Safety and Security: A cross-professional comparison

Riana Steen

BI Norwegian Business School, Norway. E-mail: riana.steen@bi.no

Hugo Ribeiro

ICL Group, Brazil, E-mail: hugo.ribeiro@icl-group.com

Anurag Shukla

GlobalConnect, Norway, E-mail: anurag.shukla@globalconnect.no

From the theoretical perspectives, traditionally, safety and security represent different contexts, which challenges exchanging ideas, methods, and results between these two scientific fields. Therefore, a distinction between these two contexts, based on the intentionality behind unwanted events, the way risk is understood, and the methods used to assess and manage risk in these contexts. From the practical point of view, distinguish between the roles and responsibilities of these two professional communities are unclear. This study explores the extent of the commonalities and differences in safety and security professionals' current stage. We conduct a qualitative analysis based on 28 semi-structured interviews with the safety and security domain professionals, focusing on the conceptual narratives, responsibilities, and risk assessment approaches from a practical perspective. Our findings indicate that while the professionals in these two fields strongly distinguish between the context of their activities, they share many commonalities regarding their day-to-day tasks. A fundamental common problem in managing risk is that it is difficult to express uncertainty and determine how likely it is that an incident/event happened; we are unable to give strong arguments for specific likelihood assignments of threat occurrence. Yet, a likelihood can always be assigned based on available knowledge. A holistic risk management approach, integrating risk- and resilience-based thinking, acknowledges this and considers a set of qualitative and quantitative methods to reflect this (lack of) knowledge.

Keywords: safety and security, Security, Security professionals, Safety professional, Resilience-based risk management, increase preparedness.

1. Introduction

A considerable body of academic literature in the security management system argues that the safety concept does not capture all security settings. Thus, they separate these two fields (Ganin et al., 2017) and argue for considering security as "an independent science, detached from the safety science" (Jore, 2019). Their rationales are built on the intentionality behind unwanted events, how risk is understood, and the methods used to assess and manage risk in these contexts. Analyze and manage risk, either in the safety or security context, requires an approach or framework defining what risk is and how risk should be assessed and handled. Many such approaches and frameworks exist. For instance, (Renn 2008, 2020) introduces a classification structure based on disciplines and perspectives. He distinguishes between statistical analysis, epidemiology, probabilistic risk analysis, the economics of risk, the psychology of risk, natural hazards and cybersecurity.

To solve practical problems, several of these perspectives are required. Besides, Aven (2017) highlights the importance of "robust thinking", the quality discourse and organizational learning (in terms of collective mindfulness) in managing surprises and black swan's types of events. Robust thinking reflects on the "thinking about risk that sees beyond the probabilistic perspective."

Consider a risk scenario with the potential for extreme consequences and where the uncertainties are immense, for instance, the wake of an insider threat. Three main aspects of an insider threat are as follows: the threat actor's intention to conduct a malicious act, the perpetrator's capability and competence for carrying out a malicious plan, and an opportunity to be exploited by the perpetrator (there may also be an absence from doing one's duties intentionally or unintentionally, i.e., locking the warehouses when leaving the working day, so that intrusion easily carried). Using the statistical approach (including the probabilistic risk analysis) to determine the risk level in this example has its limitation. An underlying assumption in statistical methods is that sufficient data can predict future performance, and systems are tractable. This means that how a system works is known, and that the subsystems' details and descriptions are uncomplicated and that systems do not change while they are being described (Braithwaite, Wears & Hollnagel, 2015; Patriarca, Costantino, Falegnami, & Bilotta, 2018; Provan, Woods, Dekker & Rae, 2020).

However, an insider threat has a complex nature of concern in both safety and security. For instance, while the intention behind such an act is malicious, it might be deficient in the system design, making it vulnerable to such a scenario. Another possibility is that various violations, including situational, routine, and organizationally induced violations, might unintentionally provide such an attack opportunity. The organizationally induced violations occur when "an organization attempts to meet increased output demands by ignoring or stretching its safety defenses" (ICAO, 2012).

Proceedings of the 31st European Safety and Reliability Conference
Edited by Bruno Castanier, Marko Cepin, David Bigaud, and Christophe Berenguer
Published by Research Publishing, Singapore.
ISBN: 978-981-18-2016-8; doi:10.3850/978-981-18-2016-8_091-cd

This example highlights that turbulent changes, growing complexities and interdependencies across organizations, and increasing uncertainty levels have created a grey zone between the safety and security field. The threat vectors are interwoven. In this zone, dealing with challenges is beyond the boundaries of traditional safety or security approaches. We need to see beyond the conventional safety approaches' results based on the historical data and the expected net present value calculations. Risk perception, social concerns, and cultural aspects of risk are important for the risk management system (governance) and the safety and security management system.

