VTT

beyond
the obvious

Integrated management of safety and security synergies in Seveso plants

Final report

M. Ylönen, M. Nissilä, J. Heikkilä et al.

VTT TECHNOLOGY 386

VTT TECHNOLOGY 386

Integrated Management of Safety and Security Synergies in Seveso plants (SAF€RA 4STER)

Final report

Marja Ylönen, Minna Nissilä, Jouko Heikkilä, Nadezhda Gotcheva

VTT Technical Research Centre of Finland Ltd

Alessandro Tugnoli, Matteo Iaiani, Valerio Cozzani

University of Bologna

Gabriele Oliva, Roberto Setola, Giacomo Assenza

University of Roma, Campus Biomedico

Dolf van der Beek, Wouter Steijn, Heather Young, Maaike Roelofs

TNO

ISBN 978-951-38-8746-9

VTT Technology 386

ISSN-L 2242-1211
ISSN 2242-122X (Online)
DOI: 10.32040/2242-122X.2021.T386

JULKAISIJA – PUBLISHER

VTT
PL 1000
02044 VTT
Puh. 020 722 111
https://www.vtt.fi

VTT
P.O. Box 1000
FI-02044 VTT, Finland
Tel. +358 20 722 111
https://www.vttresearch.com

Cover image: Shutterstock

Preface

This report presents the main results of Integrated Management of Safety and Security Synergies in Seveso plants (SAF€RA 4STER) research project. The project is motivated by the increasing convergence of process-safety, physical security and cybersecurity risks that could lead to major accidents in Seveso plants. The research project was carried out in 2019-2021. The research partners were the University of Bologna and the University of Roma, Campus Biomedico in Italy, the Netherlands Organization for Applied Scientific Research (TNO), and the Technical Research Centre of Finland, VTT, as coordinator of the project.

This report and the separate online guidelines are targeted for safety and security managers, top managers, regulators and all those who are interested in developing management of safety and security in a coordinated fashion in Seveso plants and process-industries. We hope that this report provides new ideas and insights into the need for integrated management and synergies of process-safety, physical security and cybersecurity management.

We thank for SAF€RA consortium, and Finnish Work Environment Fund (FWEF), Finnish Safety and Chemicals Agency (TUKES) and the Italian National Institute for Insurance against Accidents at Work (INAIL) for funding this project.

Contents

Preface **3**

1. Introduction **6**

2. Ensuring safety and security in the chemical industry **8**

2.1 Importance of both safety and security in Seveso plants 8
2.2 Seveso III Directive 10

3. Core concepts and motivation for integration **12**

3.1 Safety and security—differences and similarities 12
3.2 Definition of management and integration 13
3.3 Why integrate safety and security management? 14

4. Methods and materials **16**

4.1 Literature review on concepts, cultures, and management of safety and security 16
4.2 Interviews with safety and security experts 17
4.3 Literature review on cybersecurity awareness 18
4.4 Survey on attitudes and awareness of cyber-physical security threats 18
4.4.1 Survey design 21
4.4.2 Distribution of the survey 22
4.5 Methodology for analysis of past security incidents 22
4.5.1 Retrieval of past security-related incidents (SRIs) 23
4.5.2 Structure of the database 25
4.5.3 Investigation of the database 27

5. Attitudes and awareness of cyber-physical security threats in organizations **29**

5.1 Summary of the literature review on cyber security awareness 29
5.1.1 Relevant definitions 29
5.1.2 Connection between cyber and non-cyber world 30
5.1.3 System 1 vs System 2 thinking 30
5.2 Survey results 31
5.2.1 Demographics 31
5.2.2 General questions 31
5.2.3 Outcomes 32
5.2.4 Interventions 33
5.2.5 Conclusions of the survey results 34

6. Lessons learnt from security-related events **35**

6.1 Results from an analysis of chemical and petroleum sector SRIs 35
6.1.1 Attack modes triggering final scenarios 35
6.1.2 Cause-consequence chains 38
6.1.3 Attack-patterns related to physical security threats 41

6.1.4 Final outcomes of the attacks 43
6.2 Results from an analysis of cyber-SRIs (CSIs) 45
6.2.1 Characterization and steps of the cyber-attack 45
6.2.2 Impacts of the CSIs 49
6.2.3 Countermeasures and lessons learnt 51

7. Integrating safety and security management in Seveso plants 60

7.1 Motivations for integrated management 60
7.2 Prerequisites for integration 61
7.3 Current state and development of integrated management of safety and security in Seveso establishments 63
7.4 Institutionalisation of IMSS and the role of regulators 65
7.5 Guidelines for integrating safety and security management on Seveso plants 66

8. Discussion and conclusions 68

8.1 Summary and discussion of results 68
8.2 Implications for the industry and regulators 73

Acknowledgements 78

References 79

Appendices

Appendix A: Themes of the expert interviews
Appendix B: Survey on attitudes and awareness of cyber-physical security threats
Appendix C: Definitions for analysis of past security incidents
Appendix D: Results from analysis of SRIs
Appendix E: Definitions of key terms for cyber-attack characterization
Appendix F: Selected cybersecurity-related incidents used in the discussion of the phases of intentional attack and countermeasures

Abstract
Tiivstelmä

1. Introduction

This is the final report of *Integrated Management of Safety and Security in Seveso plants* (SAF€RA 4STER) research project supported by the SAF€RA consortium and financed by the Finnish Safety and Chemicals Agency (Tukes), Finnish Work Environment Fund (FEWF), and the Italian National Institute for Insurance against Accidents at Work (INAIL). The two-year research project was launched in spring 2019 and it ended in February 2021. The research partners were the University of Bologna and the University of Roma, Campus Biomedico in Italy, the Netherlands Organization for Applied Scientific Research (TNO), and the Technical Research Centre of Finland, VTT, as coordinator of the project.

Safety has long been a major concern for industries with hazardous technologies and activities such as the chemical and process industries. Especially since the 9/11 terrorist attacks, security aspects have gained more attention in high-risk industries such as Seveso sites, i.e., industries, which have an activity linked to handling, manufacturing, or storing dangerous substances (e.g., refineries, petrochemical sites, chemicals industries). This is because an attack on a facility with large amounts of dangerous chemicals could cause severe consequences to humans and the environment. In recent years, increasing digitalisation and the use of new technologies such as artificial intelligence (AI) on Seveso sites have made industrial automation and control systems (ICS) susceptible to cybersecurity interference if the ICS are connected to public network. Thus, this research project was motivated by the increasing convergence of cybersecurity, physical security, and process-safety risks that could lead to major accidents.

The objectives of the research project were the following:

1. To gain insights into synergies and tensions related to the management of safety and security in Seveso plants.
2. To find a solution to the challenge of managing safety and security in a coordinated manner.
3. To provide guidelines for managing safety and security in an integrated way in Seveso plants.
4. To provide tools for the identification of security scenarios triggered by malicious human intentions.

The research questions were the following:

1. What are the main differences and similarities in safety and security concepts, management, and cultures in Seveso plants? Can safety and security management be linked?
2. How are cyber threats caused by digitalisation identified and taken into account when assessing and ensuring safety of a process plant?
3. What is the current state of cyber-situational awareness in Seveso plants?
4. How could intentional cyber-physical interference be better taken into account in Seveso plants?
5. How could safety and security threats concerning major hazards be handled in an integrated manner? What are the benefits and drawbacks?

In order to answer to these questions, we have drawn on safety, security, cybersecurity, and accident disaster studies, and carried out a literature review as well as interviews with regulators and safety and security experts on Seveso sites. The purpose has been to provide a background to understanding differences and similarities between the safety and security concepts, cultures, and management, demands for integrated management of safety and security, as well as the current state of integrated management on sites. Furthermore, we have analysed past accidents induced by malicious human intent both in the form of physical security violence and cybersecurity interference, in order to gain insights into the occurrence of physical and cybersecurity breaches. Moreover, we conducted a survey on cybersecurity awareness and physical security awareness in companies. However, possibly due to survey fatigue, the sensitivity of the topic, or the Covid-19 pandemic, the number of respondents of the survey remained low. For that reason, the survey results can only be used as indicative and in combination with other results.

Based on this study, we outlined guidelines for the integrated management of safety and security in Seveso plants. The guidelines provide a framework for designing and implementing the integration. However, the guidelines aim not to be exhaustive, and therefore they can be complemented and concretised further depending on the context.

This final report summarises the findings of the SAF€RA 4STERS project. Chapter 2 deals with the importance of ensuring safety and security in the chemical industry. In Chapter 3 the core concepts of this project: safety and security, physical security, cybersecurity, as well as management and integration are presented. Chapter 4 introduces the implementation of the project and the used data and information. Chapter 5 summarises the findings of the literature review on cybersecurity awareness as well as the results of the survey on attitudes and awareness of cyber-physical security threats in companies. Chapter 6 summarises the results obtained by analysing past physical security- and cybersecurity-related incidents. The results of the literature review and interviews on cultures and management of safety and security are presented in Chapter 7. Chapter 8 presents the conclusions.

2. Ensuring safety and security in the chemical industry

This chapter considers the importance of both safety and security in chemical and process industries and introduces the essential content of EU Directive 2012/18/EU on the control of major-accident hazards involving dangerous substances.

2.1 Importance of both safety and security in Seveso plants

Chemicals play a key role in today's high-tech world and the chemical industry is extremely important to the economy in all countries. This industry contributes to almost every branch of industry. The chemical industry is upstream of various sectors such as construction, transport, food, health, personal cleanliness, home use, clothing, electronics, etc. This industry is also able to supply intermediate products for downstream industries and it contributes directly to creating materials for the consumer market. Since the chemical industry has such a strategic position, it is fully involved in the question of industrial sustainability (Mannan et al. 2015).

Safety must be at the top of the chemical industry's agenda. Many of its products are potentially hazardous at some stage during their manufacture and transport. These chemicals may be solids, liquids or gases, flammable, explosive, corrosive and/or toxic. Manufacturing processes frequently involve high temperatures, high pressures, and reactions which can be dangerous unless carefully controlled. Due to these hazards, the chemical industry operates within the safety limits demanded by national and international legislation (Cozzani 2017).

Traditionally, the primary focus of the chemical industry has been on safety and productivity. However, the framework has changed calling attention to security threats and intentional acts of interference which may lead to major accidents. In the EU countries Directive 2012/18/EU on the control of major-accident hazards involving dangerous substances (Seveso III Directive) lays down the rules for the prevention of major industrial accidents involving hazardous substances and for limiting the consequences of such accidents for human health and the environment. However, security issues are not included in the scope of the Seveso III Directive.

The *European Programme for Critical Infrastructure Protection (EPCIP)* promotes the prevention, preparedness and response to terrorist attacks involving energy sector installations (electricity, oil, and gas installations), but does not extend to other chemical or process industries, and depends on the Member State for its implementation (Casson Moreno et al. 2018).

According to Casson Moreno et al. (2018), the security of industrial sites, and in particular of the chemical and process industry, has become a matter of increasing concern in recent years. Chemical and process industry sites, and especially Seveso sites, are potentially attractive targets due to the storage of hazardous materials in relevant quantities, and due to the possible presence of chemicals that may be used to manufacture improvised explosive devices (IEDs), and to the

increasing use of automated controls and safety-instrumented systems that may allow cyber intrusions.

- Process plants may be subject to physical or cyber-attacks or a combination thereof. According to Baybutt (2017), physical attacks target assets within a facility or process such as inventories of hazardous materials. The attackers may try to reach these assets by penetrating the facility or reaching the assets remotely from outside the facility perimeter. Physical attacks may result in e.g.:
    - release of hazardous materials,
    - theft or diversion of materials,
    - contamination of chemicals, materials, or products,
    - damaging, destroying, or stealing assets,
    - manipulating or disabling equipment, processes, plants, or other assets.

Process plants use computer systems to control manufacturing processes and to operate safety systems, store information, manage value chain activities, etc. In modern plants, these computer systems are often connected to other networks driven by the need to communicate process information to business groups. This exposes the systems to access by more people and access through the Internet.

All these computer systems and their support systems are subject to threats, including the following:

- manipulation of process equipment such as pumps, valves, and motors to cause a hazardous material release, runaway reaction, diversion of materials, contamination or poisoning of products, etc.,
- misdirection of material transfers,
- modification of set points for such process parameters as pressure, temperature, and levels,
- disabling or overriding alarms and trip settings, disabling interlocks, safety instrumented systems, or visual display units that are required for safe process operation,
- disabling, damaging or destroying cyber assets to prevent their proper operation or to cause a financial loss,
- loss, theft, disclosure, damage, destruction, corruption, or prohibition of access to valuable data or information stored in cyber assets.

As a result, both physical and cybersecurity attacks in chemical and process industries can pose severe safety threats, such as, the release of toxic gases or explosions.

2.2 Seveso III Directive

The Seveso III Directive (2012/18/EU)[1] aims at the prevention of major accidents involving dangerous substances. Such accidents pose a significant threat to humans and the environment, and they may cause huge economic losses and disrupt sustainable growth. However, the use of large amounts of dangerous chemicals is unavoidable in some industry sectors which are vital for a modern industrialised society. The Seveso III Directive also aims to limit the consequences of major accidents involving dangerous substances.

The directive covers establishments where dangerous substances may be present (e.g., during processing or storage) in quantities exceeding certain thresholds. Depending on the amount of dangerous substances present, establishments are categorised in lower and upper tiers, the latter are subject to more stringent requirements. In the European Union, the Seveso III Directive applies to more than 12,000 industrial establishments where dangerous substances are used or stored in large quantities, mainly in the chemical and petrochemical industry, as well as in fuel wholesale and storage (incl. LPG and LNG) sectors. https://ec.europa.eu/environment/seveso/

According to the Seveso III Directive, operators of all establishments are obliged to take all necessary measures to prevent major accidents and to limit their consequences for human health and the environment. The main obligations for operators are:

- To notify the relevant competent authority about the inventory of dangerous substances, specifying the quantities, physical form, and the hazardous properties of the dangerous substances present in the establishment.
- Draw-up a major accident prevention policy (MAPP).
- Implement an MAPP by appropriate means and by using a safety management system.
- Provide information to the competent authorities to identify the risks of domino effects.

Additional obligations for operators of upper tier establishments

- Produce a safety report for upper-tier establishments.
- Produce internal emergency plans for upper tier establishments.

