclear security interact, (3) constant attention to prevent people from becoming complacent, and (4) ways to measure whether integration is successful. (WINS 2019a).

In the development of an integrated approach to safety and security, three levels of the organisation should be considered: strategic, operational and staff (WINS 2019a). The strategic level considers the senior managers that influence policy in their organisation. The operational

level considers the actions that need to be taken by the departments that have an interface with security to guarantee integration. Finally, the staff level considers actions that must be taken by the workforce and visitors to the site.

The above-mentioned levels resemble our framework of integrated management in terms of structural and functional point of view. However, the cultural level, including organizational culture that is relevant to all organizations and their operations, is not explicitly addressed in the WINS (2019a) report.

5.1.2. Management of safety-security interface in the Finnish nuclear regulatory framework

In the Finnish nuclear regulatory framework both safety and security have been considered from the beginning (Johansson, et al. 2018). Safety, and security (and safeguards) are integrated in the same set of regulations and regulatory guides. The Radiation and Nuclear Safety Authority (STUK) has the responsibility for the regulatory control of safety and security (and safeguards). STUK considers the safety-security interface to be a decision point where both safety and security issues should be taken into account (Johansson, et al. 2018).

Leadership and the management of safety, security, and safeguards (3S) are highlighted in the regulatory framework in Finland, which includes an organizational culture considering safety and security aspects (Johansson, et al. 2018). An effective risk management process can be advanced through a safety and security-oriented leadership and management system. The overall integrated management system should include both nuclear safety and security. Within the organizational culture the people should understand how their actions (and omissions) affect the safety and security. The resilience of an organization can be increased with an organizational culture with a strong emphasis on safety and security. STUK considers that the development of separate safety cultures and security cultures would be harmful to overall safety and security (Johansson, et al., 2018).

The safety-security interface should be considered during the entire lifecycle of the plant (Johansson, et al. 2018). The design phase is considered the most efficient life cycle phase of a nuclear facility to aspire to safety and security. During maintenance and when implementing modifications also lies a significant safety security interface.

5.1.3. Security integration of IT and I&C systems

In a nuclear facility, the security of IT and I&C systems is generally a multi-disciplinary activity requiring several departments to share the responsibility for IT and I&C system security (WINS 2019b). The departments need to work together, communicate regularly and learn from each other. The security department is responsible for protecting the organization from external and internal threats including cyber threats. They set and assess the security policy. The engineering department designs and evaluates the security systems according to the set security principles. The operations department runs the nuclear processes using IT and I&C systems. The IT and I&C systems are maintained by the maintenance department. The IT department manages the office environment. The process control vendors and suppliers play a large role both in the initial implementation of the systems and their maintenance. They need to have a good understanding of security issues, and they need to be effectively managed by the organization that engaged them. However, it is the responsibility of senior management to make organizational and infrastructural decisions considering IT and I&C measures and to allocate the funds necessary to implement them.

The nuclear power plants' external environment ranging from geopolitical changes to international and national regulatory frameworks as well as vendors and suppliers, is relevant to consider when thinking about efficient IMSS.

5.2. Motivations for IMSS

The following motivational factors for the IMSS were presented in the Safety Science (Ylönen et al. 2022) publication and identified in the SAF€RA study. 1) safety and security have mutual interactions and influences (e.g., Song et al. 2019; Kriaa et al. 2015; Pièvre-Cambacédès and Bouissou 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 cyberattack against the nuclear power plant's I&C system (e.g., the Stuxnet computer worm that targeted components also on the SCADA network (WINS 2019b)) 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 (Ylönen et al. 2022). The motivation is well indicated in the IAEA technical report (IAEA 2021a) and in the Finnish regulatory framework (Johansson et al. 2018).

Another motive for integration 2) relates to avoiding conflicts arising from competing logics and related contradictions regarding safety and security. An example of contradictory logic between safety and security management is that the management of safety relies on openness and transparency, whereas the management of security requires the concealment of data and sharing it only between a 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 in the nuclear industry context, where during 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 relevant targets. Thus, promoting safety and security in a high-risk industry requires understanding the contradictory logic of safety and security, and this calls for IMSS.

Still another incentive for integration 3) relates to economic reasons embracing cost-efficiency measures, such as a reduction of administration and audit costs when combining the management of safety and security. In addition, cost benefits can be achieved 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 a cost-benefit and synergy obtained from the IMSS.

Furthermore, a strong justification for integration is that 4) pure safety or pure security approaches cannot identify and mitigate systemic risks or risks to the I&C 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, integrated management is required to identify, assess and mitigate the convergence of different safety and security risks.

These motivations represent an academic understanding of the need for IMSS. They can provide an impetus to IMSS, especially if they are internalized by the organization's leaders.

5.3. Organizational cultural and management perspectives on IMSS

This section presents findings from the interviews and examines them from the organizational culture and integrated management perspectives. Further discussion of results continues in the discussion and conclusions section.