While keeping in mind the arguments mentioned above, we shift our attention from the theoretical perspective to the realistic view in this paper. We address the following research question:

RQ: How the practitioners of safety and security distinguish these two fields in their day-to-day activities?

We believe this question's answer contributes to safety and security science in developing appropriate guidelines that support professionals in conducting their daily tasks. The remainder of the paper is organized as follows. Section 2 briefly presents the theoretical background for this study, including the fundamental safety and security management concepts. Section 3 outlines the methodology for exploring our research question. Then, in Section 4, we summarise our findings and discuss how a more holistic approach to safety and security management might enhance practitioners' capacity in conducting their daily tasks. Finally, Section 5 concludes and provides recommendations for further research.

2. Safety and security professional: A theoretical view

This section compares safety and security professionals concerning the conceptual narratives, risk assessment approaches, and the risk management process.

2.1 *Safety management*

The International Organization for Standardization (ISO 31000) defines safety as "a condition or set of circumstances, where the likelihood of negative effects of uncertainty on objectives is low". In its traditional way, the so-called Safety-I, this definition links the safety concept to a condition where "as few things as possible go wrong". Thus, the safety management system aims to avoid things going wrong (Hollnagel, 2014). As an alternative approach, modern safety management relies on safety as a condition where "as many this as possible go well" (Safety-II). The underlying idea of Safety-II is that "we cannot make things go right simply by preventing them from going wrong" (ibid). In the same field, it has been argued that a traditional Safety-I perspective might be appropriate and effective until system complexity is limited in terms of interactions and couplings among different system agents and components (Patriarca et al., 2016). In dealing with complexities, in line with risk- and resilience-based thinking (Aven, & Thekdi, 2018), the Safety-II approach is considered necessary based on the following assumptions (Hollnagel, 2014):

- Systems cannot be decomposed in a meaningful way
- Everyday performance is flexible and variable, i.e., system functions are not bimodal
- Success, as well as failures, is a result of human performance variability.
- Even though some outcomes can be interpreted as linear consequences of other events, some events result from coupled performance variability.

As a part of the safety management system, the risk assessment process focuses on accidents caused by failures and malfunctions and aims to identify causes and contributory factors. Its rationality is based on a causality credo, i.e., a cause logic, based on the following arguments (Hollnagel, 2014, p. 63):

The causes for that thing go right or wrong are different. The reason for adverse outcomes (accidents, incidents) is that something has not functioned as it should. Similarly, the reason for successful outcomes is that everything worked as it was supposed to do. As the undesirable consequences have causes, it must be possible to figure out these causes by collecting enough evidence. The identified causes can be eliminated, encapsulated, or otherwise neutralized to reduce the number of adverse outcomes and improve safety. To this end, handbooks and organizational procedures provide work descriptions that constitute an imagined variety of work domains, i.e. Work-As-Imagined (WAI). However, when an event happens, dealing with the challenges sharp-end require different degrees of adaptation. This point implies that the real actions are inescapably different from the WAI, constituting another variety of work named Work-As-Done (WAD) (Steen et al., 2021).

The risk assessment process can be subdivided into various categories, simplified, standard, and model-based (Aven, 2008):

- Simplified risk assessment is a less formal approach using brainstorming and group discussion to establish the risk picture. The process is qualitative.
- Standard risk assessment, a more formalized approach using established techniques for hazard identification (HAZID, HAZOP, crude risk assessments, etc.). This approach is qualitative or quantitative (or a combination), using risk matrices with defined risk categories to map the risk picture and results.
- Model-based approach, which is primarily a quantitative approach. This approach applies Probabilistic Risk Assessment (PRA) methods (for example, the Poisson model), techniques such as fault tree analysis (FTA) and event tree analysis (ETA), as well as more advanced physical models of phenomena and processes such as fires and explosions. Also, models such as Hazard Analysis and Critical Control Points (HACCP), Failure Mode and Effect Analysis (FMEA), Hazard and Operability Studies (HAZOP) are commonly included in the assessment.

Among these approaches mentioned above, the PRA is the most commonly used to evaluate risks in safety management. It is a formalized quantitative decision-support tool built to estimate probabilities and expected values for attributes like injuries, loss of lives, environmental damage or reputational damage. PRA has been widely used in different sectors over the past 40 years. The assessments originated in the aerospace and nuclear industries but are now also common in many other sectors, including healthcare (Broekhuizen et al., 2015), pharmacology (Tardieu, Simonneau, & Muller, 2018), Chemical (Ricardez-Sandoval, 2012), and the oil & gas industry (Mujeeb-Ahmed, Seo, & Paik, 2018).