[1] Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012L0018&from=EN

Obligations associated with safety management systems (Annex III of the Seveso III Directive): for implementing the operator's safety management system, account should be taken of the following elements:

a) the safety management system must be proportionate to the hazards, industrial activities, and complexity of the organization in the establishment and must be based on an assessment of the risks; it should include the part of the general management system which includes the organizational structure, responsibilities, practices, procedures, processes, and resources for determining and implementing the major-accident prevention policy (MAPP);

b) the following issues should be addressed by the safety management system:

- organization and personnel
- identification and evaluation of major hazards
- operational control
- management of change
- planning for emergencies
- monitoring performance
- audit and review.

The Seveso III Directive focuses on safety-related issues and does not address the need for a security analysis or for security countermeasures in industrial installations that may be considered attractive or vulnerable targets of terrorist attacks. However, according to this directive operators have a general obligation to take all necessary measures to prevent major accidents, to mitigate their consequences and to take recovery measures. It is obvious that e.g. cybersecurity attacks in chemical and process industries can cause severe safety threats such as the release of toxic gases or explosions.

3. Core concepts and motivation for integration

The research project includes several concepts that have different meanings depending on the context and the area of expertise. This chapter presents the definitions of the core concepts of this project: safety and security, physical security, cybersecurity, as well as management and integration.

In addition to the core concepts, we will discuss different motivations and justifications for integration. These are important to reflect upon because this allows us to understand the relevance of integration.

The context of this project are the chemical and process industries. The focus is especially on establishments where dangerous substances may be present (e.g. during processing or storage) in large quantities (Seveso plants).

3.1 Safety and security—differences and similarities

The terms *safety* and *security* have varying meanings depending on the context and on the technical communities they are used in. They differ substantially when used for instance by an electrical engineer, a computer scientist, or a nuclear expert. In fact, there are no absolute definitions for such concepts (Piètre-Cambacédès et al. 2013). Therefore, it is important to define the concepts and the way they are used in the context of the process industry and Seveso sites.

Safety can be defined as the antonym of risk (Hollnagel 2012) or to be without unacceptable risk (SRA 2018). Safety risks are sometimes limited to non-intentional events such as accidents, and continuous exposure (SRA Glossary, 2015). A safety risk may derive from the biophysical world or from extreme weather conditions such as floods or earthquakes, or they may be due to technical failures.

There are also different safety areas relevant to Seveso plants, such as environmental, occupational, and process safety. We refer by safety to process safety and to a holistic, systemic understanding of safety that means plant safety, which consists of technical and organizational systems which external factors and actors also affect. This definition recognizes that safety is an emergent phenomenon that is a continuous process, and that is created as organizations carry out their activities (Woods 2006, Hollnagel 2014).

Erik Hollnagel, a founder of resilience engineering, has distinguished between two different safety strategies: Safety I and Safety II. Safety I refers to strategies of avoiding things going wrong, and it takes lessons learned from accidents. Hollnagel sees a paradox in the way safety is often approached, namely, safety is usually approached via its absence, i.e., focusing on incidents and accidents, instead of via its presence. Therefore, he has introduced Safety II that refers to learning from how things go right. Distinguished from Safety I, Safety II aims to learn from success. Both strategies are used in the high-risk industries.

In this study, we adhere the definition of safety as the antonym of risk, when the risks derive from biophysical world, but also from human and organizational factors,

and when risks are unintentional as distinguished from security risks, which are intentional.

Karanikas (2018) argues that literature and practice indicate that the relationship between safety and security has not yet been clearly defined and their boundaries remain blurry. Reviews of the relationship between safety and security and the similarities and differences between them have been presented by Kriaa et al. (2015) and Karanikas (2018), among others. We will deal with the relationship of safety and security, and their differences and similarities more in Chapter 7.2.

Similarly, to the definition of safety as the absence of unacceptable risks (assuming the risks are unintentional), we adhere to the definition of security as the absence of unacceptable risks, when the risks derive from malicious human intent (see SRA 2018). Hence, it is the intentionality that separates security risks from safety risks.

Security in this study includes both physical security and cybersecurity. Physical security refers to the protection of plants and their systems as well as humans and the environment from malicious human intentions and human intrusion.

Cybersecurity is defined as the protection of privacy, integrity, and accessibility of data information in cyberspace (ISO/IEC 27032 Cyber Security).

The following definitions provide an idea of what security in a positive sense means. A general definition of security can be defined as implying “a stable, relatively predictable environment in which an individual or group may pursue its ends without disruption or harm and without fear of such disturbance or injury”. (Fischer and Green 2004).

According to Jore (2019) security can be defined as “the perceived or actual ability to prepare for, adapt to, withstand, and recover from dangers and crises caused by people’s deliberate, intentional, and malicious acts such as terrorism, sabotage, organized crime, or hacking”. Security threats represent the possibility of hostile action, which can take various forms. Processing plants may be subject to physical or cyber-attacks or a combination thereof.

3.2 Definition of management and integration

We acknowledge that the word integration may create negative connotations in the minds of readers. Therefore, the term synergy would be perhaps more suitable. It could provide more positive connotations than the term integration. Even though, we use the term integration in this project, we refer to synergies deriving from close collaboration and co-construction of a common understanding of the convergence of risks and common ways to tackle systemic risks.

Important prerequisites for integration include an understanding of different levels of integration as well as relevant processes and tasks related to management systems, such as the management cycle.

By management, we refer to 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

and leaderships are closely connected, leadership refers to developing fresh approaches, opening up 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 in order to fulfil its tasks. However, these are much more involved in management and leadership in the current sociotechnical and complex environment, e.g., there are needs to create adaptive responses to new challenges and to balance between many contradictory demands (e.g., Cameron and Quinn 2011; Dekker et. al. 2011; Harvey and Stanton 2014; Reiman et al. 2015). A general management cycle that refers to plan-do-check-act applies is also valid in safety management.

Integration can be divided into three levels (Jorgensen et al. 2006). The first level refers to the increased compatibility of system elements. This includes making the systems parallel using the similarities of standards to structure the system. Yet, separate procedures for each area are continued. Hence, compatibility is only a small, gradual, but necessary step towards an integrated management system. An example of the compatibility of system elements is to combine safety and security management into the same handbook.

The second level of integration embraces the coordination of generic processes, such as the management cycle i.e., plan-do-check-act, or establishing relevant management tasks such as having a visible safety and security policy, defining clear roles and responsibilities and performance measurements, evaluating and developing safety and security management and related training.

The third level of integration includes embeddedness of an integrated management system in a culture of learning and continuous improvement. This third level is more advanced, and it includes having an organization culture that supports learning and internalisation of what integrated safety and security means on different levels of the organization and in different tasks. This relates to developed integrated safety and security cultures (e.g., van Nunen et al. 2018; Reniers et al. 2011).

The potential benefits of integration include better possibilities to understand, identify, anticipate, prevent, mitigate, respond, and learn from safety and security risks. In addition, the benefits include better internal coordination and reduction of possible trade-offs, competitive advantages, reduction of administration and audit costs.

3.3 Why integrate safety and security management?

Traditionally safety and security have been treated as separate issues, and different persons have been assigned to deal with them. However, safety and security both concern the avoidance and mitigation of losses and in the process industry, the goal is to prevent harm due to loss of containment of hazardous substances. To accomplish this successfully it is essential to predict potentially disastrous

scenarios, the degree and extent of damage associated with a scenario, as well as the actions necessary to prevent them, and to reduce the consequences if an undesirable scenario does occur. This includes understanding all of the possibilities, related either to safety or security issues, by which a process can derail and the consequences of each scenario (Mannan 2015).

According to Kriaa et al. (2015), an increasing number of information technologies and communication devices are being integrated into modern control systems, which in turn increases the degree of complexity and interconnection between systems. In the context of industrial control systems, neither a purely security- nor a pure safety-based approach can mitigate risks to the physical infrastructure of the system. Safety and security are complementary and should be treated jointly to improve risk management (cf. Amundrud et al. 2017; Askeland et al. 2017).

The systems required for preventing, detecting, or responding to a chemical accident or chemical security incident are often found to overlap. As such, an integrated approach to chemical safety and security risk management may support more effective implementation of risk reduction measures, provide better detection and risk communication, can be used to support a culture of safety and security within the chemical sector, and allow for the more effective implementation of limited resources (OPCW 2016).

Integration of the approaches, tools, means, and practicalities in both safety and security management provides the possibility to improve both the impact and resource efficiency of safety and security management. However, the differences between safety and security must not be ignored. Certain means and activities of safety and security management are very different, and they will remain as such. This may also cause conflicts between safety and security management activities. In such cases, integration means the connection of different means and activities as an effective overall safety and security management strategy and solving conflicts considering both aspects.

4. Methods and materials

This chapter presents how the research project was carried out and on what type data and information the presented results are based on. The fundamental features of safety and security concepts and management were studied via a literature review and interviews with regulators and safety and security experts in Seveso establishments. In addition, a literature review on cybersecurity awareness and a survey of attitudes and awareness of cyber-physical security threats were carried out. Third, past incidents caused by intentional interference were analysed based on open data sources, and the analyses provided data for the study of security-related scenarios concerning intentional interferences.

4.1 Literature review on concepts, cultures, and management of safety and security

The literature review on safety and security concepts, cultures, and management, consists of 31 articles, four reports in the nuclear context regarding cybersecurity, computer security, as well as security culture, and five books.

Articles were searched from the Journal of Loss Prevention in the Process Industries, Process Safety Progress, Safety Science, Reliability Engineering and System Safety, the Security Journal, and the Journal of Integrated Security Science. Later the literature review was complemented by reviewing Computers in Industry and the Journal for Cleaner Production. The used key words were “safety and security”. In addition, we browsed journals by looking at articles on safety and security cultures and management, as well as integrated management, and the Internet of Things in an industry context.

In the 10-year period from 2009–2019, 16 interesting articles regarding our topic, were found in Process Safety Progress (3), Reliability Engineering and System Safety (8) and the Journal of Loss Prevention in the Process Industries (5). The focus of the papers was not so much on safety and/or security management or integrated management of safety and security, but more on identifying and assessing safety and security risks in the process industry.

In addition, in the Safety Science journal, 13 articles were originally picked as relevant for the industrial safety and security perspective, and out of these nine articles were further reviewed. Furthermore, from Security Journal and the Journal of Integrated Security Science we selected three articles relevant to the topic, from Computers in Industry one article was selected and from Cleaner Production one article was chosen for review.

Besides the 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. Besides this, we reviewed books on security science, the coupling of safety and security and on risk,

crisis and security management (Bieder et al. 2020; Nolan 2018; Smith and Brooks 2012; Borodzicz 2005).

The analysis of this material involved a qualitative content analysis (Krippendorff 2013). When reviewing the articles, the first criteria we used were the following: the motivation for the article, whether it was a theoretical or empirical paper, industry specificity, if the article included a definition of safety, if the article included a definition of security, what specific features of security were described, (ontological differences), specific features of safety (ontological differences), interfaces between safety and security, 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. The main results of the literature review are summarised in Chapter 7.

4.2 Interviews with safety and security experts

Interviews were conducted with the representatives of the chemical industry and Seveso sites (11), a service providing company (2) and the regulatory body (5), as well as confederations of organizations in the chemical industry and oil and gas industry (3). Interviews were carried out in Finland and Italy. In the Netherlands, we did not succeed in getting any interviewees despite strong efforts. There could be several explanations for this, and we can only make good guesses as to why this was. It might be that from the regulator's point of view in their mandate to provide oversight the security aspects were not yet decided on, and the issue of including security aspects in the oversight work of the regulator may have led to concerns about increasing workloads and the need for new expertise.

The interviews were semi-structured thematic interviews that lasted around 1–1.5 hours. The consent of interviewees was requested for their participation in the interviews and for recording them. During the interviews, notes were taken, and after the interviews, the recordings were transcribed. According to the GDPR, interviewees and their companies were anonymised so that they could not be identified. The themes of the interviews are listed in Appendix A.

Thematic interviews cannot be generalised quantitatively, but qualitatively. Content-wise the interviews provided information about the current situation of the integrated management of safety and security in Europe. This is because the companies interviewed, apart from one, represented multinational companies with headquarters in the USA and Europe, and several sites in different countries in Europe, which follow similar procedures and management practices in safety and security. Thus, it can be argued that the study provides at least indicative results regarding the current situation of IMSS in Europe.

The method of analysis was a qualitative content analysis (Krippendorff 2013). Themes were used as a basis of the analysis. We examined the current state of the integrated management of safety and security in Seveso plants, including the ways

safety, security, and cybersecurity were managed. We also looked at the opportunities and constraints regarding the integration of safety and security in a coordinated way and raised relevant aspects regarding the regulators' roles in inspecting safety and security, among other areas. The main results of the interviews are presented in Chapter 7.

4.3 Literature review on cybersecurity awareness

The literature review concerning cybersecurity awareness was based on existing knowledge and the database within TNO. The existing knowledge was supplemented with an extra scan of the available literature. The overarching goal was to provide an overview of existing literature as input for the survey.

From TNO's existing database 38 papers and reports were collected. The researchers decided also to carry out an extra literature search to supplement these papers with relevant meta- and review papers. Meta- and review papers were chosen, as it was expected that such papers would give a good overview of the current state of knowledge concerning this topic. On the 26th of July 2019, a search was performed in the Scopus database with the following query:

> Title: Cyber* AND ((Awareness OR (Behaviour OR Behavior)) AND ("Review" OR "Meta"))

This query resulted in 13 additional papers that were meta or review studies concerning cyber awareness or behaviour. The 51 (38+13) papers were then briefly scanned for thematic relevance based on their titles, leading to the exclusion of 24 papers. The remaining 27 papers (4 from the Scopus search) were used for our literature scan.

The summary of the findings from the cybersecurity awareness-related literature scan is presented in Chapter 5. This information was used as input to develop our survey, which is described in the next section.

4.4 Survey on attitudes and awareness of cyber-physical security threats

Given the context of the overall goal of this project, to look for the synergy between safety and (cyber) security management, the aim of the survey was to collect data concerning cyber awareness among employees of Seveso plants and awareness concerning the connection between safety and security issues in their daily practices. Based on findings from the literature scan, the survey objectives were as follows:

1. Examine the relevance/importance to human cyber behaviour of employees beyond information security to physical safety outcomes (meta-awareness).
2. Compare the state of safety and security management between three European countries.