5.3.1. Organizational cultural aspects of IMSS: artifacts, espoused values and underlying assumptions

From the organizational culture perspective, *an artifact,* i.e.*, visible behaviour* in the security domain, includes two different tendencies: one making security (information and cybersecurity) aspects more mundane and shared in the company by providing security training for the personnel and emphasising individuals' responsibility for information

and cybersecurity. However, security training for shop floor workers may repeat the same topics, which can be seen as trivial, such as an emphasis on not opening the links in emails. One power company has adopted a company-level policy that prohibits the use of USB sticks as a means of combating information and cybersecurity risks.

Another tendency is legitimising secrecy, meaning that matters belonging to the security domain cannot be discussed or shared. The interviewees understood and accepted that security aspects involve secrecy, on the other hand some interviewees mentioned that secrecy is seen also as annoying and restrictive. In addition, it was mentioned that it is easy to hide behind the secrecy explanation. In the interviews it was suggested that security aspects should be opened at a general level, for instance by explaining which aspects cannot be asked about or discussed, and why. These kinds of general-level explanations would better meet people's will to know and would provide better understanding about security aspects in the NPPs without harming security. Instead, the interviewees reported that often it is simply stated that a certain topic is a security issue and cannot be discussed. *The espoused value* is that security management belongs to security experts, and many security issues cannot be discussed.

We interpret above mentioned as manifestations of deficiencies in the organizational culture in terms of security aspects and IMSS in the sense that many employees of NPPs acknowledge that security aspects cannot be openly discussed. This may result in some relevant safety-security interfaces remaining unnoticed, unaddressed, or untouched because security experts may not see all the safety implications. Similarly, safety experts do not always receive input from security experts. This may have safety or security effects, and implications for IMSS.

Regarding the safety-security relationship, the interviewees mentioned that historically security has been considered the little brother of safety. In the nuclear context, *the espoused value* is that nuclear safety and radiation safety are the priority, and the physical security, cybersecurity and information security are subordinate to safety. Thus, thinking of safety as a big brother and security as a little brother prevails in the nuclear field. Some interviewees held the view that security aspects served nuclear and radiation safety. Thus, safety is a principal goal and security is just one element that needs to be managed to enhance safety. Similarly, in the safety and security culture context, the *espoused value* is that safety and security cultures are part of the organizational culture. Almost all the interviewees emphasized that the organization does not need a separate concept or framework for addressing security matters. We argue that this espoused value has roots in *underlying assumptions* that safety and security can be developed in parallel within the organizational culture, and that the organizational culture can automatically support strong performance in security, similarly to how it supports the safety culture. Moreover, good security practices were seen to enhance a good safety culture, i.e., as a component of a good safety culture. However, the problem of conceiving of security and safety in this way is that it hampers better understanding, identification, evaluation, analysis, and management of systemic risks. It is exactly in the co-identification of safety and security risks and the subsequent analysis and management of these risks where safety and security domains should meet.

Another concern arising from the separation of safety and security fields, and the subordination of security to safety, is that safety experts or security experts are not necessarily experts in organizational culture. The problem is then how to enhance an organizational culture that promotes IMSS, and a better understanding of converging safety and security risks? What challenges could the interaction between different experts embrace?

Based on the interviews, it was revealed that security experts involve broad range of safety experts in their meetings. As there are several safety domains, this is important. Yet, when the safety culture experts were asked, they stated that they did not participate in security related meetings very much. This we interpret as a deficiency from the IMSS viewpoint. What risks may emerge when safety culture experts and security experts do not meet much? Our interpretation is that from the IMSS point of view, the understanding of each other's' fields may remain superficial, and therefore also the understanding of systemic safety and security risks remains thin, not to mention that the contribution to IMSS remains inadequate. In the discussion section we will raise some potential aspects in which proper collaboration between safety culture and security experts would be relevant.

Considering the safety and security culture, there were somewhat mixed answers. The interviewees stressed that the organizational culture covers both safety and security. The development of a separate security culture was seen as unnecessary, and even harmful from the overall NPP safety perspective. This can be interpreted as a call for IMSS instead of separate safety and security cultures. However, our concern is the big bias between already well-developed safety culture and "unnecessary" security culture. As the safety culture is a well-known concept that is institutionalized in regulations and organizational practices in the NPPs, and it has historically a strong, if not dominant position in organizational culture, it may lead to a situation in which the organizational culture is focused more upon safety than security. This will not contribute to understanding the content of security or understanding convergence of safety and security risks.

We argue that it would be relevant from the organizational culture perspective that the security related culture is acknowledged, recognized, known, supported, and developed. So that it gets strong enough position in the organizational culture.