The main steps of a PRA are the identification of initiating events, cause and consequence analysis, and risk description. The assessment focuses on basic techniques such as Fault Tree Analysis (FTA) and Event Tree Analysis (ETA). Besides, models for Human Error Analysis (HRA) are commonly included in the assessment. The risk estimation utilizes both an objective approach (based on hard data) and a subjective approach (based on expert judgments). The motivation for conducting a PRA is decision support on the choice of arrangements and measures. By measuring risk, the decision-maker is informed. In the design phase of a system, the PRA can, for example, guide what accidental loads the system should withstand. In operation, the PRA can signify which maintenance measures have an immense impact on risk.

One of the critical terms in the safety management system is robustness (antonym: vulnerability) refers to the insensitivity of performance to deviations from normal conditions. Measures to enhance robustness include incorporating safety factors as an assurance against functional variation. Other measures could be different types of barriers, introducing redundant and diverse safety devices to improve structures against multiple stress situations. Establishing building codes to protect against natural hazards and improving the organizational capability to initiate, enforce, monitor, and revise management actions (high reliability, learning organizations) are also among measures to improve a system's robustness.

2.2. *Security risk management*

A typical definition of security is a "condition/set of circumstances where the likelihood of intentional negative effects on objectives is low", as proposed by Blokland and Reniers (2020). There is an involvement of multiple parties in such a setting, with malicious intentionality and hostile intent, where the threat is rooted outside an organization (e.g., by hackers and terrorist) (Schulman, 2020; Jore, 2019). In the context of security, the risk is defined based on three factors: value (asset), threat, and vulnerability (consequences) (Alberts et al., 1999; Landoll, 2011; Standard Norge, 2008, NS 5814; Standard Norge, 2014, NS 5832).

The threat is referred to as "*an undesired event that may result in the loss, disclosure or damage to an organizational asset*" (Landoll, 2011). The term is also considered a "risk source" in the Society for Risk Analysis Glossary (2018).

According to Ojanen (2017), defining a threat involves making decisions on what to work on next. In the security context, as for the safety context, a threat can lead to different consequences, e.g., fatalities, environmental damage, reputational damage, and economic loss. By identifying threats, studying their causes and consequences, and describing risk, decision-makers know the risk level and main contributors to risk. In this way, a security risk assessment's primary function is to support decision-making in responding to threats. Several existing security risk assessment frameworks have the same basic elements in conducting a risk assessment as in a safety context: asset valuation, threat analysis, vulnerability analyses, and security risk evaluation (Landoll, 2011). Examples include ISO/IEC 27005:2018 Standard on security management (International Organization for Standardization and International Electrotechnical Commission, 2018);

OCTAVE framework: Operationally Critical Threat, Asset and Vulnerability Evaluation risk assessment (Alberts, 2002); and OCTAVE Allegro framework (Caralli et al., 2007).

Risk assessment in ISO/ICE 27005:2018 is one of the main parts of this risk management framework, founded on the three-factors risk perspective. It consists of the following processes; risk identification (including identifying assets, threats, existing controls, vulnerabilities and consequences), risk analysis (including assessment of consequences, the likelihood of incidence and level of risk determination) and risk evaluation. Risk assessment supports finding appropriate risk treatment options and producing a risk treatment plan (p. 8-12).

The OCTAVE framework is based on the three-factors risk perspective (threat, asset and vulnerability). It is founded on qualitative risk evaluation criteria that describe the 'organization's operational risk tolerances. The risk OCTAVE Allegro approach (Caralli et al., 2007) is built on the same three phases, illustrated in figure 1.

The first step focuses on asset-based threat identification, evaluation and identifying security requirements based on existing knowledge at multiple levels within the organization and standard catalogues of information. The second step concentrates on the identified threat scenarios and evaluating vulnerabilities. The results of the second phase provide insights to develop security protection strategies and establish a plan to manage security risk.

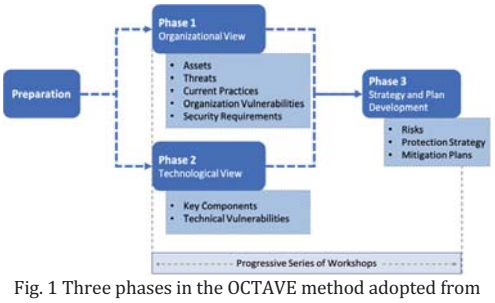

Fig. 1 Three phases in the OCTAVE method adopted from Caralli et al. (2007)

When it comes to managerial practices in the domain of security, Petersen and Rønn (2019) highlight three areas of concern. They include intelligence collection and communication, a new form of technologies in data gathering and utilization (e.g., social media information), changing the threat agent and practices (e.g. cybersecurity). Petersen and Rønn argue that these elements create a storm of complexities and uncertainties, with an ever-increasing demand for providing security. However, according to these scholars, this is challenging to make well-informed judgments and decisions on security measures. They address a need for new methods, coalitions and partnerships to deal with these challenges.