3. Gain insight into control measures and interventions organizations use to avoid cyber threats escalating into consequences.
4. Explore potential differences in meta-awareness and security behaviour between (IT) employees and managers.

Simplified, one could state that safety management concerns managing the physical systems to avoid any incidents that may cause harm or a loss of containment. (Cyber)security management on the other hand primarily focusses on avoiding any damage or disruptions of the physical systems of a plant. These two worlds come together in situations where a cybersecurity breach indirectly leads to a process or occupational safety threat (Figure 1). IT risks have become an important or even crucial component of the overall operational risk scenarios within certain businesses, especially in Seveso plants.

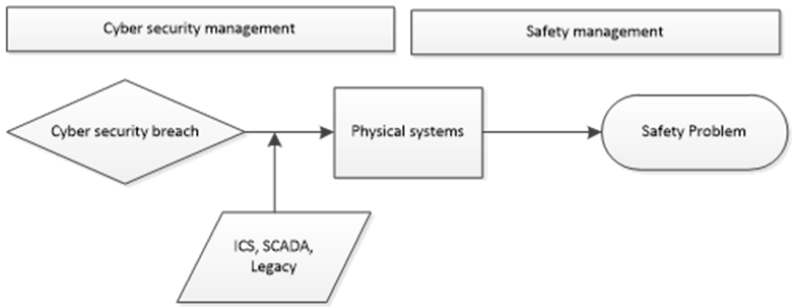


Figure 1. Connection between cybersecurity management and safety management.

The survey examined how aware employees were of cyber security breaches that could lead to safety problems in the real world. The survey contained lists of cyber security breaches and potential safety problems, with questions asking how likely one could lead to another. To assess the resulting response properly would require insight into how likely it would be that certain breaches could lead to safety problems.

Bowties are a commonly used tool to visualize and manage risks. Figure 2 provides an example of the structure of a bowtie. It includes the relationships between threats that can cause a top event, which is the moment you lose control over a hazard (something that can cause damage), and lead to several consequences. It also has room for preventive barriers to avoid the top event from happening, and recovery barriers to mitigate the consequences.

In line with the results from our literature scan, a bow tie approach can help visualize how cyber security aspects can lead to consequences in the physical world. This way we can fill an existing gap, to our knowledge, concerning the relationship between cybersecurity behaviour and safety outcomes.

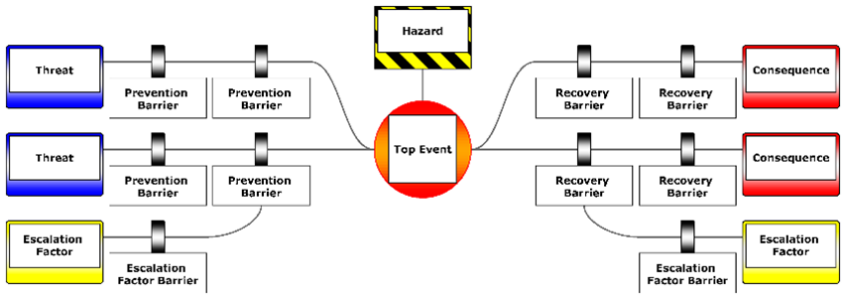


Figure 2. A bowtie consisting of (from left to right) threats, preventive barriers, a top event and related hazard, recovery barriers and finally the consequences.

The following threats, events and outcomes were relevant for our survey:

Threats

1. Hardware misuse. Examples include losing hardware, attaching devices, sharing hardware.
2. Software misuse. Examples include not performing updates and installing unofficial software.
3. Public misconduct. Examples include the use of public WiFi and shoulder surfing.
4. Information misuse. Examples include unsecure sharing of sensitive information and downloading unofficial files.
5. Ignorance. Examples include password management or not recognizing a threat (e.g. phishing).
6. Negligence. Examples include not locking a computer and not reporting incidents.

Events

1. Loss of data
2. Loss of service
3. Loss of process control
4. Unauthorized access.

Outcomes

1. Financial damage
2. Reputation damage
3. Competitors obtaining sensitive data/losing competitive edge
4. Occupational safety incident

5. Process safety incident (i.e. damage to installations or buildings)
6. Loss of containment (i.e. environmental damage or health hazards).

This results in the bowtie (Figure 3), which were addressed in our survey.

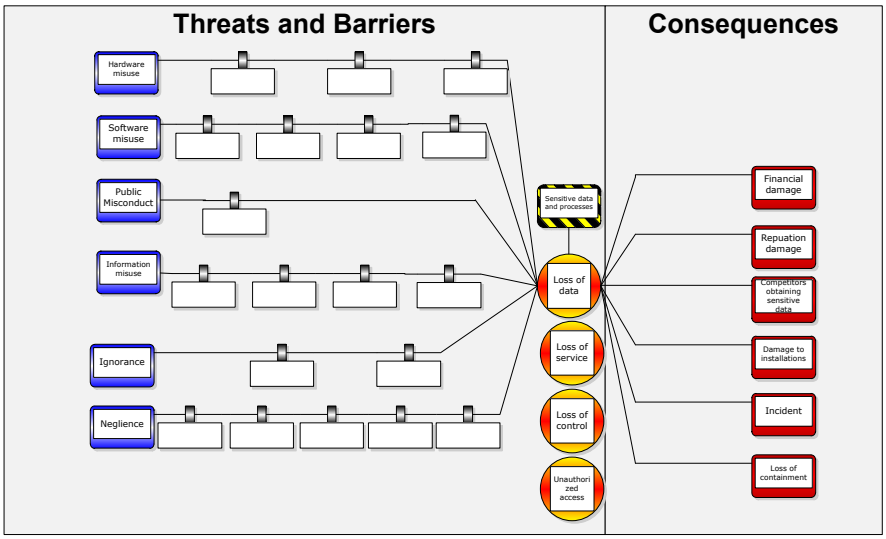


Figure 3. Relevant threats, events, and outcomes related to the survey.

4.4.1 Survey design

The survey contained five parts. The first part introduced the topic and provided some relevant definitions, followed by a few questions concerning the department and function of the participant in his/her organization. These questions were necessary to make sure that questions that were not relevant for an individual could be skipped.

The second part contained the questions related to the bowtie framework described above. The aim of the questions was to determine how likely the participants considered threats and outcomes to occur, while also identifying the awareness of existing links between:

- Threats and outcomes,
- Threats and events, and
- Events and outcomes.

The third part contained general questions concerning cyber security management within the organization and steps taken to integrate safety and security management. The fourth part aimed at the various interventions organizations employ to avoid cyber security incidents, how employees work with

systems, the organizational policy, or the IT-systems. The fifth part contained questions concerning the demographics of the organization where the participants worked. The complete survey is presented in Appendix B.

4.4.2 Distribution of the survey

The survey was distributed in Finland, Italy, and the Netherlands. The survey was developed in English and was translated into Finnish, Italian and Dutch by the consortium partners. Translated surveys were translated back into English to validate the translations. Next, the survey was programmed in Survalyzer to allow distribution.

Organizations were approached in the period of February–July 2020. This was done through existing contacts, but some organizations were approached by mail with a link for access to the survey. We made use of general survey links and specified survey links for organizations. The general survey links were used to send to multiple organizations and could be further spread but would not allow us to identify responses from the same organization. The specified survey links were organization-tied and were used only by one organization, which allowed us to identify participants of a single organization (without identifying the organization). Informed consent and data protection information were included in the introduction of the survey, explaining for instance, that responses were not traceable to identifiable individuals. Furthermore, participation was voluntarily.

Unfortunately, the response rate was low and only seven valid responses were gathered. It is likely that the low response rate is due to the sensitive nature of the topic. Previously we found evidence that organizations are unwilling to share information concerning cyber security and their vulnerability to cyber threats (Steijn et al. 2016). One reason for the low response rate could also be general 'survey exhaustion' among organizations that often are approached to participate in surveys by research institutes. In addition, at the time the survey was conducted organizations worldwide were struggling with the consequences of the Covid-19 pandemic leaving less room for participation in scientific endeavours.

A short summary of the results and a semi-qualitative/semi-quantitative assessment of the results are presented in Chapter 5. Due to the low response rate, the results need to be interpreted with caution.

4.5 Methodology for analysis of past security incidents

A security-related incident (SRI) is an event consisting of physical and/or remote access to the assets of a facility with the aim of giving rise to impacts such as loss of life, loss of production capability, loss of equipment and property, including sensitive data.

The methodology for the analysis of security-related incidents (SRIs) consists of three main steps (Figure 4):

- retrieval of past SRIs from data sources according to specific inclusion criteria
- database population with all the SRIs recorded
- analysis of the overall database or of specific subset of SRIs using tools such as descriptive statistics, correspondence analysis, or Ishikawa diagrams to frame a clear picture of the security threats affecting Seveso plants.

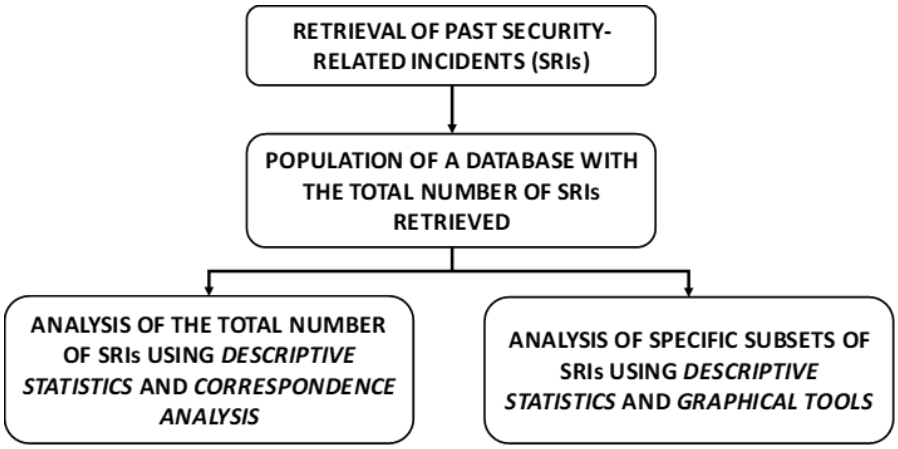


Figure 4. Flowchart of the methodology for analysis of past security-related incidents.

4.5.1 Retrieval of past security-related incidents (SRIs)

In order to provide a more comprehensive view of the issue, the scope of the data collection was expanded beyond the limit of Seveso plants in Europe (chemical and petroleum facilities). Sectors such as energy production, hazardous material transportation (via rail, road and pipeline) and wastewater treatment were included. These sectors were selected as they present at least some features in common with hazmat sites (e.g., similarity in process equipment and facility structures, similarities in the materials handled).

Data was gathered from different sources: scientific literature, the web and specific open-source databases reporting industrial accidents/incidents and near misses (as defined by Rathnayaka et al. 2011). The sources are identified in Appendix C.

Two criteria were used to include SRIs in the database:

- The event should originate as a result of a malicious act aimed at interfering with normal operations (not necessarily with the intentionality of triggering a major accident such as a fire or explosion).
- The event should involve an industrial facility belonging to one of the following sectors: chemical and petroleum, energy production, pipelines, transportation, bioprocesses, and water/wastewater treatment.

The sets of keywords used for querying were different for the investigation of the open-source databases (and differentiated by groups of databases) with respect to the investigation of the open literature. In addition, the mining for physical security- versus cybersecurity-related events required different sets of keywords. Figure 5 (Panel a) shows the complete list of keywords (divided into 7 groups) that were used for querying the data sources. Each group contains synonyms or equivalent terms:

- Group A: type of physical-threat actor
- Group B: type of cyber-threat actor
- Group C: generic terms referring to security-related events
- Group D: generic terms referring to cybersecurity-related events
- Group E: generic terms referring to physical industrial infrastructures
- Group F: generic terms referring to hardware and software
- Group G: generic terms referring to industrial sectors.

The total sets of keywords for querying the open-literature as well as all the above-mentioned databases (with the exception of the Global Terrorism Database [GTD], RISI database, and CSIS database to search for both cyber-SRIs and for physical-SRIs,) can be generated by taking one keyword per group and solving the trees (in Figure 5b) by using Boolean algebra. Since the GTD, RISI database, and CSIS database collect security-related incidents only, records in these three databases were found simply by selecting the industrial sectors of interest.

When looking for SRIs in the open literature, the keywords were translated into several European languages (English, Italian, French, German, and Spanish), while each database was investigated also in its native language. Only English terms are reported in Figure 5a. Due to the high number of open-sources exploited, particular attention was given to avoid the double counting of incidents. Specific checks were carried out considering the date, country and type of facility involved in the event.

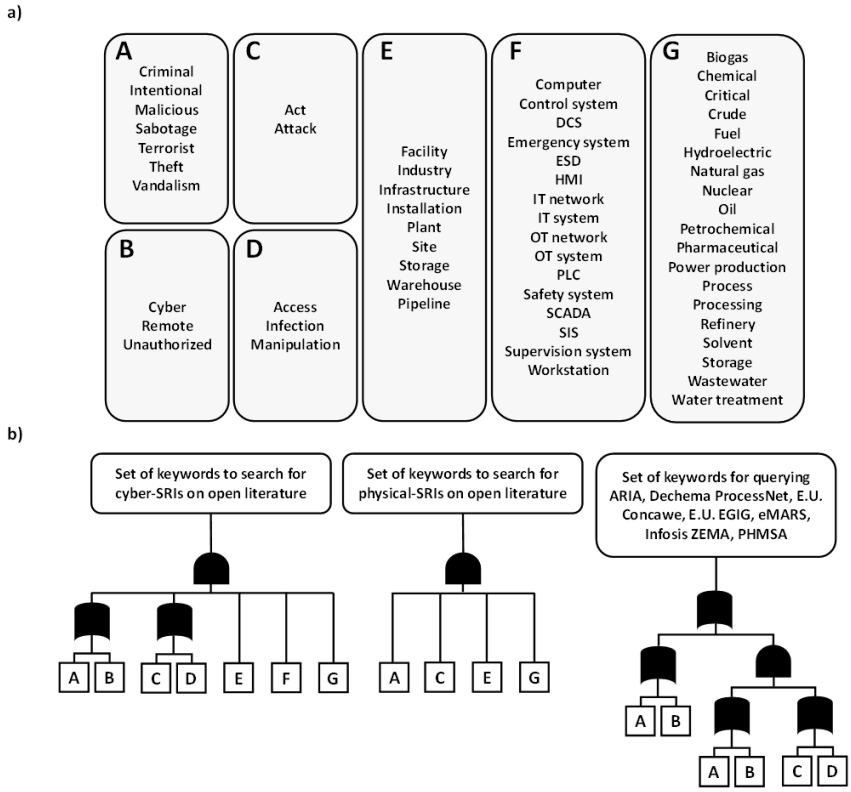


Figure 5. a) Complete list of keywords (in English) used for querying the data sources (groups from A to G; b). The method used was based on Boolean algebra to define the sets of keywords employed to query each different category of data source.