5.3.2. IT and I&C systems

Even though, I&C and IT systems are separated in the NPPs the interviewees expected that digitalization would increase the cybersecurity challenges. *Espoused value* is that people need to be vigilant in terms of digitalization related cybersecurity risks. For example, managing maintenance and configurations may become more challenging, e.g., during the maintenance it may be possible to insert new vulnerabilities intentionally or unintentionally into the I&C system, e.g., by installing malware in the system or by updating setpoints incorrectly. The maintenance department needs to have an adequate understanding of information security and cybersecurity. Corporate security can provide expert help when needed (Appendix D). In addition to separating, I&C from IT, the resources are separated. Additionally, IT support is separated from IT security. The nuclear power actors are involved in different cybersecurity related networks. There are some wishes to exploit data from I&C for further analysis on the IT side. To enable secure data transfer from the I&C to IT different unidirectional data transfer approaches are being studied.

Based on the interviews, there are some changes in the risk landscape. Cyberattacks are a growing threat, even though direct attacks on I&C have not occurred. Challenges related to non-alcohol intoxicants may increase. There seems to be a slight increase in recreational drug use. Possible legalization of cannabis may further increase such challenges. Even though the threat posed by insiders has not as such increased, it is receiving more attention, e.g., in the form of different analyses.

5.3.3. Structural and functional aspects promoting and constraining IMSS in the regulatory and NPP context

From the *structural integration* perspective in the regulatory context, we can refer to the Nuclear Energy Act (990/1987) that states that STUK supervises all aspects of 3S, i.e., safety, security, and safeguards. This was considered beneficial by interviewees, as delegating all 3S oversight responsibilities to the same authority contributes to better understanding of safety-security interfaces within the regulatory body. In addition, our interpretation is that the regulatory body can also contribute to integrated management in NPPs by providing regulatory guidelines which affect the NPP management of the safety-security interface. In comparison to international practices, often the supervision of 3S is more fragmented, as different state agencies take care of different

domains, e.g., safety may belong to nuclear regulators, whereas safeguards may belong to the foreign ministry. In that sense, the Finnish system is more integrated as the supervision of all these 3S aspects belongs to the STUK. However, inside the STUK there are separate units that manage these three domains. Thus, functionally (i.e., how safety and security management is combined and coordinated in practice), the management of safety, security and safeguards is separated into different units in the STUK.

Regarding the IMSS, the interviewees emphasised that one company cannot manage safety-security interface alone. Effective IMSS requires collaboration with external companies. The National Cyber Security Center, and special arrangements within a country with other nuclear power plants and other relevant actors help in gaining situational awareness.

The *structural integration* was manifested in NPPs so that safety unit also included corporate security, including cybersecurity and physical security. From the functional integration perspective, in NPPs the line organization has the responsibility for the management of 3S. However, the different sectors of 3S have their own management models and principles, which can lead to a silo effect. An example of different management models and principles is that safety management is based on the principles of openness, transparency, and a questioning attitude, whilst in security management the sharing of information is possible only within the small group of security experts. From the point of view of *functional* management, it would be important to explain the difference between the safety management and security management principles, so that people would understand them. This would enable a better implementation of IMSS so that safety is not developed at the expense of security and vice versa.

An example of *functional integration* is that the responsible leader of an NPP should have the overall picture of 3S. However, it is possible to ask whether this picture is formed just by picking the main knowledge from security and safety specialists from different domains. From the IMSS perspective, the ideal way would be close collaboration between different safety and security experts and co-construction of knowledge related to safety and security, such as co-identification of safety and physical security and cybersecurity risks, and co-assessment of risks in coordinated ways. However, based on our interviews, despite the regular meetings with different safety and security experts, these kinds of practices, such as co-identifying risks in the same models are not in use. Thus, our interpretation is that the management of the safety-security interface would require further development from the functional perspective, and especially from the collaborative risk identification and risk assessment viewpoint.

6. Discussion and conclusion

The importance of managing the safety-security interface is acknowledged in the nuclear industry globally. However, the current state of IMSS varies between countries and nuclear power plants. This study focused on the Finnish nuclear community but provides some general comments on the current state of IMSS in the nuclear industry globally.

Integrated management was approached from the structural, functional, and cultural perspectives (Jørgensen et al. 2006) as well as examining it as an organizational cultural model, based on artifacts, espoused values and underlying assumptions (Schein 2010).

From the structural perspective, the IAEA technical reports and Finnish nuclear regulatory framework promote the understanding of safety-security interface. Both aim at better integration of safety and security throughout the whole lifecycle of the nuclear power plant. However, from the functional point of view the interviews revealed the lack of some important practices which would contribute to IMSS, such as continuous co-identification and co-assessment of safety and security risks. The situation is the same in Seveso plants according to the SAF€RA study, which identified that safety and security risks are identified and assessed separately, and that common risk identification practices are lacking. However, coordination and better integration of safety and security would be relevant for a better understanding and preparing for systemic risks and their management (Ylönen et al. 2022).