3. Research Methodology

Our research aims to provide an in-depth understanding of how the "safety and security" practitioners distinguish these two fields in their "day-to-day activities". We applied a qualitative method to provide an exploratory edge to clarify how professionals function in their working environment. We used the study's theoretical background (Section 2) as a roadmap to conduct our analyses. We carried out 28 in-depth semi-structured interviews (in-person and online), with safety and security professionals, during October - March 2021, with an average duration of 60 minutes. All subjects agreed and were assured that all information would be treated in the strictest confidence and anonymized data so that no individual, incident or organization could be identified. To capture the diversity of practitioners' experiences, our interviewees included professionals from both the safety and security domains in the various industrial sector.

We used the "Purposive" sampling approach to select individuals who will best help them understand the research problem and the research questions (Creswell & Creswell, 2017, p. 189). It involves "practitioners who have expertise in the substantive domain of interest" (Suri, 2011) working within the safety and security domain regarding the context of this study.

Our participants come from the following countries: Brazil, Canada, Chile, China, USA, France, Guatemala, India, Israel, Italy, Japan, Mexico, Mexico, Norway, Panama, Singapore, Spain, Trinidad, and the UK. It is important to note that several participants work in multinational companies, which indirectly may be in several countries. The following figure illustrates our participants' background divided into continents.

Fig. 2 Participants' background divided into continents

To enhance our data saturation, we used semi-structured interviews with an open-ended question-style. We attempted to link our topics of interest to the interviewee's context—this style allowed for additional information from every new interview. Regarding data sufficiency, we were concerned about having an in-depth discussion rather than testing hypotheses through statistical methods. This is in line with Dworkin (2012), saying that "in-depth interview work is not as concerned with making generalizations to a larger population of interest and does not tend to rely on hypothesis testing but rather is more inductive and emergent in its process." Instead, we followed Creswell and Creswell (2017, p. 189) advice about the sample size, depending on the qualitative design being used. For grounded theory types of research, they recommend conducting twenty to thirty interviews.

Our interview process sought to understand how the participants' job description covers all aspects of their daily tasks and activities in both fields. While we attempted to link our topics of interest to the interviewee's context, we developed a set of trigger questions in advance to use during the interviews:

- Can you describe your work?
- What role or function do you have?
- What is the difference between safety and security-related tasks in your domain?
- Is your job description cover all aspects of your tasks? What is missing?
- What variations associated with your tasks?
- Is the best way to do your task is the same as the way described in the procedure? Is it the way you were trained?

4. Discussion

The objective of this study was to provide insight into the safety and security professionals' experience and perceive how they distinguish between safety and security context in their daily activities. We sought to understand current practices, elements of differences, and convergence areas. We organize and discuss our findings into two parts; (1) conceptual narratives and (2) day-to-day tasks (WAD) and job descriptions (WAI).

4.1. *The conceptual narratives*

To explore whether there is any difference in understanding the main concepts in the safety and security field (Section 2), we asked our participants the following question: What do you understand by safety and security? Participants expressed safety as mainly related to the working environment, accidents in the workplace, life and health, environment and surroundings, etc.

Participants' perception was that safety generally deals with unintended, unwanted events. Regarding security, participants expressed that this is related to physical conditions, vandalism, sabotage, protecting people, and others' values. Some of the statements are as follow:

- *"Safety is linked to avoiding accidents at work. Security is related to vigilance, avoiding robbery, violence at work. It is about policing."*

- *"Safety is related to process-related risks in an industry, i.e. with no intention to cause harm. Security means protection from theft, violence, terrorism, etc."*
- *"Safety is intended to keep the worker safe and ensure the continuity of the company's activities, while security is about preventing damage to its assets, piracy, and attacks."*
- *"For me, safety is about managing health and safety at work, comprising the controls of the work stations regarding occupational risks, occupational accidents and fire protection. On the other hand, security is access control and risk management to the company's / 'organization's assets."*
- *"Safety issues are involved with the integrity of people, and security protects assets and facilities."*
- *"Both safety and security deal with caring for employees and ensuring they are safe at work."*

These statements show that security mainly deals with intentional unwanted events and safety with unintentional ones, aligning with the theoretical views.