4.5.2 Structure of the database

Figure 6 shows the structure of the database containing all the SRIs from the investigated data sources. Each entry in the database consists of free text fields and itemized fields. Free text fields allow retaining general details concerning the record (e.g., date, location, data source, etc.), while itemized fields help to unambiguously describe a certain feature of the incident.

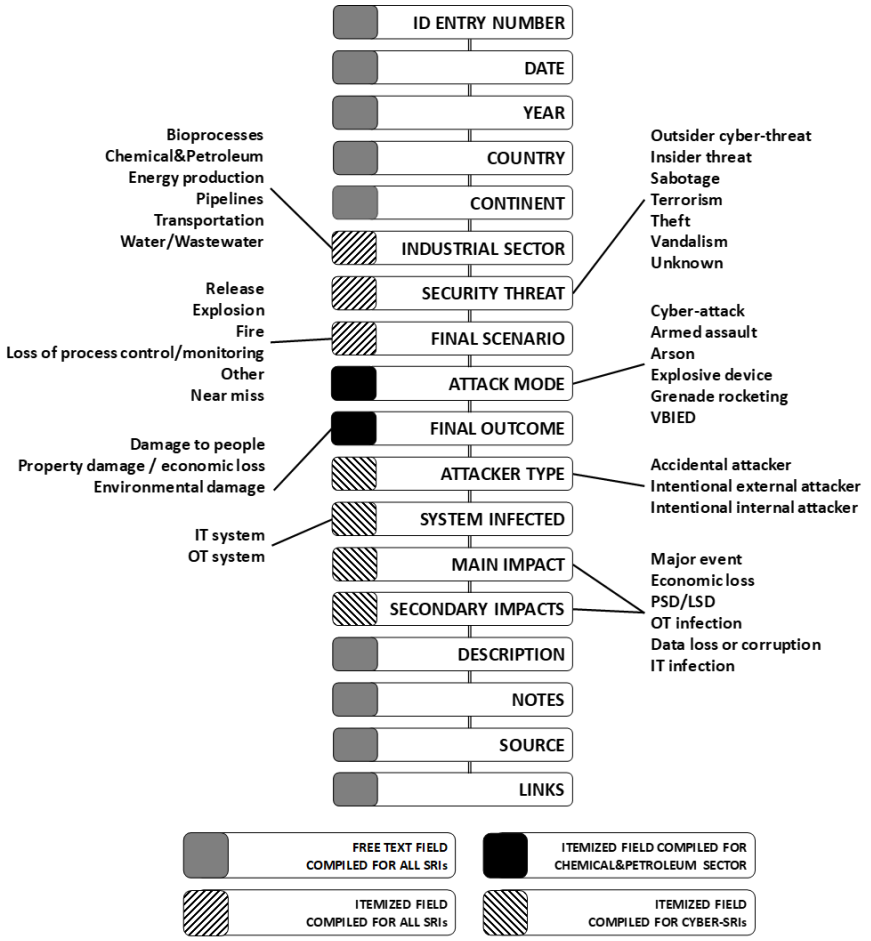


Figure 6. Structure of the database in the present study. The classes associated with each itemized field are reported (see definitions in Appendix C Table 1).

The definitions of the itemized fields considered for the total number of the events, i.e., “Industrial Sector”, “Security Threat” and “Final Scenario” are given in Appendix C (Table 1). The availability of more detailed information on the chemical and petroleum sector events allowed two additional itemized fields, “Attack Mode” and “Final Outcome”, for these events to be considered. Both of these are reported and described in Appendix C (Table 2). Given the different nature of the cyber-attacks with respect to the physical attack modes, three further itemized fields were considered for cyber-SRIs (all defined in Appendix C Table 3): “Attacker Type”, “System Infected”, and “Impact (main and secondary)”.

4.5.3 Investigation of the database

Descriptive statistics and correspondence analysis (CA) were used to analyse the data. The latter statistical tool allowed finding strong correlations between pairs of itemized fields, and more specifically, the correlations between the industrial sectors, the security threats, and the final scenarios for the total number of the SRIs recorded.

A correspondence analysis is a statistical technique, which is helpful in analysing cross-tabular data in a graphical form that reveals the relative relationships between and within two groups of variables (i.e., the itemized fields of the database in the present study). The input data is given in the form of a contingency table, i.e., a table with row and column labels filled with the combined frequencies of the variables (i.e., number of SRIs in the present study). The computing and the theoretical framework of CA can be found in Greenacre (2016). Some important concepts of CA are described and defined in Appendix C (Table 4).

An investigation of the attack patterns was carried out for the SRIs recorded in the chemical and petroleum sector, since more detailed information was available. A fishbone diagram or Ishikawa diagram (Ishikawa 1982) of a general scenario reporting its direct causes in terms of attack modes was built. Moreover, the information available in some records allowed the construction of a simplified adversary sequence diagram, ASD, (Garcia 2007) for a sample chemical and petrochemical site reporting the level of penetration reached by the attackers within the facility and the specific patterns they followed.

Finally, for those records rich in detailed information, cause-consequence chains (Paltrinieri et al. 2013) that linked the attack modes to the final scenarios and the secondary or cascading events which led to the final outcomes for the affected facilities, was made.

In order to frame a clear picture of the cyber threats affecting the process industry and similar sectors, descriptive statistics were used. Cyber-SRIs were analysed to point out ongoing patterns in cyber-attacks, and to get a deeper insight of the type of cyber-attacker (intentional/accidental), the type of system infected (IT system – OT system) and the impacts of the incidents. Table 1 summarizes the aspects that are shown and discussed in Chapter 6 with respect to the sets of SRIs collected in the database.

Table 1. Aspects analysed for the different sets of SRIs collected in the database and the tools used in the analysis.

Set of SRIs	Aspects analyzed	Tool used in the analysis
Total number of SRIs recorded	Time trend Geographical distribution Industrial sectors Security threats Final scenarios	Descriptive statistics and Correspondence Analysis
SRIs collected for the Chemical and Petroleum sector	Attack modes Final scenarios Final outcomes	Descriptive statistics Ishikawa diagram Cause-consequence chain Adversary Sequence Diagram
The total number of cyber-SRIs recorded	Phases of a cyber-attack Type of attacker Type of system infected Impacts	Descriptive statistics

5. Attitudes and awareness of cyber-physical security threats in organizations

This chapter deals with attitudes and awareness of cyber-physical security threats in organizations. Both the results of the literature review on cybersecurity awareness and the survey are presented.

5.1 Summary of the literature review on cyber security awareness

5.1.1 Relevant definitions

Cyber security awareness

Based on the reviews, it appears that an important distinction between a knowledge and a motivational component can be made when discussing awareness. In their review of the literature concerning cyber situational awareness, Franke and Brynielsson (2014) relate situational awareness to sense making, i.e., situational awareness generally means understanding available information so that informed action can be undertaken to achieve desired outcomes. However, Aldawood and Skinner (2019) state that "*Many conducted studies confirm that most computer users have a lack of information security knowledge due to insufficient awareness*". Here awareness is explicitly detached from the knowledge component—which is what situational awareness primarily seems to be for Franke and Brynielsson—and instead awareness becomes a motivational component. Similarly, while not using the word awareness, Chowdhury and Adam (2019) conclude, "*If users feel that there is a lack of importance of cybersecurity in the organization, they are more likely to ignore security requirements …"*

When discussing cyber security awareness, it appears worthwhile to make a distinction between the knowledge (cognitive/reasoned action) and motivational (importance/relevance) components of awareness. It is important to realize that even if the (knowledge and motivational) awareness is optimal within an organization this is still no guarantee for correct cyber secure behaviour. Factors such as conflicting tasks or time constraints and the fact that cyber secure behaviour is not the main goal of the employee can still lead to incorrect behaviour. A further distinction should be between employees who are aware but make an unsecure decision versus employees who lack this awareness.

Cyber security

Almost all papers in our literature scan addressed cyber security primarily from the context of information security, meaning loss, theft, or degradation of information (e.g., Rahim et al. 2015, Franke & Brynielsson 2014).

In the literature from our scan, we rarely came across a definition concerning cybersecurity. An example is von Solms and van Niekerk (2013) who define cyber security as the protection of those that function within cyberspace, including people

and organizations. As such, they explicitly distinguish cybersecurity from information security, which they define as the protection of information and the technologies that store it. This is not to say that literature addressing other aspects of cyber security such as disruptions of industrial processes does not exist. Only that it did not show up in this literature search on cyber security awareness. However, another literature review on safety and security also included the reflections on the relationships between the IT and OT or IACS (e.g., Boyes et al. 2018). The main message is that it is crucial to pay attention to IT-OT relationships due to growing digitalisation tendencies that make OT systems increasingly coupled with public networks, and thus susceptible to cybersecurity interference. This would increase the need for cybersecurity awareness within Seveso establishments.

Cyber safety

The concept of cyber safety refers to safety in cyber space. Cyber safety seems to be a much broader concept (e.g., also addressing e-fraud, child pornography and cyber warfare) and does not solely focus on our topic of research i.e., cyber security risks within Seveso companies. Therefore, we opt not to use this term in our study.

5.1.2 Connection between cyber and non-cyber world

Franke and Brynielsson (2014) argue that cyber situational awareness is a subset of situational awareness in general. Situational awareness, they argue serves to enhance sense making of available information in order to make informed decisions on what actions are required. They state that cyber situational awareness can serve to help awareness of a non-cyber situation, but vice versa, non-cyber information can also help improve the cyber situational awareness.

5.1.3 System 1 vs System 2 thinking

In their study of the effect of time pressure on human cybersecurity behaviour, Chowdhury, Adam, and Skinner (2019) mention the distinction between investigating the effect of system 1 decision making (automatic and emotional) on behaviour as opposed to system 2 decision making (reasoning and effortful). System 2 decision making is often the focus in research.

In our existing body of knowledge, numerous papers explored (overlapping) psychological and environmental factors influencing information security behaviour through various models. This included protection motivation theory (PMT; Hanus & Wu, 2016; Martens et al. 2019; Torten et al. 2018, van Bavel et al. 2019), the theory of planned behavior (TPA; Ajzen 1991, Lebek et al. 2014) and the behavior motivation and trigger capability (B=MAT; Fogg 2009), opportunity motivation behavior (COM-B; Michie et al. 2011), the technology acceptance model (Davies 1989), health belief model (Becker 1974; Becker & Rosenstock 1987), and deterrence theory (Gibbs 1975, Piquero & Tibbetts 1996).

5.2 Survey results

Next, we will highlight the most important results from the survey. The low response rate must be taken into account when interpreting the results (see chapter 4.4.2). Due to the low response rate, it was impossible to exploit fully quantitative survey methods, and the results are only indicative. A full overview of the results is in Appendix B. However, the low response rate must be considered regarding these results (see Chapter 4.4.2).

5.2.1 Demographics

The participants were supervisors or middle management working in various departments (i.e., operations, security, safety, and senior management). Three participants worked only with IT-systems in their daily activities, whereas four participants worked with IT- and OT- systems in their daily activities.

Three participants responded through a specified link, showing that they were from the same organization. This concerned an organization with fewer than 250 individuals, older than 20 years, in the chemical and pharmaceutical sector, with an upper tier obligation under the Seveso regulation (although one respondent appears to have mistakenly reported the organization to be lower tier), and which is a part of an international organization, with multiple sites.

Of the remaining four participants who used a general link, one worked at an organization with fewer than 250 employees, which was younger than 10 years, in the energy sector, with no Seveso obligation. The other three participants worked at an organization with more than 250 employees, which was older than 20 years, in the energy (n =1) or oil refining sector (n = 2), with upper tier obligations under the Seveso regulation (one respondent had not answered this question), and as part of an international organization, with multiple sites (n = 2), or independent (n = 1).

5.2.2 General questions

Overall, all participants had (very) great confidence in the cyber security of their organizations. Six participants reported the IT department to be responsible for cyber security and three participants indicated the security department also to be responsible. For three participants, the IT department was the only responsible department. One participant indicated a cybersecurity department as being responsible and was the only responsible department according to that participant.

Six participants indicated that cyber security policies were taken into consideration daily, and the seventh participant had to do this at least once a week. All participants thought that employees in their organization were to some or a great extent aware of the potential impacts of cyber security. Two participants did not know if safety and security managers had meetings, two reported weekly meetings and two reported monthly meetings. One participant did not answer this question.

There was variety in responses to the question as to whether safety and cyber security management were interdependent. Three participants took the middle road and reported this to be true to some extent. In the box below, we provide some of the elaborations by the participants on the relationships between safety and cybersecurity.

Elaboration on the relationships between safety and cybersecurity

- *The answer to this question obviously varies according to the respondent's main business. In our case, there are relatively few impacts of a cyber incident involving the HSE function.*
- *Partly handled by different departments.*
- *There are different departments with their organizations, but they work together.*
- *We have completely separate things.*
- *Organizational measures, access control and contractor qualification.*

Three participants shared their activities and tools to integrate safety and cyber security management, given in the box below.

Activities and tools to integrate safety and cyber security management

- *Both of these risks are managed in an integrated and supervised manner by the chief risk officer. Molt and BIA (business impact analyses) are carried out jointly by their respective functions.*
- *Safety indicators and their monitoring, Monitoring of near misses and determination of corrective measures, staff training, use of change management systems, safety and process safety risk assessments, root cause analyses.*
- *Firewall, internet access limitations, security, mail servers outside the company domain.*

5.2.3 Outcomes

The participants indicated that employees in their organizations never or sometimes demonstrated unsecure behaviour. One participant reported that information misuse occurs often, whereas another participant indicated that ignorance and negligence was often the case among employees in his or her organization.