There are some developed risk analysis tools, which facilitate co-identification and co-assessment of safety and security risks, and which would help the line organization that is responsible for 3S, and the responsible manager to obtain an overall picture of 3S related risks. These tools include the **PHAROS** (Process Hazard Analysis of Remote manipulations through the cOntrol System) tool which was developed in the SAF€RA project to identify scenarios that can potentially originate from malicious manipulations, which may lead to major events (Iaiani et al., 2021b). 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. This also promotes functional integration in terms of co-identification and co-assessment of risks. In addition, the close collaboration of different experts has obvious effects on the organizational culture, such as the adopted values (espoused values), such as the need to respect the knowledge and opinions of other experts and to have a continuous dialogue with them. Moreover, PHAROS could contribute to IMSS in its deepest level, i.e., cultural level that refers to learning from co-assessment of systemic risks, and better understanding of the importance of IMSS.

Furthermore, PHAROS would be suitable for a systemic understanding of safety and security risks as it enables the recognition of risks that could otherwise be disregarded, e.g., risks that could be deemed unlikely in the safety assessment or which would be considered out of its scope. For instance, PHAROS could include risks originating from malicious intents. In addition, external risks, such as geopolitical changes and their effects on, e.g., the increase in cyber-attacks on NPPs or difficulties in obtaining spare parts, have direct or indirect effects on the safe operation of the nuclear facility. These external threats could be included in PHAROS. As Pharos is a new method, it has not yet been used or tested in practice (see Iaiani et al., 2021b; Ylönen et al. 2022). Pharos could be tested in a NPP context.

However, in order to be effective, PHAROS and other developed risk analysis tools (see Iaiani et al., 2021b) for co-identification and co-assessment of safety and security risks would require sufficient organizational support behind them.

Based on this study, we argue that despite the structural support for integration, and obvious motivational aspects to better understand systemic risks, the functional and cultural support is inadequate in the power plants under study.

What prevents integration are the mindset and organizational cultural aspects, including artifacts, espoused values, and underlying assumptions (Table 2). The artifacts refer to visible processes, and practices, such as the already mentioned safety and security risk identification, which maintains separation. In addition, different management principles in security (secrecy) and safety (openness and transparency) may not facilitate the exchange of information between the two domains. Espoused values include goals and rationalizations, such as categorical denial of the need for a separate security culture, and seeing the nuclear and radiation safety, or overall safety as a priority, to which security aspects are subordinated. This thinking emphasizes overall safety as the main goal, and therefore a separate security culture is not promoted, but is seen even to be detrimental to overall safety. Good security practices are seen as supporting a good safety culture.

However, we argue, that this subordination of security to safety is problematic because there is a bias between safety and security. Necessary security-related practices may remain underdeveloped, whereas the safety culture is relatively well developed. The concern is that the security-content is not well understood by safety and safety culture experts, and this may prevent efficient learning from security in the nuclear power plants. In addition, current practices do not

adequately contribute to a systemic understanding and understanding of the convergence of security and safety risks.

In addition, the underlying assumption includes seeing organizational culture as an umbrella under which safety and security can be combined neatly and in a balanced way, almost automatically. We see this as problematic, as it is difficult to see how safety and security aspects could be combined under an organizational culture if there is no developed security culture, and when safety culture experts are not experts on security issues, and security experts are not usually experts on organizational culture.

The thinking that safety and security can be developed in parallel within the organizational culture framework may be harmful from the overall safety and IMSS viewpoint, as the organizational culture as a conceptual framework and in current practice does not contribute to a better understanding of security or IMSS. In addition, the security content often remains thin, less known, and it is trusted that the security experts will take care of it themselves as they cannot disclosure many issues. This may prevent the relevant exchange of information between safety and security experts and learning from each other.

What keeps these safety and security domains apart relates also to different logics between these domains, as safety management adheres to openness and transparency and a questioning attitude, while the security management resorts to secrecy. In addition, the safety and security domains have their own specialized experts with their own disciplinary frameworks, which makes collaboration and communication challenging. Thus, IMSS is not currently adequately developed in the current NPPs.

IMSS would require the efficient exchange of information and communication between safety and security experts, between organizational units. Single meetings alone between the experts do not promote IMSS. Furthermore, IMSS would require resources from the organization, for instance in terms of creating new competences, and arenas to discuss the safety-security interface.

What would be required would be the need to think beyond safety and security expert frameworks, collaboration across organizational and disciplinary boundaries to co-create understanding of emerging safety and security risks, and fresh organizing of management and related responsibilities. We argue that security requires attention so that IMSS can be developed. It is true that both safety and security domains need their own special expertise, and this needs to be acknowledged. However, in addition to that, especially the broad co-identification of risks, and co-assessment of risks would be needed.

We have identified some potential aspects in which proper collaboration between safety culture and security experts would be relevant. These include training, and learning from incident investigations and good practices, planning tailor-made security education for people acting in different positions in the organization, supporting the development of the co-identification of safety, physical security, and cybersecurity risks, as well as the development of mindfulness in terms of technology and software providers, to be prepared to understand the risks related to their interests. However, all these would require close collaboration and that safety culture experts should have a better understanding of the main differences, conflicting aspects, as well as similarities between safety and security at the general level. Safety culture experts could help to provide adequate general level explanations as to why certain aspects are secret and cannot be disclosed.