To understand participants' perception of risk definition, we asked the following questions: *"How do you define risk, and how do you assess it?"* Our observations clearly show that they have different risk perceptions; several mentions that risk is an adverse outcome, usually linked to something dangerous and relates it to frequency and probability. Some of the responses we received are as follows:

- *"Risk is the exposure to occupational hazards, and they are evaluated by methodologies to eliminate the risks or control them."*
- *"Risk is crossing the frequency and probability of a hazard. I assess risk through field observations; the key point is understanding process operation and human tasks. However, in my job, the risk assessment is a form filled on the desk."*
- *"Risk is something that has the potential to cause harm to someone. Assess it by identifying it, deciding who could be harmed and how, Evaluating the risks, and deciding on precautions to put in place, record and implement to all employees. You should review and update when required."*
- *"It is the likelihood of an event happening and its consequences."*
- *"Risk is an opportunity to learn and improve."*
- *"Probability of event occurring x Severity of event occurring."*

To our surprise, only one participant mentioned uncertainty related to the risk concept, while several relied-on ISO's definitions of risk.

For instance, one of the participants described risk and risk assessment methodology in the following way: *"We define risk differently, depending on the context, which means that we use different risk definitions depending on the work scope. Generally, we use different risk methods for Security and Safety. In our industry, there are strict requirements based on the fact that the consequences can be severe for society, the environment, and life. Therefore, risk management has been used for several decades in various degrees. We have extensive experience with risk analysis. The main methodology used is the probability x consequence (C x P) approach, secure job analysis, and FMEA methods. However, there has been more focus on the security discipline in the last five years, where we have also adopted the tree-factor model."*

We ask follow-up questions, why do you think this is so? *"National security regulation has changed in the last ten years, from specific and detailed requirements to becoming functional requirements. The Act says something about how the end state should be, a reasonable security level, and risk assessments. Safety and Security have many common features, not just reactive (when you lose focus, you typically work reactively), and by this, I mean that both must be proactive".* This comment highlights that the risk analyses were based on ISO 31000 and FMEA for the safety area over several decades. The focus in recent years on security indicates that the company uses the tree-factor model (value, threat, and vulnerability) and applies methods according to Standard Norge NS 5814 (2008) and Standard Norge NS 5832 (2014) standards and have many commonalities with the OCTAVE model (Section 2.2).

The results from the interviews reflect that there are many similarities between the safety and security disciplines. Here we can point to the complexity associated with insider threats and their relation to the safety and security issues (Section 1) and example related to an emergency exit for a data center (Section 4.2).

4.2. *Work as done versus work as imagined*

The survey mapped the work experience and the role or function of participants related to safety and security (fig. 3). Participants have work experience from 1 year to 30 years, with an average of 12 years.

In the survey, responsibilities mapped out whether the participants' companies had a different department that handled safety and security or managed by the same department. About 37 % of participants answered that their company has the same department responsible for both of these disciplines. Some of the participants' area of responsibility include; Health, safety, environment and quality (HSEQ), Health, Safety and Environment (HSE), Health, Safety, Environment and Security (HSES), Safety and Security, training, regulatory affairs, audit and legal compliance.

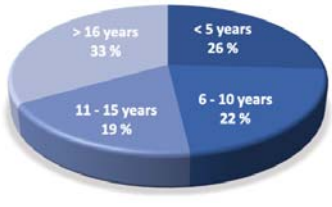

Fig. 3. Participants' work experience

When we asked which areas of responsibility or tasks the participants did, the result is the opposite. About 63% of the participants worked with the safety and security subject

areas. In contrast, 36% only work with the safety domain. From our data, we observe that some participants who have worked with the subject for a long time have been given additional work tasks and more responsibilities.

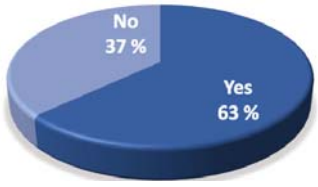

Fig. 4. Different departments for managing safety and security in participants' company or organization

Our finding indicates that companies (where our participants work) mostly (63%) want to differentiate between safety and security disciplines by organizing and placing the responsibility on different departments or parts of the organization (fig. 4). Typical examples from interviews are that "*the HR department is responsible for safety with a background in HSE / HSEQ area, while the business's operational part is responsible for security."*

Some of the participants also said that HR is also responsible for knowledge development. In some cases, the result of the interview shows that the HR department is responsible for human resources while seeing a little trace of the inside threat's challenges and handling (example in Section 1). Some of the differences were related to the participants' daily activities and responsibilities (WAD) and job descriptions (WAI). Some of the differences were related to the participants' daily activities and responsibilities (WAD) and job descriptions (WAI). Some of the differences were related to the participants' daily activities and responsibilities (WAD) and job descriptions (WAI). We see that 63% of participants work with or are responsible for both safety and security areas (*fig. 5*).

Fig. 5. Participants' area of responsibility only safety or safety and security

Regarding functional variability, safety professionals mentioned administrative work as the most significant variation in their role, compared with their job description. Several participants from the safety domain noted that their daily activities (WAD) include security tasks even though they are not explicitly defined in their job descriptions (WAI).