Financial damage, reputational damage and loosing competitive edge were the most likely outcomes of a cyber security breach according to our participants. Occupational safety incidents were considered the least likely. However, all participants indicated that none of the outcomes had ever occurred in their organization as a result of a cyber security breach.

The participants appeared to be aware that unsecure behaviour could have various outcomes. Occupational safety incidents were the least reported. Only two participants mentioned occupational safety incidents as a consequence of

negligence or ignorance. Financial damage and reputational damage were considered the most likely outcomes.

Loss of data was reported to be the most likely cyber security breach as the result of unsecure behaviour. Loss of data was not associated with the outcomes of an occupational safety incident or asset damage by our participants. This seems to suggest that cyber security incidents were not strongly associated with physical damage (to employees or assets) other than loss of containments, which was reported more often.

5.2.4 Interventions

Below we provide tables which illustrate the interview responses concerning the cyber security interventions aimed at how employees work with systems (Table 2), organizational policy (Table 3), and IT-systems (Table 4). The tables show that organizations employee numerous interventions to safeguard their cyber security.

Table 2. Cyber security interventions aimed at how employees work with systems.

Interventions	***N***
Awareness campaigns	5
Mobile device management (e.g., separating work use and private use of devices)	3
Use of VPNs (to protect against unsafe use of networks)	6
Multi-factor authentication	3
Fake phishing mail exercises	3
Enforcement of strong passwords	6
Exercises*	1
End point protection measures*	1
Social network tools guidelines*	1

Total N = 6. Interventions with an asterisk were provided by a participant.

Table 3. Cyber security interventions aimed at organizational policy.

Interventions	**N**
Managers set a good example	4
Reporting and monitoring of incidents	6
Extra attention for safety protocols	5
Access security (physical & digital)	5
Periodic report of the cybersecurity function to the Supervisory Bodies*	1

Table 4. Cyber security interventions aimed at IT-systems.

Interventions	N
Risk analysis	4
Automated software updates	4
Timely replacement of outdated hardware	4
Anomaly detection	5
Partitioning	2
Penetration tests	3
Business impact analysis	1
H24 cybersecurity monitoring	1
Third party audit	1

5.2.5 Conclusions of the survey results

Although we had a very limited sample pool, the demographics showed that it was a relevant sample with supervisors and middle management from various departments. Therefore, we feel that the above results have some validity, in spite of the limited number of responses. The participants indicated that their organizations had proper cyber security, although only one participant reported a separate cyber security department. However, IT departments are often responsible for cybersecurity. Furthermore, the organizations reported numerous interventions used to safeguard their cyber security on a human, policy, and technology level.

Little evidence was given of any integration between safety and cyber security management. Occupational safety incidents were considered to be the least likely outcome of a cyber security breach. As such, this outcome differentiated strongly from the other possible outcomes. Unfortunately, we do not have data to confirm whether this assumption (occupational safety incidents are less likely related to cyber security incidents) is true. Organizations are generally unwilling to share much about the status of their cyber security. For example, all participants reported that no negative outcomes had been suffered as the result of a cyber security incident. Although this is possible, it also aligns with the general attitude of secrecy surrounding this topic. Sharing of information will boost learning and resilience towards future events and threats.

6. Lessons learnt from security-related events and security scenarios

The database described in Chapter 4.5 contains altogether 369 security-related (both physical security and cybersecurity) incidents (SRIs) from the years 1965–2019. The results obtained by analysing the SRIs in the chemical and petroleum sector and the cyber-SRIs are presented in Chapters 6.1 and 6.2. The results of the total number of SRIs are presented in Appendix D. This chapter also presents physical security scenarios.

6.1 Results from an analysis of chemical and petroleum sector SRIs

6.1.1 Attack modes triggering final scenarios

A specific analysis concerning the attack modes carried out by the threat actors and the cascading events that led to the experienced final outcomes in the affected facilities was carried out for the chemical and petroleum sector. Definitions of the attack modes and the final outcomes considered in the present analysis are reported in Appendix C. Figure 7 shows the 3D-plot reporting the share of the attack modes with respect to security threats.

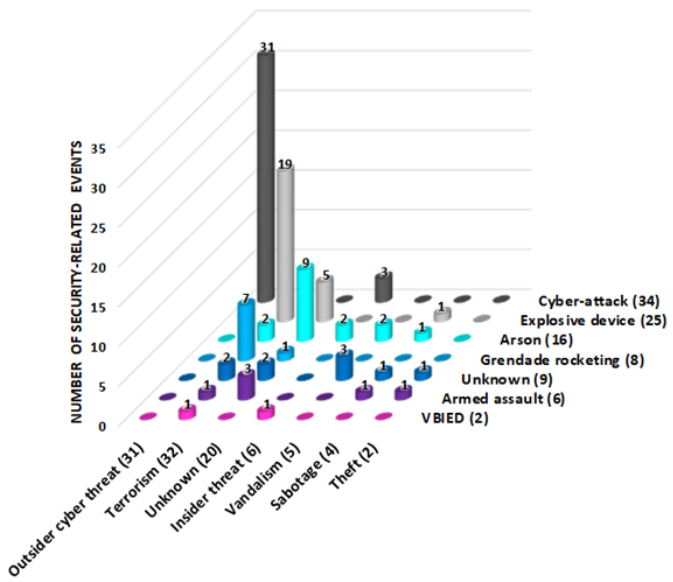


Figure 7. 3D-plot reporting the share of the attack modes with respect to the security-threats. (VBIED: vehicle-born improvised explosive device).

For 91 SRIs out of 100 recorded in the chemical and petroleum sector, it was possible to identify the attack mode through which the threat actors tried to penetrate the security barriers in place and give rise to impacts in the target facilities. A cyber-attack (i.e., an attack via the cyberspace to the IT-OT network of a facility) was the attack mode with the highest number of events recorded (34 SRIs). Almost all of these events were related to an outsider cyber threat. Only three were performed by insiders (e.g., disgruntled employees).

Among the physical attack modes, the use of explosive devices (i.e., devices that provide a violent release of energy when detonated) was the most common (25 SRIs). This type of attack is usually carried out by highly capable and well-motivated adversaries such as terrorist organizations (19 of 32 SRIs related to terrorism were caused by the detonation of explosive devices). The was true for grenade rocketing (i.e., shooting missiles with a rocket launcher or by remotely controlled drones): and seven out of eight SRIs were found in the terrorist matrix. Sixteen cases of arson were recorded, revealing that this is a common attack mode as it does not require the threat actors to be highly equipped nor well-motivated, as in most of the cases (9 out of 16 SRIs) the security threat behind the arson was unknown. Furthermore, six cases of armed assault with firearms and two cases of vehicle borne improvised explosive device (VBIED) attacks were also registered against chemical and petrochemical facilities. Figure 8 shows a 3D-plot reporting the share of the attack modes with respect to the final scenarios triggered by the attackers.

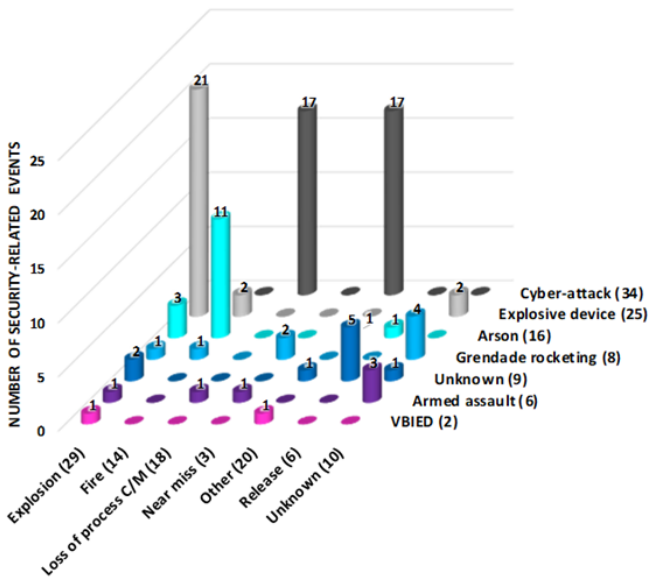


Figure 8. 3D-plot showing the share of the attack modes with respect to the final scenarios triggered by the attackers (VBIED: vehicle-born improvised explosive device).

A physical explosion of chemical equipment was by far the most common event that occurred as a direct consequence of the detonation of an explosive device (21 cases of explosion out of 25 cases of detonation of an explosive device). Industrial fires involving process equipment were by far the most frequent final scenario triggered by arson (11 cases of industrial fire out of 16 cases of arson). It is interesting to note that in two cases of grenade rocket attacks a near miss occurred. However, the attacks were unsuccessful since the missiles were intercepted by air-defence forces. The same happened for one case of armed assault in which the security guards succeeded in interrupting the assailants.

When cyber-attacks are considered, in case of infection of the OT system, the impacts experienced by the affected facilities spanned from an infection of the HMI workstations (12 SRIs) to a local or process shutdown (LSD/PSD, 5 SRIs). On the other hand, when only the IT system became infected, data theft or corruption and technical inconveniences at the IT level were registered (respectively 3 and 14 SRIs). No major events occurred in chemical or petrochemical facilities because of cyber-attacks. Thus, as shown in Figure 8, a loss of process control/monitoring and one “other” scenario were the two final scenarios that followed cyber-attacks, each with 17 SRIs recorded.

Only one event recorded a loss of process control/monitoring following a physical attack mode, more specifically an armed assault. In the event that took place in Libya in 2018, the assailants entered the Sharara Oilfield and physically threatened employees and forced them to shut down the oil pumps.

An explosion and one “other” scenario followed the two recorded VBIED SRIs. It is also interesting to notice that the attack mode was unknown for five out of six SRIs leading to releases of chemicals. Since these events often result from intentional acts realized by the use of simple hand tools or even by simply opening valves manually, the events are characterized by low media interest when compared to the other attack modes, and therefore such information might be often not reported, or under-reported in the media.

An Ishikawa diagram (also referred to as a fishbone diagram due to its shape) of a generic final scenario was obtained from the analysis of thirty-five (35) SRIs that occurred in the chemical and petroleum sector and included sufficient details about the attack modes. The diagram, shown in Figure 9, presents the direct causes of a final scenario in terms of security attacks performed by the attackers.

In four cases where an “explosive device” was the attack mode, the explosives were placed within the site area of the target chemical or petrochemical facility: i.e., the attackers managed to enter the perimeter of the facility bypassing the barriers in place without being disturbed. In another two cases the specific attack consisted of an external bombing. In two cases where an “armed assault” was the attack mode, the attackers made use of firearms. Gasoline- or alcohol-based incendiary weapons were used in four cases by the threat actors in an arson attack, while in one case arson was carried out using an improvised source of ignition (i.e., a cigarette) that was able to ignite a flammable gas mixture. With respect to the “VBIED” category (2 SRIs recorded), in one case a vehicle with flammable gas cylinders entered the plant and exploded near the facilities, while in the other case

a car bomb with 20 kg of dynamite inside was detonated close to the facility fences, in an off-site area. Missiles launched by drones (one case) and rockets launched by rocket launchers (3 SRIs) were used in the “grenade rocketing” cases.

With respect to cyber-attacks, the following specific attack modes were detected:

- 7 cases of buffer overflow attacks (i.e. an attack aimed at overwriting parts of the memory data);
- 4 denial of service attacks (i.e. an attack aimed at making a machine or a network resource unavailable);
- 2 software reprogramming attacks (i.e. an attack aimed at reprogramming parts of the software code);
- 1 ransomware attack (i.e. an attack aimed at publishing the data contained in the target machine or perpetually blocking access to it unless a ransom is paid);
- 1 wiper attack (i.e. an attack aimed at wiping the hard drive of the target machine);
- 1 spyware attack (i.e. an attack aimed at gathering information about a person or organization).

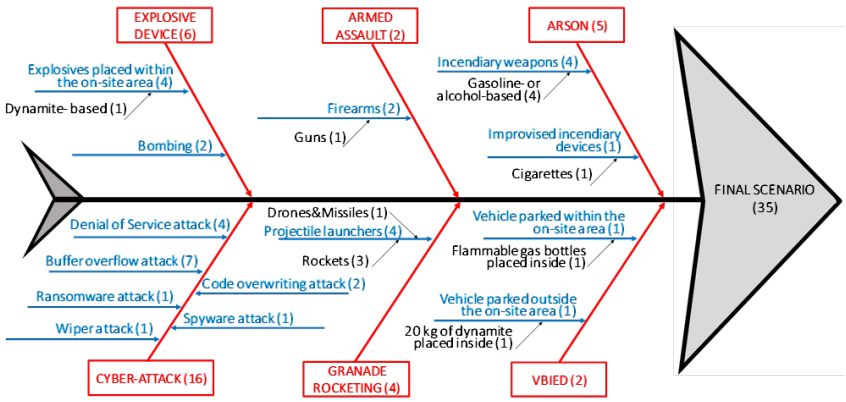


Figure 9. Fishbone diagram reporting the detailed causes in terms of attack modes in the case of successful final scenario (i.e. explosion, fire, release, loss of process control/monitoring, other, or a near miss).

6.1.2 Cause-consequence chains

Figure 10 shows the event-specific cause-consequence chains obtained from seven (7) SRIs with sufficiently detailed information available. Despite being a limited set of data, the incidents selected for this analysis still represent different significant combinations of attack modes and threats. The cause-consequence chains link the attack modes perpetrated by the attackers, the final scenarios triggered and the

secondary or cascading events, which lead to the final outcomes of the event. The cause-consequence chains were obtained applying the “Why Tree” technique (CCPS 2003).

At first, the basic event (i.e., the attack mode in this case), the critical event (i.e., the final scenario) and the outcome event (i.e., the final outcome) were identified and displayed in separate boxes. Then, the other elements in the chain were identified and defined asking the question “why?”, or, more specifically “what is directly necessary and sufficient to cause this event?”. In the present study, two levels of “attack event” leading to the final scenario and three levels of “cascading events”, from the scenario to the final outcome, were considered.