In addition, the regulatory bodies could enhance IMSS by carrying out joint inspections with other regulators, and by asking about IMSS during their inspections, and by providing some criteria for assessing the quality of integration in NPPs. Moreover, the power companies and the regulator could also develop deeper functional integration of safety and security in their own organizations.

The underlying assumption of organizational culture as an adhesive mechanism between safety and security is not adequate to make the content of security and safety domains visible and clear or contribute to their better coordination. This study also raises the need for further research into how the co-construction of knowledge about the safety-security interface could be enhanced, and how the organizational culture could best contribute to better coordination of safety-security management.

We conclude that the current organizational structures, functions, and cultures contribute only lightly to IMSS in nuclear power plants. Safety and security are managed by different principles, experts, and units in the organization. In addition, safety whether overall safety, or radiation and nuclear safety, and the safety culture play a relevant role in the organizational culture, whilst security is still in the position of a little brother in relation to safety. This study provides a tentative understanding of IMSS in the nuclear context. The results are similar also in the other high-risk industries, such as Seveso plants (Ylönen et al. 2022). More efforts to promote IMSS are needed both at the institutional level, including legislation and standards, as well as at the organizational level including their structures, functions and cultures.

Finally, there is a need for further research on IMSS regarding comparisons between countries and between nuclear power plants. It would be interesting to examine the differences between safety and security cultures and their relationship within the framework of organizational culture in one company and in several companies. In addition, further research would be needed on the risk identification and risk assessment practices and how safety and security risk analysis could be combined, e.g., by testing the new methods, such as the PHAROS method developed in the SAFЄRA research project (Iaiani et al. 2021b; Ylönen et al. 2022).

CRediT authorship contribution statement

Marja Ylönen: Writing – original draft, Project administration, Methodology, Investigation, Formal analysis, Conceptualization. **Kim Björkman:** Writing – original draft, Investigation.

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

This paper is part of the Development of Framework of Overall Safety (OSAFE) research project and it was funded by the Finnish Research Programme on Nuclear Power Plant Safety 2018-2022 (SAFIR 2022)

Appendix A. The core concepts and their definitions

See Table 1.

Appendix B. Information about the interviewees and the interview themes (including some questions)

Interviewees

3 security managers, working with the cybersecurity, physical security and nuclear security fields.These security experts had 10–20 years' experience with working with nuclear security field. They worked in the middle management or leading positions.

3 safety experts, who had over 20 years' experience in working with nuclear safety and safety culture fields. These people worked in the principal advisor and middle management positions.

Interview themes and questions

1. **Background Information** (education, position, experience in working with nuclear industry)

a. What is your education?
b. What is your position in the organization?
c. How does your work relate to safety/security/cybersecurity?
d. How long have you worked in the current organization?

2. **Corporate security**
   a. What belongs to corporate security?
   b. How is it organized?
   c. How is its relationship to other safety and security areas?
   d. What is the ideal background for the person who is responsible for corporate security?
3. **Situational awareness of safety and security risks**
   a. How does your organization keep itself aware of the actual safety/security/cyber security situation?
   b. What kind of external (governmental) organizations, consultants, etc. do you collaborate with in order to get proper understanding of the security situation?
   c. What kind of practices, forums, or methods do you use for maintaining security situation awareness?
4. **Changes in the risk landscape, digitalization and automation in the nuclear industry (IT I&C)**
   a. What types of changes has occurred in the risk field?
   b. How is the relationship between IT and I&C?
   c. How is the IT-I&C relationship managed?
   d. How are (cyber)security induced threats to I&C managed by your organization?
5. **Security & cybersecurity risks**
   a. How do you define security?
   b. How is security (physical security or cyber security) taken into account in risk assessment? (methods?)
   c. What are typical security risks in your company?/ or in the industry?
   d. What are the main concerns related to security risks in your company?
6. **The relationship between safety and security**
   a. How would you see the relationship between safety and security?
   b. What are the main differences between safety and security management?
7. **IMSS, management of safety-security interface, current structures and functions (practices)**
   a. Why IMSS is needed?
   b. How are safety and security (physical security and cybersecurity) managed in your company?
   c. How are these safety, security and cybersecurity organized in your company, under which departments?
   d. What kinds of practices belong to IMSS?
   e. How do safety and security experts collaborate?
   f. How do you identify and conduct risk assessments? Do you co-identify or co-assess risks?
   g. What kind of challenges you can find in management of safety-security interface?
   h. What would be required from an efficient IMSS?
8. **The relationship between safety culture- security culture**
   a. Does your company/organization have a security culture?
   b. Would you see it beneficial to have a security culture? (why?/ why not?)
9. **How security-safety-safeguards and their management is in contradiction with each other?**
10. Other?

Appendix C. information about the literature review on safety and security concepts and integrated management based on SAF€RA study (Ylönen et al. 2021) and description of SAF€RA interviews.

As secondary data the study uses the literature review on safety and security concepts and (integrated) management that was conducted in connection of the SAF€RA 4STER study on the IMSS in Seveso plants. The key words "safety and security" were used in the search for articles from the Safety Science, Reliability Engineering and System Safety, the Journal of Loss Prevention in the Process Industries, and Process Safety Progress.