These tasks include incident investigations, checking alarms and cameras, and more. We followed up with questions on "why this is the case." One participant explained, *"[…] safety and security are linked together by having similar objectives and tools. However, the challenge is that it is taken for granted that we have enough knowledge and skills to perform both safety and security-related activities*."

However, findings from the security domain did not imply having such overlapping and expectation. It seems they (security professionals) had a more accurate job description (WAI) in line with their daily activities (WAD). They mentioned, however, that a task variation is about the gap between the security field and information security domain, particularly cybersecurity.

One of our participants said, *"when a cyberattack or cyber incident occurs in the information security domain, the IT department takes the investigation' 's lead, even though it is the security department's core task. The deviation here is related to the role confusion when the security department supports the IT department during cybersecurity investigations."*

An example mentioned by one of our participants was related to an emergency exit for a data center. "*It is crucial for the company that the data center works as it should; otherwise, it affects its functionality, hence reputation*". If an incident occurs in the data center so that personnel inside must evacuate themselves, according to best practice guidelines (WAI). Then the emergency exit must be open or easily opens so that the evacuation can occur in a minimum time. On the other hand, the same emergency exit door must resist burglary, detect attempted burglary, sabotage, and notify it (WAD).

This example illustrates the possible gap between WAI and WAD, namely, operational variability. In dealing with variability, it is necessary to consider safety and security simultaneously (Steen, 2019); otherwise, the final solution will have serious vulnerabilities. Suppose we take a starting point that the emergency exit should open quickly in an incident that requires evacuation. Besides, there are many functional and technical requirements, focusing on how fast it could be opened to secure the location against other threats, for instance, burglary.

Let's look at a concrete technical example with a time delay at the emergency exit. The right solution here is entirely dependent on having a balanced measure that takes care of the needs for evacuation and the need to protect the Data Center at the same time. This example points to what Goessling-Reisemann and Thier (2019, p.122) put it, the "*dynamic changes in system structure and environment, irregular conditions, limited predictability, and surprises acting on the system*".

Another variation between WAI and WAD highlighted in our interviews was related to training activities. It touches on how to adapt the knowledge from adverse circumstances. Participants, both from the safety and security domain, mentioned the conduction of debriefs after an incident. Formal education is also cited as another source of learning.

One of the participants (security domain) describes it as "*my education is dynamic, and I am still learning and develop myself, and try to apply learning points in my daily tasks*." Here, the participant pointed to the importance of dynamic learning to increase explicit and tacit knowledge,

judgment skills, and abilities. For both the safety and security domain, dynamic learning enhances coping capabilities to deal with complexities in performing daily tasks (Provan, Woods, Dekker, & Rae, 2020; Steen, Patriarca, & Di Gravio, 2021).

Another participant (in the safety domain) commented on learning it in the following way, *"there is no focus on learning related to events in our risk management procedures. […] Near-miss incidents or events are not reported, or at best, are under-reported.*

This comment may indicate a culture of fear in the company, which means that important information does not reach senior management. It also points to organizational culture and its effect on learning from the incident and near-miss incidents. Insight into organizational learning is key to understanding contexts, hence improving resilience (Hollnagel, 2014. The "*learning process develops general skills needed for future anomalies*" (Woods, 2018), thus enhances the ability to anticipate changes.

Regardless of which domain, organizations need to look at how they maintain operations when the traditional way of planning for operations no longer provides adequate action guidelines. Rather than addressing the system's safety and security traditionally, based on causality credo, built on a sense of predictability of a system's future performance, they need to acknowledge performance variability. Safety and security cannot be obtained by constraining performance variability since that would also affect the desired outcomes. Instead, the solution is to dampen variability that may lead to adverse effects and simultaneously reinforce variability that may lead to positive results. A potential solution to the challenges involved in the situation with high uncertainty is to develop a holistic approach, integrating risk- and resilience-based thinking (Boin & Van Eeten, 2013; Thekdi & Aven, 2019).

Our finding also includes comments about the group dynamic (Jones & Roelofsma, 2000) between safety and security domain: *"[…] I have a good example a few weeks back about a project that deals with transport. The project group consisted of seven people with both safety and security disciplines who were to take a closer look at the transport of a product that is very critical for our business. At first glance, the report was based on FMEA, and the analysis seemed good. But when I asked about some parts of the report on how you had arrived at the result. The project team could not answer my questions. I quickly concluded that there was a lack of traceability and verifiability."*

Another participant (from the safety domain) mentioned an observation related to the COVID-19 situation: *"We do everything we can to disseminate people and avoid people getting together to avoid collective or community infection. The security decided to block the badges if personnel have not used them (entered the building), the last seven days. Suddenly "everybody" needed to get inside to realize that their badge was blocked and could not get in. The result was an enormous line of people at the main gate to unblock their badges."*

Here, we see the need for mechanisms that ensure synchronizing various safety and security goals and activities. Such a mechanism has to strengthen cooperation between these two domains and increase interoperability, integrating plans and strategies. It is linked to an operational communication strategy built on trust and openness between the parties involved. Resilience in this context is about being both efficient and proactive. While effective communication is about communicating all relevant information in an open, honest, accurate and precise way (Spetalen, Stølen, & Hem, 2015), proactivity embraces being at the forefront of possible intrusive situations.