The case of the “explosive device” is of particular interest since the details of the incident were sufficient to fill all the boxes in the chain. The attackers entered the facility bypassing the physical barriers in place (e.g., the facility fences), and positioned an explosive device on the roof of a gasholder. The detonation of the explosive caused the physical explosion of a gasholder with the consequent release of the flammable gas contained inside, as well as the ejection of missiles and the generation of overpressure. The direct event that occurred was the formation of an airborne flammable mixture that, once ignited, resulted in a fireball, causing property damage and huge economic losses to the facility affected.

The two cases of “VBIED”, confirmed that impacts on the target facility can also be generated by physical attacks that do not involve the intrusions of the attackers within the restricted areas of the site. In one case the attacker parked a car bomb with 20 kg of dynamite inside outside the site, near to the fence, and detonated it causing damage to the facility buildings (“other” consequences as defined in the “methodology” section) and injuring two operators. In the other case, the explosion of a vehicle with cylinders containing a flammable gas parked in a closed hangar within the facility caused the physical explosion of inert gas vessels contained in the hangar, leading to one fatality, two injuries and property damage, because of the ejection of missiles and overpressure generation that followed the explosion.

The case of “armed assault” confirmed that the threat actors executing the attack were highly trained, well-motivated and highly equipped: they entered the facility by opening fire on security personnel with guns and then detonated dynamite-based explosives in buildings and in the plant, giving rise to physical explosions that caused property damage and related economic losses to the facility affected.

Figure 10. Cause-consequence chains (from the attack modes to the final outcomes on the process facility under attack), based on seven records which reported detailed information on the incidents.

The case of “grenade rocketing” is particularly significant, since the threat actors air-bombed the plant with missiles launched by drones, possibly controlled from a remote site far away from the attacked facility, causing several explosions leading to the release of flammable substances which resulted in multiple fires. The prevention of this type of attack is very challenging, since drones, missiles or rockets have to be destroyed or diverted before they physically impact the facility. Nevertheless, there have been cases of successful defence from such type of attacks: e.g. in two different air-attacks in Saudi Arabia in 2018 the air-defence forces succeeded in destroying the missiles.

The case of “cyber-attack” shows a typical attack pattern through the network architecture of a process facility. According to Iaiani et al. (2020), a worm managed

to access the OT system of a chemical facility through a poorly configured firewall after accessing its IT system. Then, by exploiting a distributed control system (DCS) buffer overflow vulnerability, it disabled two HMI workstations in the control room. No production was lost thanks to the antivirus (AV) software that revealed and stopped the worm infection.

6.1.3 Attack-patterns related to physical security threats

Physical attack patterns are inherently different from those carried out via cyberspace (i.e., cyber-attacks). In the latter case, attacks need to bypass the barriers of the IT-OT network, e.g., authentication system, firewalls, AV software, etc. In a physical attack the threat actors have to bypass the barriers of the physical protection system (PPS), e.g., fences, gates, locked doors, etc. Therefore, attack modes such as an “armed assault”, “arson”, “explosive device”, “grenade rocketing” and “VBIED” have similar attack patterns, since they take place through the PPS of the target facility, while a “cyber-attack” has its own specific features. Thus, in the following, only physical security-related incidents that occurred in the chemical and petroleum sectors were taken into account.

In particular, seven SRIs reporting sufficiently detailed information allowed the identification of the specific paths through the PPS of the affected facilities that were followed by the attackers. An adversary sequence diagram (ASD) was found to be a useful tool to represent such attack patterns and to show the level of penetration reached by the threat actors within the facility. In order to represent the paths more effectively in a general framework, they were adapted to a reference chemical and petrochemical site and are reported in a single ASD.

The layout of the sample process facility is shown in Figure 11a. An off-site area, an on-site area, some buildings, a warehouse, a control room, a tank farm, and a process plant were the physical areas considered in the reference layout adopted. Site fences and the manned reception with personnel and vehicle gateways were considered to separate the off-site area of the facility from the on-site area. Walls and roofs were considered to protect the buildings (including the control room), which are accessible through doors and vehicle doorways. A dike is present around the plant which is interrupted by the part that is used for the entrance of personnel and vehicles. A basic process control system (BPCS) and a safety instrumented system (SIS) remotely connect the control room and the process plant.

Figure 11b shows the simplified ASD of the process site described above and shown in Figure 11a. The main simplification introduced in the ASD (Figure 11b) consists of reporting the physical areas and the elements of the physical protection system without considering probabilities of detection and delay times as in the complete ASD, since these parameters are out of the scope of the present analysis.

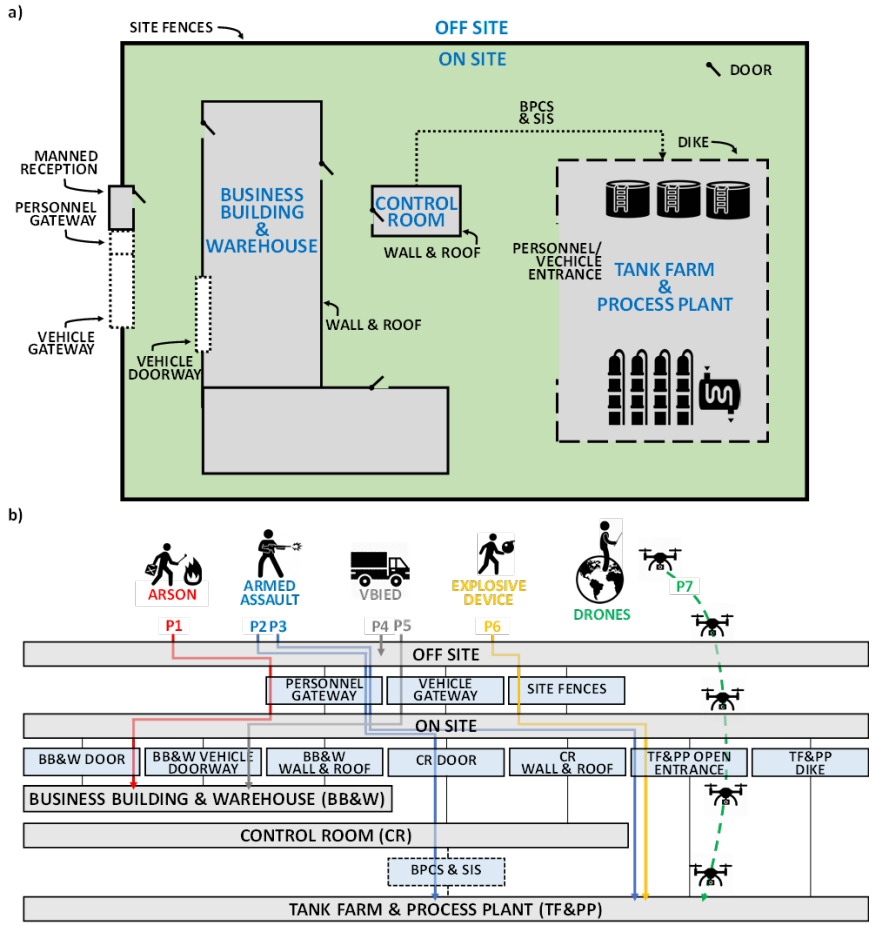


Figure 11 a) Reference layout representing the position of the different targets considered in the simplified adversary sequence diagram (ASD); b) Attack patterns derived from events for which sufficient details were available, represented through a simplified ASD.

As shown in the simplified ASD, the attackers can access the tank farm and process plant area (TF & PP) both directly and indirectly. Actually, in two cases the assailants managed physically enter the TF & PP area through the dedicated personnel and vehicle entrance after accessing the on-site area. In one case the on-site area was accessed through the personnel gateway by opening fire on the security personnel (P3 in the ASD), while in the other case the attackers entered the facility crossing the site fences, bypassing the manned reception (P6 in the ASD). In a further attack path, the TF & PP area was accessed indirectly through the manipulation of the control and supervision system (BPCS and SIS) once the assailants had physically accessed the control room: in particular, the assailants

entered the facility through the personnel gateway and, by threatening the employees with firearms, they gained access to the control room and forced the operators to shut down the oil pumps (P2 in the ASD). Moreover, path 7 in the ASD (P7) shows that the process or storage equipment can also be accessed by air, and more specifically by remotely controlled drones: unlike all the other cases reported in Figure 11b, in this specific attack mode the attackers may carry out the attack from a remote site far away from the site.

In two cases (P1 and P5 in the ASD), the target of the attackers was the warehouse area of the facility. In both cases the threat actors were insiders: in case P1, a former employee managed to enter with his old credentials and to access the warehouse where he triggered a fire with an improvised source of ignition (a cigarette). In case P5, a certified delivery driver entered the facility through the dedicated gateway and drove his light-duty vehicle (containing flammable substances) inside a closed hangar where he caused the physical explosion of the inert gas vessels contained in the hangar. Moreover, path P4 in the ASD highlights that the threat may arise from the off-site area immediately close to the facility fences. In that particular case the attacker did not enter the industrial site, but rather parked a vehicle containing explosives outside the target industrial site and detonated it.

In four out of the seven SRIs with more detailed information that allowed us to build the simplified ASD shown in Figure 11b, the threat actors entered the on-site area of the target facilities through the personnel and vehicle gateways (i.e., through the site entrance) in order to give rise to impacts. The site entrance can be crossed by insiders without any detection as they have authorized access to the facility (resulting a very critical category of threat), while concerning outsiders, the main entrance can be crossed by counterfeit authorization (e.g., counterfeit badge) or by force (e.g., armed assault). Overall, the analysis of the available data indicates that the site entrance is a key element when designing the PPS of a process facility.

6.1.4 Final outcomes of the attacks

It is important to conclude the discussion highlighting the potential severity of the SRIs experienced and included in the database. Figure 12a shows the distribution of the final outcomes concerning the chemical and petrochemical facilities for which more detailed data was available. Property damage and economic losses turned out to be the most common class of impact experienced by the affected facilities (77 SRIs, 77% of the total). At least one injury or a fatality occurred in 15 SRIs (15%), while environmental damage was registered for three SRIs (3%). Moreover, no final outcome was recorded for three SRIs (3%), in those cases a near miss took place. In two SRIs (2%) no information on the impacts was available.

Figure 12b reports the number of injuries and fatalities associated with the events. In particular, 113 injuries and 41 fatalities were recorded. Compared to the data by Casson Moreno et al. (2018) these values are smaller than those obtained in the case of pipelines for oil and gas transportation and are similar to those of the energy production sector. Fixed installations have a more limited extension than

pipelines, and are generally better protected from outsider physical threats with security barriers, which allow easier protection from malicious intrusions. Moreover, in facilities where hazardous substances are stored or handled, more intense surveillance is usually in place, thus a timely activation of safety systems that may contribute to the mitigation of the consequences of the security attacks can be achieved.

In more detail, 15 injuries and 23 fatalities were directly caused by the attack modes perpetrated by the threat actors, and 61 injuries and 8 fatalities were, instead, strictly due to the scenarios triggered by the security attacks. No data was available for the remaining 37 injuries and 10 fatalities. The incident with the largest number of injuries and fatalities (respectively 27 and 8) occurred in 2014 in Pakistan in which attackers bombed a chemical plant. The event with the highest number of fatalities (19) was recorded in 2014 in Libya, where assailants with firearms and missiles attacked military personnel protecting a petrochemical plant.

Figure 12c reports information about the economic losses of chemical and petrochemical facilities associated with 14 SRIs for which data was available. In particular, six SRIs led to losses of less than 100 k$, five SRIs led to losses between $ 100 k$ and 1 million$, and three SRIs led to losses higher than 1 million$. For example, in 1997, a warehouse of 30,000 m^2, including a refrigeration plant using ammonia and a battery charging plant, were intentionally burnt down in an act of sabotage. According to the EU's eMARS database the economic losses for the affected company were over 2 million$. Another relevant case occurred in 2015 in France, where two tanks (one containing gasoline, and the other containing naphtha) were set on fire because of a malicious act, causing damages of over 2 million $.

Since only three cases of environmental damage were registered for the chemical and petroleum sector, it was not possible to obtain relevant results for the other final outcomes. However, a relevant incident occurred in Italy in 2016. As a consequence of a malicious act, 2,600 tons of hydrocarbons (diesel fuel and heavy fuel oil) spilled from the pipes of a plant loading docks and poured through the sewer into the river Lambro and the river Po, causing huge environmental damage, confirming the possibility and potential severity of such consequences.

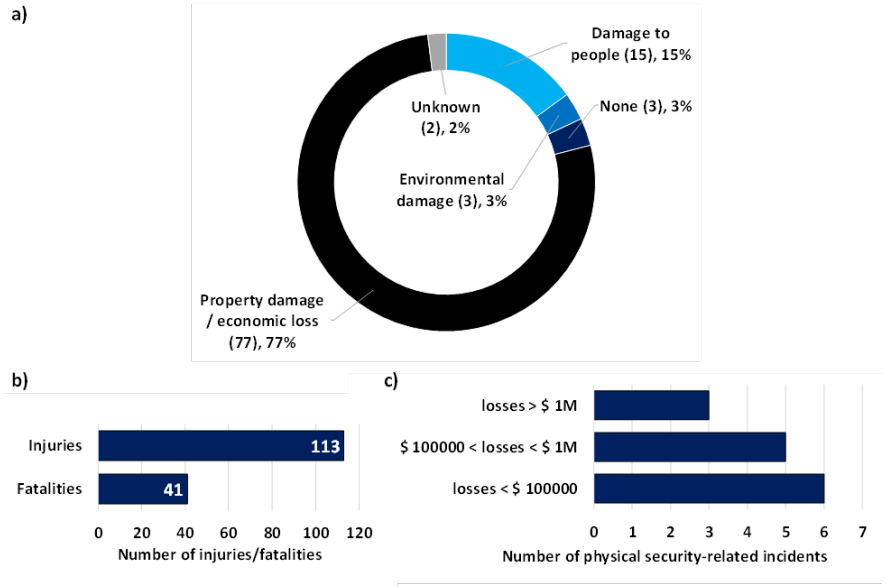


Figure 12. a) Distribution of the final outcomes in chemical and petrochemical facilities (based on 100 records). b) Number of injuries and fatalities (based on 15 records). c) Number of physical-SRIs with sufficient details to estimate the economic losses (based on 14 records).