There were 2 searches for Safety Science, and they cover the period of May 31, 2009 – June 3, 2019. In the first search, the titles of the articles were searched with the keywords safety and security. In the second search, abstracts were searched using the same keywords. In the first search 9 hits were found and in the second search 29 hits were found. 13 articles were gathered for the reading because of their relevance for the industrial safety and security, or the concepts and management of safety and security. Further reading showed relevance of 9 articles.

Regarding the other journals, these were approached similarly by using the keywords safety and security. The articles that were not relevant from the point of view of the concepts or management of safety and security, or industrial safety and security were excluded. 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 and Pettersen Gould, 2020; Nolan 2015; Smith and Brooks 2012; Borodzicz 2005). Thus, total number of reviewed literature included 31 artic.es, four reports in in the nuclear context regarding cybersecurity, computer security, as well as security culture; and four books.

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 SAF€RA 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. 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. (Ylönen et al. 2022).

The results of the SAF€RA interviews together with this study provide information about the needs and challenges regarding IMSS in the high-risk industry.

Appendix D. Interviewees' expectations for the expertise of the person responsible for corporate security

In the Finnish power companies, corporate security is defined similarly to the Confederation of Finnish Industries' (EK 2021) concept of corporate security. Corporate security constitutes the security of all functions of a corporation including the physical security, cybersecurity, and environmental security. Based on the interviews, no specific education or work background was emphasized for a corporate security manager. Some sort of corporate security background was considered beneficial, and the manager should have the skill to perceive dependencies between different security and safety domains. In several answers, NPP-related business knowhow was emphasized, whereas a police or military background was not considered as optimal, since they may not have sufficient business knowhow. However, some interviewees considered that it would be beneficial if the security manager of the operative unit had a police or military background because the operative models and plans are based on the approved operative models of the police or other authorities. Both security measure and cybersecurity knowhow are needed.

The study is inspired by the change in the risk landscape caused by the development of digitalization and automation in the high-risk industry. The increasing convergence of process-safety, physical security, and cybersecurity risks can lead to major accidents. Integrated management of safety and security (IMSS) is a necessary means of preventing and preparing for accidents. The objective of this paper is to get new insights into the current state of IMSS and related challenges in the nuclear industry. The data includes the International Atomic Energy Agency (IAEA) and World Institute for Nuclear Security (WINS) reports, articles on digitalization, IMSS, and interviews with safety and security experts from two power companies and the Radiation and Nuclear Safety Authority in Finland. The paper compares the results with those in Seveso installations. The methods are thematic and qualitative content analysis. Theoretical framework consists of organizational culture and management perspectives. The paper provides new meanings to the ways in which IMSS is currently implemented. The paper shows the IAEA structural support to IMSS, differences in IMSS implementation in the nuclear industry, and organizational cultural aspects that constrain the IMSS. The latter include the subordination of security to safety, the assumption that organizational culture automatically integrates safety and security, the lack of co-identification and co-assessment of safety and security risks, which prevents a better understanding of systemic risks. The conclusion is that the current state of IMSS is not adequate to address converging, systemic risks, and coordination of safety and security aspects requires more attention.

References

Alvesson, M., Sveningsson, S., 2015. Changing organizational culture. Cultural Change Work in Progress. Routledge, London.

Aven, T., Ylönen, M., 2018. A risk interpretation of sociotechnical safety perspectives. Reliab. Eng. Syst. Saf. 175, 13–18.

Aven, T., Ylönen, M., 2021. How the risk science can help us establish a good safety culture. J. Risk Res. https://www.tandfonline.com/doi/full/10.1080/13669877.2020.1871056.

Aven, T., 2019. The Science of Risk Analysis: Foundation and Practice (1st ed.). Routledge. https://doi.org/10.4324/9780429029189.

Baylon, C., Brunt., R., Livingstone, D., 2015. Cyber Security at Civil Nuclear Facilities. Chatham House. The Royal Institute of International Affairs. UK.

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.

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

Boyes, H., Hallaq, B., Cunningham, J., Watson, T., 2018. The Industrial Internet of things (IIoT): An analysis framework. Computers in Industry, 101, 1-12. https://doi.org/10.1016/j.compind.2018.04.015.

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

Cameron, K.S., Quinn, R.E., 2011. Diagnosing and Changing Organizational Culture: Based on the Competing Values Framework, 3rd ed. Jossey-Bass, San Francisco.

Collins, S., McCombie, S., 2012. Stuxnet: the emergence of a new cyber weapon and its implications. J. Polic. Intell. Count. Terror. 7, 80–91. https://doi.org/10.1080/18335330.2012.653198.

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.

Edwards, J.R.D., Davey, J., Armstrong, K., 2013. Returning to the roots of culture: a review and re-conceptualisation of safety culture. Saf. Sci. 55, 70–80. https://doi.org/10.1016/j.ssci.2013.01.004.