5. Conclusion and final remarks

Our analysis demonstrates that safety and security professionals have many commonalities in conducting their daily tasks. For instance, they both consider their core responsibility to protect organizational values concerning employees, property, environments, reputation, operational, and more. Both acknowledge the role of training to enhance day-to-day activities. However, different terminology is used, and various aspects are highlighted. The terminology is, to a varying degree, consistent with the intentions and ambitions of the analysis. They also apply different risk assessment techniques, tools and, standards to provide insights into the threat phenomena, processes, activities, and vulnerability of the system being analyzed and identify appropriate measures to deal with the system's vulnerabilities.

On the one hand, the continually increasing level of uncertainty in the organizational environment and the growing integration of information technologies into industrial control systems have created a borderline between safety and security contexts. On the other, focus on efficiency, ideally aimed at working faster, better, and creating contradictory organizational goals. Adversities, stress, and reduced functionalities in the day-to-day operation for both professionals (safety and security) typically relate to the treatment of uncertainties, which is not explicitly reflected in the traditional risk assessment process. Processes need to be initiated to strengthen the application of theoretical view in practice for both disciplines. Rather than managing safety and security separately, based on diagnostic controls, a potential solution to high uncertainty situations is to develop a holistic risk management approach, integrating risk- and resilience-based thinking. This promising area should be explored from normative, conceptual, and descriptive (mode of obtaining practical and operational implications) lines of research in future.

References

Alberts, C.J. (2002). Managing information security risks : the OCTAVE approach : *Boston, Addison-Wesley*.

Alberts, C.J., Behrens G.S. & Pethia D.R. (1999). Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework, Version 10 : *US Department of Defense The Software Engineering Institute : Wilson RW*

Aven, T. (2008). Risk analysis : assessing uncertainties beyond expected values and probabilities.

Aven, T. (2017). A conceptual foundation for assessing and managing risk, surprises and black swans. In G. Motet & C.

Bieder (Eds.), *the Illusion of Risk Control* (pp. 23-39). Springer, Cham. doi: 10.1007/978-3-319-32939-0_3.

Aven, T. & Thekdi, S. (2018). The Importance of Resilience-Based Strategies in Risk Analysis, and Vice Versa. In B. D. Trump, M.-V. Florin & I. Linkov (Eds.), IRGC resource guide on resilience (Volum 2): Domains of resilience for complex interconnected systems. (33-38). Lausanne, Switzerland: International Risk Governance Council (IRGC).

Blokland, P. J. & Reniers, G. L. (2020). The Coupling of Safety and Security. Exploring Interrelations in Theory and Practice: 9 – 16. Sprinter Open. doi: 10.1007/978-3-030-47229-0

Boin, A. & van Eeten, M. J. G. (2013). The Resilient Organization : Vol. 15 Issue 3, 429 – 445: *Public management review*.

Braithwaite, J., Wears, R.L., Hollnagel, E. (2015). Resilient health care: turning patient safety on its head. : *International Journal for Quality in Health Care 27(5)* : 418 - 420.

Broekhuizen, H., Groothuis-Oudshoorn, C. G. M., van Til, J. A., Hummel, J. M., & Ijzerman, M. J. (2015). A Review and Classification of Approaches for Dealing with Uncertainty in Multi-Criteria Decision Analysis for Healthcare Decisions. *PharmacoEconomics, 33(5)*, 445-455. doi:10.1007/s40273-014-0251-x

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). Introducing octave allegro: Improving the information security risk assessment process. *Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst.*

Creswell, J. W., & Creswell, J. D. (2017). Research design: Qualitative, quantitative, and mixed methods approaches. *Sage publications. Thousand Oaks, California: Sage publications.*

Dworkin, S. L. (2012). Sample Size Policy for Qualitative Studies Using In-Depth Interviews. *Arch Sex Behav, 41(6)*, 1319-1320. doi:10.1007/s10508-012-0016-6

Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I. (2017). *Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management. Risk Anal, 40(1)*, 183-199. doi:10.1111/risa.12891

Goessling-Reisemann, S., & Thier, P. (2019). On the difference between risk management and resilience management for critical infrastructures. In *M. Ruth & S. Goessling-Reisemann (Eds.), Handbook on Resilience of Socio-Technical Systems*: 117-135. Cheltenham, UK: Edward Elgar Publishing Limited.