6.2 Results from an analysis of cyber-SRIs (CSIs)

6.2.1 Characterization and steps of the cyber-attack

The general mechanism by which an attacker originates a cyber-SRI (CSI) is summarized in Figure 13. Definitions of key terms for cyber-attack characterization are presented in Appendix E. The attacker gives rise to a cyber-threat by exploiting vulnerabilities of the target system through one or more hacking techniques. Once a threat scenario takes place, there may be or may not be direct impacts on the assets of the facility under attack. This depends on the presence and effectiveness of security and safety countermeasures in the system under attack (Henrie 2013, Stouffer et al. 2008). Foot printing, scanning, gaining access, escalating privileges and final hacking are the well-known steps for cyber-attacks on IT systems.

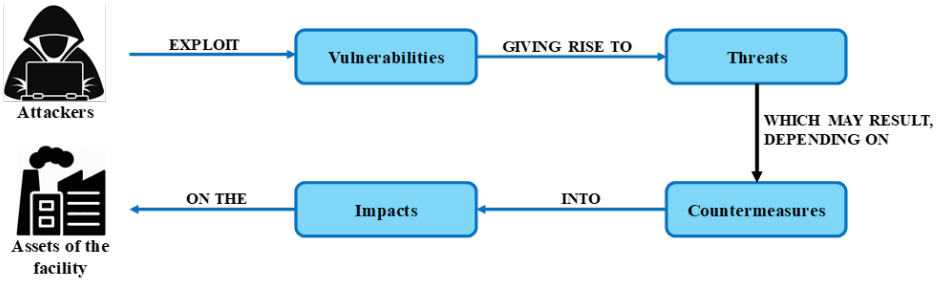


Figure 13. Mechanism of a cyber-attack.

Foot printing and scanning allow an intentional attacker to collect as much information as possible about the target system (e.g., reachable IP addresses, authentication mechanisms, network topology, etc.), and to identify the vulnerabilities which can be exploited in order to gain access (Ethical hacking 2019). The description of the recorded CSIs generally lacks information on these steps, as the details are usually unknown and/or undisclosed in public reports. Even in the well-known case of Stuxnet (CSI O in Table AY) only hypotheses are available regarding how the network system of the Natanz nuclear power plant was spied on (Appelbaum and Potras 2013).

Gaining access to the IT or OT system consists of penetrating the network of the target system through its vulnerable access points. Different types of attackers can access the network using different hacking techniques. Intentional external attackers obtain the necessary access information during foot printing and scanning phases. The analysis of eight CSIs with a sufficient level of detail from the database evidenced that different hacking techniques were applied in external attacks: brute force password-cracking (CSI Q), phishing (CSI R) and trojan horse (CSI C) attacks. Four entries of the database showed that gaining remote access can also involve physical actions on the IT-OT system, most commonly by use of infected USB sticks (e.g., in CSI P a USB stick connected to a computer started the spread of malware into the network). No recorded CSI featured an unauthorized attacker physically accessing the hardware to infect the system or launch the attack (i.e., a cyber-attack following a physical security breach).

Accidental attacks penetrate the IT network when they are able to exploit its vulnerabilities. For example, in CSI J an operator browsing external mail websites accidentally installed a mail-based trojan backdoor on an HMI workstation in the control room.

As regards intentional internal attackers, eight CSIs were documented in the database as being caused by individuals related to the target organization (e.g., employees, contractors, etc.). These attackers took advantage of their own credentials and knowledge of the system and were able to access at least some levels of the CIM network without the need for foot printing and scanning techniques. For example, in CSI N, a disgruntled employee accessed and disabled the leak detection system of three oil derricks on purpose using his own authentication

credentials. As insiders usually have extensive knowledge of the process and the plant, they are potentially a highly critical category of attackers.

Figure 14a shows the overall results of the analysis of the recorded CSIs with concern to the type of attacker. Intentional and accidental CSIs are found to be equally credible patterns (respectively 44 and 34 events). The figure confirms that external cyber-threats against process facilities were the more frequent CSI reported. Nevertheless, the role of insiders is also evidenced as a possible threat (about 10% of the total CSIs recorded).

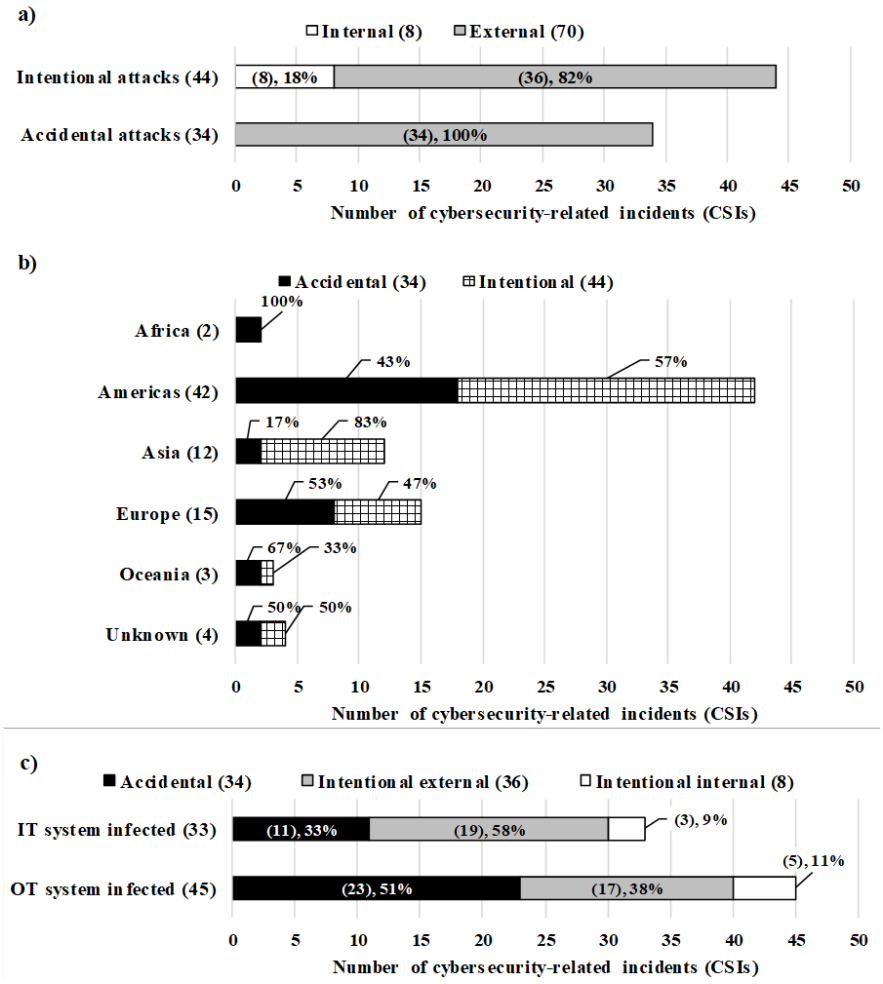


Figure 14. Distribution of the recorded CSIs: (a) based on the type of attacker; (b) with respect to the geographical areas; and (c) the affected CIM levels.

Figure 14b shows the geographical distribution of the events collected with respect to their nature (i.e., accidental/intentional). The figure seems to suggest that the distributions of accidental and intentional attack patterns are not influenced by geographical location, though for Asia a slightly higher percentage of intentional cyber-attacks were reported (i.e., 83%). In the case of Africa and Oceania, the percentages are not relevant, since only a few CSIs were recorded in the database (respectively 2 and 3 CSIs).

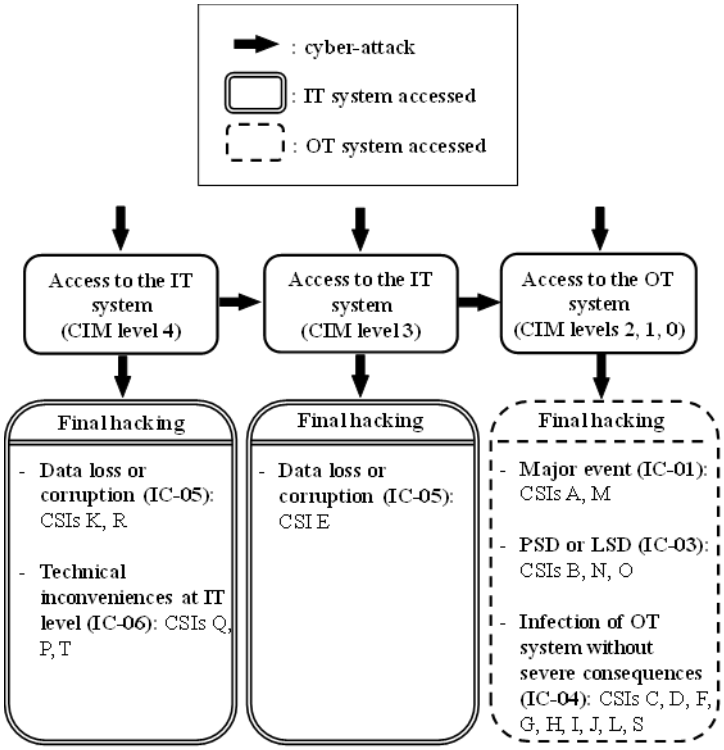


Figure 15. General steps of a cyber-attack on the IT-OT system of a process facility. The CSI that exploited the final hacking impacts identified are also shown in the figure (refer to the table in Appendix F).

The escalation of privileges consists of obtaining elevated access to resources that are normally protected from an application or user (e.g., admin, root, kernel resources), in order to manipulate the system more deeply [Rouse 2010]. In particular, this step is necessary to infect the OT system after access is granted to the IT system. The network of the OT system is generally a trusted network, separated from the IT system by means of network security systems (e.g., firewalls) (Boudriga 2010). However, six recorded CSIs confirm that a network design lacking firewalls (e.g., CSI H in Appendix F) or with an incorrect firewall configuration (e.g., CSI D and CSI I in Appendix F) can result in escalation of the infection spreading

from IT to OT systems. In CSI O (Stuxnet worm) the escalation of privileges used 0-day vulnerabilities (i.e., unknown computer-software vulnerabilities), allowing network security systems to be bypassed (Falliere et al. 2011).

The classification of the collected CSIs with respect to the type of system infected is reported in Figure 14c. As shown in the figure, there were more CSIs that affected OT systems than those that affected IT systems. As an attack on the OT generally implies a former intrusion in an IT system, this result could be a consequence of higher attention worldwide towards reporting attacks that resulted/may have resulted in physical effects in a facility.

Figure 14c also shows that an appreciable number of incidents classified as “accidental attacks” (i.e., 23 CSIs, 29% of the total) affected the OT system: therefore, the infection of the control system and/or supervision system is proven to be possible also in this case. Poor configuration of the IT-OT architecture, especially due to a low attention to security/cybersecurity issues, was tracked as the cause of these incidents.

The final hacking is the last part of the cyber-attack, leading to the reported impacts on the assets of the affected facility. Figure 15 shows the connection between the level of the network system achieved by the attackers and the impacts in selected entries of the database for which a detailed description was available. No recorded CSIs with an infection of the IT system alone resulted in impacts on the process system, confirming that gaining access to the OT is a distinctive feature required to achieve impacts on the physical system in the process industry. The analysis of the 5 CSIs for which more detailed information about the final hacking was available revealed some hacking techniques used by the attackers in order to achieve impacts on the assets of the target company. These consisted of: denial of service attacks (e.g. CSI G in Appendix F where the attacker made the traffic intermittent between HMIs, PLCs and the SCADA systems of a petrochemical facility), man in the middle attacks (CSI O, where signals between filed sensors and control rooms were intercepted and modified to carry out manipulation of process parameters), and data encryption attacks (e.g. CSI T in Appendix F, a ransomware attack on chemical companies in which attackers asked for payment for the release of the decryption key).

6.2.2 Impacts of the CSIs

Figure 16 reports the distribution of the collected CSIs with respect to the classes of impact. The potentially most severe impact (i.e., occurrence of a major accident) is also the least frequent (only two CSIs were recorded in the transportation of hydrocarbons by pipeline - see CSI A and N in Appendix F). The number of recorded CSIs generally increases progressing through the defined impact classes towards those with a lower severity. In particular, a higher level of occurrences were reported for impacts that required only access to the IT system. This can be explained by the presence of a higher number of safety and security barriers (e.g., safety instrumented functions, cybersecurity countermeasures, passive safety devices,

etc.) between the attacker and the target system when access to the OT system is required.

Furthermore, while the IT system of a process plant is generally similar to the one of other business sectors, the OT system resorts to proprietary and therefore specific design solutions. In other words, a deeper and more difficult scanning and escalating phase is required for an attacker who aims to infect the OT system rather than the IT system. Figure 16 also reports the potential impacts that can originate from a cyber-attack based on the level of access obtained by the attackers in the IT-OT architecture of the target process facility. In the figure, reference to the CSIs reported in Appendix F is provided for each impact class.

No fatalities followed the two major events triggered by the malicious manipulation of the control and supervision system that were collected in the database. However, huge economic losses (business interruption and repair costs, see CSI A) and environmental damage (e.g., the release of more than 30,000 barrels of oil in an area above an aquifer, see CSI M) were reported in these incidents.

Large economic losses were reported in a significant number of cases even without the occurrence of a major accident (IC-02). It should be noted that most incident descriptions provided only a verbal description of the economic losses (expressions such as “huge economic loss”, “significant financial impact”, “loss of production”, “loss of revenue” are frequent).

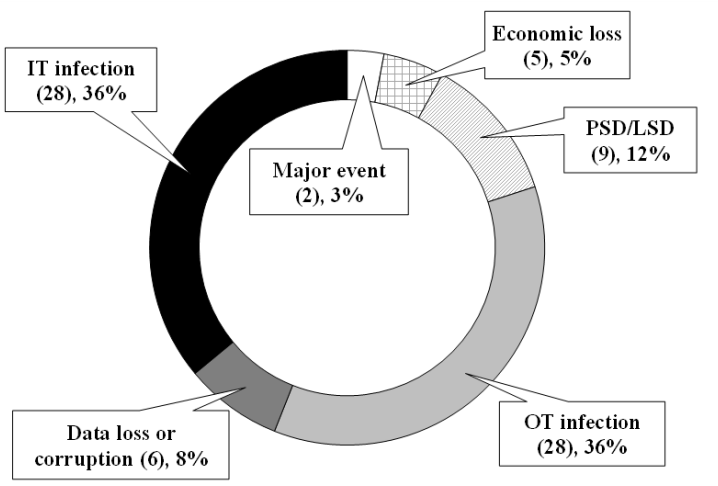


Figure 16. Category of impact recorded for the reported CSIs.