EK, 2021. Yritysturvallisuus, Confederation of Finnish Industries, (available only in Finnish) https://ek.fi/hyotytietoa-yrityksille/yritysturvallisuus/ (accessed 22.11.2021).

Glesner, C., Van Oudheusden, M., Fallon, C., Turcanu, C., 2020. Bringing symmetry between and within safety and security cultures in high-risk organizations. Saf. Sci. https://doi.org/10.1016/j.ssci.2020.104950.

Grote, G., 2012. Safety management in different high-risk domains – All the same? Saf. Sci. 50, 1983–1992.

Grote, G., Künzler, C., 2000. Diagnosing of safety culture in safety management audits. Safety Science. Volume 34, Issues 1–3, 2000, Pages 131-150.https://doi.org/10.1016/S0925-7535(00)00010-2.

Guldenmund, F.W., 2010. (Mis)understanding safety culture and its relationship to safety management. Risk Anal. 30 (10), 1466–1480. https://doi.org/10.1111/j.1539-6924.2010.01452.x.

Guldenmund, F.W., 2000. The nature of safety culture: a review of theory and research. Safety Science, Volume 34, Issues 1–3, 2000, Pages 215-257, ISSN 0925-7535, https://doi.org/10.1016/S0925-7535(00)00014-X.

Hänninen, V., 2016. Kuinka paljon on tarpeeksi? Aineiston määrä laadullisessa tutkimuksessa. Aikuiskasvatuksen tutkimusmenetelmiä. Aikuiskasvatus, 36 (2), 109-113. (How much is enough? The quantitiy of data in qualitative research). **DOI:** https://doi.org/10.33336/aik.88484.

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.

Haukelid, K., 2008. Theories of (safety) culture revisited—An anthropological approach. Saf. Sci. 46, 413–426. https://doi.org/10.1016/j.ssci.2007.05.014.

Henriqson, E., Schuler, B., Winsen, R., Dekker, S., 2014. The constitution and effects of safety culture as an object in the discourse of accident prevention: a Foucauldian approach. Saf. Sci. 70, 465–476. https://doi.org/10.1016/j.ssci.2014.07.004.

Holappa, J., Valkama, R., 2017. Kyberturvallisuus on erottamaton osa ydinturvallisuutta. (Cybersecurity is inseparable part of nuclear safety). In ATS Ydintekniikka 2, (46), 23–25.

Iaiani, M., Tugnoli, A., Bonvicini, S., Cozzani, V., 2021a. 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., 2021b. 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.

INTERNATIONAL ATOMIC ENERGY AGENCY, 1991. Safety Culture, Safety Series No. 75-INSAG-4, IAEA, Vienna.

INTERNATIONAL ATOMIC ENERGY AGENCY, 2008. Nuclear Security Culture. Implementing Guide. IAEA Nuclear Security series No. 7. IAEA, Vienna.

INTERNATIONAL ATOMIC ENERGY AGENCY, 2011. Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants. IAEA Nuclear Energy Series NP-T-3.12. IAEA Vienna.

INTERNATIONAL ATOMIC ENERGY AGENCY, 2016. Leadership and Management for Safety. IAEA Safety Standards Series No. GSR Part 2. IAEA, Vienna.

INTERNATIONAL ATOMIC ENERGY AGENCY, 2017. Self-assessment of Nuclear Security Culture in Facilities and Activities, Technical Guidance. IAEA Nuclear Security Series No. 28-T. IAEA Vienna.

INTERNATIONAL ATOMIC ENERGY AGENCY (2018a). Approaches for Overall Instrumentation and Control Architectures of Nuclear Power Plants. IAEA Nuclear Energy Series, No. NP-T-2.11, IAEA.

INTERNATIONAL ATOMIC ENERGY AGENCY, 2018b. Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T, IAEA, Vienna (2018).

INTERNATIONAL ATOMIC ENERGY AGENCY, 2021b. Enhancing Nuclear Security Culture in Organizations Associated with Nuclear and Other Radioactive Material, Technical Guidance, IAEA Nuclear Security Series No. 38-T. IAEA, Vienna.

INTERNATIONAL ATOMIC ENERGY AGENCY, 2021a. The Nuclear Safety and Nuclear Security Interface: Approaches and National Experiences, Technical Reports Series No. 1000, IAEA, Vienna (2021).

INTERNATIONAL ATOMIC ENERGY AGENCY, 2010. The Interface Between Safety and Security at Nuclear Power Plants. INSAG Series No. 24, IAEA, Vienna.

ISO/IEC 27032:2012. Information technology — Security techniques — Guidelines for cybersecurity.

Johansson, M., Järvinen, M.-L., Karhu, P, Niemelä, I. and Routamo, T., (2018). Use of nuclear energy and safety-security interface in the Finnish regulatory framework. Presented in IAEA Technical Meeting on the Safety and Security Interface – Approaches and National Experiences 29.10.–1.11.2018.