Hollnagel, E. (2014). Becoming Resilient. In P. C. Nemeth & E. Hollnagel (Eds.), *Resilience engineering in practice. : Volume 2, : Becoming resilient* : 179-192. Farnham, UK: Ashgate publishing.

ICAO. (2012). Safety Management Manual (SMM) In : *International Civil Aviation Organization*.

International Standard (2018). Risk Management – Guidelines (ISO 31000:2018)

Jones, P. E., & Roelofsma, P. H. M. P. (2000). The potential for social contextual and group biases in team decision-making: *biases, conditions and psychological mechanisms. Ergonomics, 43(8)*, 1129-1152. doi:10.1080/00140130050084914

Jore, S. H. (2019). The Conceptual and Scientific Demarcation of Security in Contrast to Safety.: *European Journal for Security Research 4(1)*: 157-174.

Landoll, D. (2011). The security risk assessment handbook : a complete guide for performing security risk assessments.: *CRC Press, Taylor & Francis Group*

Mujeeb-Ahmed, M. P., Seo, J. K., & Paik, J. K. (2018). Probabilistic approach for collision risk analysis of powered vessel with offshore platforms. *Ocean engineering*, 151, 206-221. doi:10.1016/j.oceaneng.2018.01.008

Ojanen, H. (2018). The EU's Power in *Inter-Organizational Relations*.

Patriarca, R., Di Gravio, G., Costantino, F., Falegnami, A., & Bilotta, F. (2018). An Analytic Framework to Assess Organizational Resilience. *Safety and Health at Work, 9(3)*, 265-276. doi:10.1016/j.shaw.2017.10.005

Petersen, K. L., & Rønn, K. V. (2019). Introducing the special issue: bringing in the public. Intelligence on the frontier between state and civil society. doi: 10.1080/02684527.2019.1553365

Provan, D. J., Woods, D. D., Dekker, S. W. A., & Rae, A. J. (2020). Safety II professionals: How resilience engineering can transform safety practice. *Reliability Engineering and System Safety*, 195. doi:10.1016/j.ress.2019.106740

Renn, O. (2008). Risk governance : coping with uncertainty in a complex world. London: *Earthscan*.

Renn, O. (2020). New challenges for risk analysis: systemic risks. *Journal of risk research, ahead-of-print (ahead-of-print)*, 1-7. doi:10.1080/13669877.2020.1779787

Ricardez-Sandoval, L. A. (2012). Optimal design and control of dynamic systems under uncertainty: *A probabilistic approach. Computers & chemical engineering*, 43, 91-107. doi:10.1016/j.compchemeng.2012.03.015

Spetalen, T. C., Stølen, I., & Hem, L. E. (2015). Merker i krise strategisk merkevareledelse som modererende faktor. *Magma*, 5.

Society for Risk Analysis, (2018). *Society for Risk Analysis Glossary* : http://sra.org/sites/default/files/pdf/SRA%20 Glossary% 20 -%20FINAL.pdf

Schulman, P. R. (2020). Safety and Security: Managerial Tensions and Synergies. In C. Bieder & G. K. Pettersen (Eda.), *The Coupling of Safety and Security. Exploring Interrelations in Theory and Practice*: 87-95. Springer, Cham. doi:10.1007%2F978-3-030-47229-0_9

Standard Norge, (2008). Requirements for risk assessment (NS 5814:2008). Lysaker: *Standard Norge*.

Standard Norge, (2014). Societal security : Protection against intentional undesirable actions : Requirements for security risk analysis (NS 5832:2014). Lysaker: *Standard Norge*.

Steen, R. (2019). On the application of the Safety-II concept in a security context. *European Journal for Security Research, 4(2)*, 175-200.

Steen, R., Patriarca, R., & Di Gravio, G. (2021). The chimera of time: Exploring the functional properties of an emergency response room in action *Journal of Contingencies and Crisis Management*. doi:10.1111/1468-5973.12353

Suri, H. (2011). Purposeful Sampling in Qualitative Research Synthesis. *Qualitative research journal*, 11(2), 63 - 75. doi:10.3316/QRJ1102063

Tardieu, F., Simonneau, T., & Muller, B. (2018). The Physiological Basis of Drought Tolerance in Crop Plants: *A Scenario-Dependent Probabilistic Approach. Annu Rev Plant Biol, 69(1)*, 733-759. doi:10.1146/annurev-arplant-042817-040218

Thekdi, S. and T. Aven (2019). An integrated perspective for balancing performance and risk. : *Reliability Engineering & System Safety : Volum 190*: 106525.

Woods, D. (2018). The theory of graceful extensibility: basic rules that govern adaptive systems. *Formerly The Environmentalist*, 38(4), 433-457. doi:10.1007/s10669-018-9708-3