Jørgensen, T.H., Remmen, A., Mellado, M.D., 2006. Integrated management systems - three different levels of integration. J. Clean. Prod. 14 (8), 713–722.

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. Sage Publication, California; CA.

Leavy, P., 2020. The Oxford Handbook of Qualitative Research. Oxford University Press, New York.
Linnosmaa, J., Papakonstantinou, N., Malm, T., Kotelba, A. and Pärssinen J., 2021. Survey of cybersecurity standards for nuclear instrumentation and control systems, International Symposium on Future I&C for Nuclear Power Plants, ISOFIC 2021: Proceedings. Okayama University, 2021.
Maxwell, J.A., 2012. A realist approach for qualitative research. Sage, Thousands Oaks.
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.
Pidgeon, N.F., 1991. Safety culture and risk management in organizations. J. Cross-Cultural Psychol. 1991;22(1):129-140. https://doi.org/10.1177/0022022191221009.
Pièrre-Cambacédès, L., Bouissou, M., 2013. Cross-fertilization between safety and security engineering. Reliabil. Eng. Syst. Saf. 110 (2013), 110–126. https://doi.org/10.1016/j.ress.2012.09.011.
Reiman, T., Rollenhagen, C., Pietikäinen, E., Heikkilä, J., 2015. Principles of adaptive management in complex safety–critical organizations. Safety Science, Volume 71, Part B, 2015, Pages 80-92, ISSN 0925-7535, https://doi.org/10.1016/j.ssci.2014.07.021.
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., 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. Clean. Prod. 19, 1239–1249. https://doi.org/10.1016/j.jclepro.2011.03.002.
Reniers, G., Khakzad, N., 2017. Revolutionizing safety and security in the chemical and process industry: applying the CHESS concept. J. Integrat. Secur. Sci. 1, 2–15. https://dx.doi.org/10.18757/JISS.2017.1.1547.
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.
Schein, E.H., 1992. Organizational culture and leadership, 2nd ed. Jossey-Bass, San Francisco.
Schein, E.H., 2004. Organizational culture and leadership, 3rd ed. Jossey-Bass, San Francisco.
Schein, E.H., 2010. Organizational culture and leadership, 4th ed. Jossey-Bass, San Francisco.
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.
Silbey, S.S., 2009. Taming Prometheus: Talk About Safety and Culture. Annual Review of Sociology 2009 35:1, 341-369. https://doi.org/10.1146/annurev.soc.34.040507.134707.
Smith, C., Brooks, D.J., 2012. Security Science: The theory and practice of security. Butterworth-Heinemann.
Society for Risk Analysis, 2018. Society for Risk Analysis Glossary, available at https://www.sra.org/wp-content/uploads/2020/04/SRA-Glossary-FINAL.pdf (accessed 30.11.2021).
Song, G., Khan, F., Yang, M., 2019. Probabilistic assessment of integrated safety and security related abnormal events: a case of chemical plants. Safety Science, Volume 113, 2019, Pages 115-125, ISSN 0925-7535, https://doi.org/10.1016/j.ssci.2018.11.004.
Stacey, R., 2012. Tools and Techniques of Leadership and Management: Meeting the Challenge of Complexity (1st ed.). Routledge. https://doi.org/10.4324/9780203115893.
Swartz, G. (Ed.), 2000. Safety Culture and Effective Safety management. National Safety Council Press, Chicago, Ill.
Vaismoradi, M., Jones, J., Turunen, H., Snelgrove, S., 2016. Theme development in qualitative content analysis and thematic analysis. J. Nurs. Educ. Pract. 6, 100–110. https://doi.org/10.5430/jnep.v6n5p100.
WENRA, 2019. Interfaces between Nuclear Safety and Nuclear Security. Report 10 April 2019. Western European Nuclear Regulators Association, available at https://www.wenra.eu/sites/default/files/publications/report_interfaces_between_nuclear_safety_and_nuclear_security.pdf (accessed 18.5.2022).
WINS, 2019a. International Best Practice Guide 4.2 An Integrated Approach to Nuclear Safety and Nuclear Security. Version 2.1, ISBN: 978-3-903191-50-1, Available to WINS Members at www.wins.org.
WINS, 2019b. International Best Practice Guide 4.3 Security of IT and IC Systems at Nuclear Facilities. Version 3.1, ISBN: 978-3-903191-51-8, Available to WINS Members at www.wins.org.
Ylönen, M., Nissilä, M., Heikkilä, 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 (SAFЄRA 4STER): Final Report. VTT Technical Research Centre of Finland. VTT Technology No. 386 https://doi.org/10.32040/2242-122X.2021.T386.
Ylönen, M., Tugnoli, A., Oliva, G., Heikkilä, J., Nissilä, M., Iaiani, M., Cozzani, V., Setola, R., Assenza, G., van der Beek, D., Steijn, W., Gotcheva, N., Del Prete, E., 2022. Integrated management of safety and security in Seveso sites – sociotechnical perspectives. Saf. Sci. 151, 105741 https://doi.org/10.1016/j.ssci.2022.105741.
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.