In eight recorded CSIs the attackers induced a local or process shutdown via remote manipulation (IC-03). For example, in CSI B (Appendix F) the attack resulted in the failure of the cooling system of a nuclear reactor, which triggered a shutdown. Recorded downtimes span from 30 minutes up to 1 week.

Several cases of infection of the OT (28 CSIs) resulted in no recorded severe consequences. A deeper analysis reveals types of incidents belonging to this category. These include: infections of the SCADA system (21 CSIs), short term loss of plant control (3 CSIs), malfunction of the detection system of dangerous substances (3 CSIs), remote manipulation of plant devices (1 CSE, see CSI S in Appendix F, in which control valves were manipulated).

Most of the CSIs, however, only affected the IT system. Data theft or corruption were recorded in six CSIs. These incidents featured sensitive data theft (e.g., plant history data) and data loss. The majority of attacks at the IT level only resulted in minor technical inconveniences (server crashes, PC locks, file encryption, etc.). Three CSIs also resulted in economic losses (recorded values span from £26,000 to £800,000).

6.2.3 Countermeasures and lessons learnt

The CSIs for which a more detailed description was available allowed some insights into the key role that security countermeasures may have in preventing such events. The definitions of countermeasures that can be implemented to reduce cyber-risks are necessarily specific to each system and require a detailed analysis of threats, vulnerabilities, and potential impacts (see e.g., ISO/IEC 27005 and ISA/IEC 62443).

Nevertheless, the deeper analysis of selected CSIs in the database revealed the following as key countermeasures for the process industry:

- Network segmentation. Network segmentation is highly recommended. It is part of a more general defence-in-depth strategy and it provides for the separation between the corporate network and the control and supervision network, allowing their communication only through properly controlled and configured devices (e.g., firewalls). CSI H in Appendix F evidenced the importance of this countermeasure: in fact, there would have been no infection of the control and supervision network if a firewall had been properly installed between the IT and the OT networks. Moreover, network segmentation provides a further separation of the internal network, with the addition of a DMZ (demilitarized zone), an isolated network which contains services accessible both from external unprotected networks, and from internal terminals of the company. CSI L in Appendix F would not have occurred if the network architecture contained a DMZ for the mail service.

- Proper configuration of firewalls. In addition to the highly recommended installation of firewalls for data filtering, proper configuration is important to reduce the possibility of firewalls being bypassed by malware. This mainly consists in establishing which data ports should be closed and which should be open. For example, CSI D in Appendix F would not have occurred if the firewall between the corporate network and the control and supervision network had been configured to block the intrusion of the Blaster worm virus. The same is true for CSI I in Appendix F, where bad configuration of the firewall together with the lack of other security barriers allowed the

infection of some HMI workstations in the control room of a petrochemical plant.

- Installation of antivirus software. It is recommended to equip each processor with antivirus software for the prevention, detection, and removal of malware. For example, CSI I in Appendix F occurred due to the lack of AV software on the HMI workstations that were infected.
- Authentication system. User authentication is recommended whenever users need to execute actions through a device connected to the network (e.g., by using passwords, tokens, biometric footprints, etc.) and the level of effectiveness of the authentication has to be as high as possible (e.g., long alphanumeric passwords with special characters). CSI F in Appendix F evidenced the possibility for an MUMU worm to gain the access to the network system of a petrochemical plant and to infect the fiscal metering system thanks to a weak admin password.
- Patch management. It is recommended to install all the available patches in order to update each computer program. CSI E in Appendix F would not have occurred if the corporate laptop had a patched version of msSQL.
- File encryption. It is recommended to encrypt files and transitioning data. The theft of confidential information to which the CSI K in Appendix F refers would not have had the same impact severity if the stolen information had been encrypted.
- Minimizing the use of USB devices. It is recommended to minimize the use of USB sticks since they are the most widely used means for the spread of malware, or at least, to test them through a detection system before use. For example, the Stuxnet propagation through the network system of the Natanz nuclear power plant (CSI O in Appendix F), started from an infected USB stick of an unaware employee.

The analysis of such selected CSIs confirms that the presence of general and unsophisticated countermeasures (such as those mentioned above) can prevent or mitigate the success of cyber-attacks on process facilities. This is even more important for accidental attacks, where foot printing and scanning phases are not carried out on the specific system. Similarly, for intentional cyber-attacks, the presence of multiple countermeasures (e.g., defence-in-depth) is an important defence strategy, as the attackers must perform complex attack patterns to generate impacts on the target systems. Finally, it should be remarked that an integrated design of physical and IT countermeasures may allow a more robust protection of the system.

6.3 Security scenarios

6.3.1 The bow-tie diagram approach and main results

The identification of reference physical damage scenarios triggered by intentional malicious attacks on process plants supports a more harmonized consideration of security and safety scenarios in integrated safety and major security event management studies. To achieve this goal, a bowtie (BT) diagram approach, which is widely used in safety studies, is followed.

The generic scheme of a BT is shown in Figure 17 and is used to represent possible major security event scenarios. The tree on the left side of the security event is the “Attack Tree” (AT), and on the right side is the “Event Tree” (ET). At the centre of the tree is the security event (SE), which is intended as an event (such as a loss of containment of a hazardous substance) that results in a loss of an asset, whether it is a loss of capability, life, property, or equipment (Center for Chemical Process Safety, 2003). Attack trees consider different attack modes (AM), which are the acts of interference (defined in terms of the instruments used and the level of penetration required) perpetrated by the attackers against the target process site (Störfallkommission, 2002).

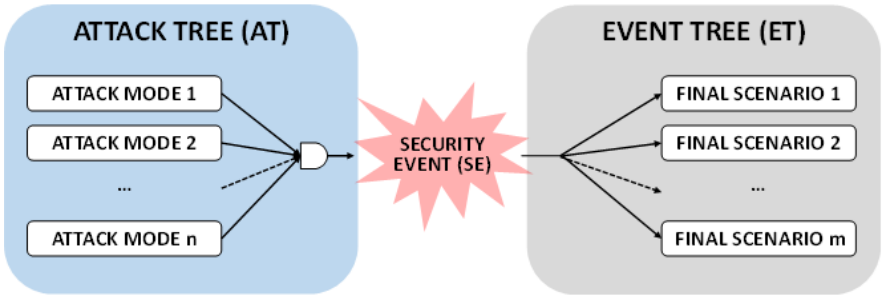


Figure 17. Scheme of a generic bowtie diagram (BT).

6.3.2 Definition and validation of attack modes (AMs)

The first phase was aimed at the definition of a set of attack modes (AMs) perpetrated by the attackers. The set of attack modes should consist of a list of generic but clearly defined types of physical attacks on a process plant (process and storage units) that can be carried out by single individuals or an organization. Cyber-attacks or physical attacks (unauthorized physical accesses) on the control room were explicitly considered to be beyond the scope of the assessment, as their mechanism strongly depends on the design of the process and control system. A dedicated approach for this purpose (PHAROS, Process Hazard Analysis of Remote manipulations through the cOntrol System) was developed within the activities of the current project (Iaiani et al., 2021).

The set of attack modes was identified from an analysis of the current main security vulnerability assessment (SVA) and security risk assessment (SRA) methods, with particular attention to their applicability to the context of process plants. Analysed sources include: Störfallkommission (Hazardous Incident Commission) (2002), CCPS methodology (Center for Chemical Process Safety, 2003), VAM-CF methodology (Jaeger, 2002), API RP 780 SRA methodology (American Petroleum Institute, 2013), and the RAMCAP methodology (Moore et al., 2007), Landucci et al. (2015), and Landucci et al. (2017). Table 5 reports the descriptions of the set of AMs adopted, their corresponding attack vectors, and criteria for success.

Table 5. Definitions of the set of AMs adopted in the present study, also showing the attack vectors and the success criteria.

AM code	Attack mode	Description	Attack vector	Success criterion
#01	Deliberate interference with or w/o aids	Deliberate acts involving simple operations without the use of instruments or using tools and aids that are present on site	n/a	Target installation location is reached
#02	Arson using incendiary devices	Incendiary attacks	Heat load	Target installation damaged due to external fire exposure
#03	Use of explosive	Use of explosives to blow up tanks and pipelines or to blow up load-bearing structures to cause the collapse of tanks	Overpressure	Target installation damaged due to overpressure effects of explosion
#04	Use of vehicle bomb	Use explosives (placed inside a vehicle) to blow up tanks and pipelines or to blow up load-bearing structures to cause the collapse of tanks	Overpressure	Target installation damaged due to overpressure effects of explosion
#05	Shooting	Interference at close distance, using various types of weapons	Projectile impact	Perforation and/or penetration of target installation due to projectile impact

Validation of the AMs was carried out on the basis of the information available in the security-related incidents collected for the chemical and petrochemical (C&P) sector in the database populated by Casson Moreno et al. (2018) and updated by Iaiani et al. (2020). In particular, suitable records in terms of relevant information, were classified according to the set of proposed AMs. This helped to check the set of proposed AMs was complete (i.e., that all records can be classified), unambiguous (i.e., a single class could be defined for each record), and exhaustive (i.e., at least one record can be identified for each class).

The validated AMs are reported in Figure 18. The numbers contained in the tags on each branch refer to the number of incidents recorded with the information available on the specific attack carried out by the attackers. The use of explosive devices (AM#03) was a very common attack mode: this type of attack is usually carried out by highly capable and well-motivated adversaries such as terrorist organizations. Additionally, incendiary attacks (AM#02) were found to be a typical attack pattern: the reason behind this is probably related to the fact that this AM does not require the attackers to be highly equipped or well-motivated. Overall, all the categories of AMs considered in the present study and described in Table 4 have been validated.

In 22 records out of those considered, a release from a physical piece of equipment was specifically reported, or, the information available on the physical scenario triggered by the security attack (e.g., pool fire, fireball, flashfire, fire etc.) was sufficient to imply a loss of physical integrity of the equipment/items containing hazardous substances.

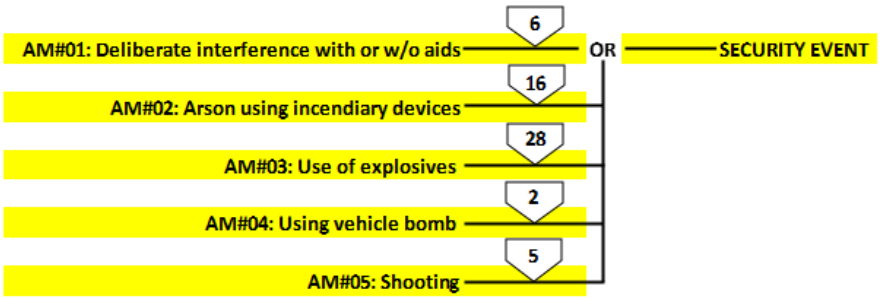


Figure 18. Set of attack modes (AMs) considered in the present study. The highlighted branches are those validated by past incident analysis. The numbers in tags refer to the number of incidents recorded in the database for the chemical and petroleum sector (Iaiani et al., 2020).

6.3.3. Definition and validation of attack trees (ATs)

The same attack mode will result in different damage on the basis of the characteristics of the target (e.g., type of equipment, design pressure) and on the minimum distance from the target unit that the attacker can reach. The second phase of this study was aimed at the definition and validation of attack trees (ATs) for a set of reference installations. ATs are graphs that represent the chain of a security breach leading to a security event (Abdo et al., 2018). In the present study

the AT for each reference installation is formed by two elements: attack modes (AMs), and the security events (SEs).

The set of reference installations considered in the present analysis were adapted from those proposed by MIMAH (Delvosalle et al., 2006) and Tugnoli et al. (2013), which feature the more common cases of large amounts of hazardous materials found in the storage areas of typical process plants. In particular the following reference installations were considered:

- atmospheric storage unit (cone roof tank, horizontal cylindrical tank, floating roof tank).
- pressurized storage units (horizontal cylindrical tank)
- storage warehouse (storage of solids in small packages, storage of liquids in small containers).

Table 6. Validation of attack trees (ATs) in a tabular form. The numbers refer to the number of incidents recorded by Iaiani et al. (2020) featuring suitable information. The AM#-codes refer to the attack modes defined in Table 5.

Attack Mode	Atmospheric storage unit	Pressurized storage unit	Storage warehouse
AM#01	**2**	0	**2**
AM#02	**1**	0	**8**
AM#03-a	**3**	0	**1**
AM#03-b	**2**	0	0
AM#04	0	0	0
AM#05	0	0	0

Validation of the ATs was carried out with the support of the information available in the security-related incidents collected for the chemical and petrochemical sector in the database populated by Iaiani et al. (2020). Table 6 reports the results of the validation of the ATs for each reference storage unit installation in a tabular form.

In case of atmospheric storage units there is historical evidence of loss of physical integrity leading to a release caused by almost all of the attack modes considered in the present study (see Table 6). Two incidents show that for this type of installation, releases of hazardous substances are also possible thorough deliberate interferences with or w/o aids (AM#01). In one case (occurred on 16/05/1989 in France) vandals caused the release of 8,000 L of oil with consequent environmental damage (French Ministry of Ecology); while in another (occurred on 23/02/2010 in Italy), attackers targeted a storage tank farm at a petrochemical plant inducing the release of 2,600 tons of hydrocarbons (diesel fuel and heavy fuel oil) (Major Accidents Hazards Bureau). Incendiary attacks (AM#02) and those using man-carried explosives (AM#03-a) leading to physical damage scenarios were also validated (respectively one and three incidents). For example, in an incident which occurred on 11/04/1970 in the United States unknown threat actors attacked an atmospheric storage tank of the Dow Chemical Company both using explosives and gasoline-based incendiary weapons (National Consortium for the Study of Terrorism Responses to Terrorism): five people were injured by the flying fragments of the tank and an estimated $250,000 in damage was caused to the company. As

reported in Table 6, AM#04 (use of a vehicle bomb) and AM#05 (shooting) could not be validated. However, this does not mean that they are uncommon attack modes. In fact, on 25/12/1999, unidentified attackers detonated a car bomb containing 20 kg of dynamite in the industrial section of Paloquemao in downtown Bogota (Colombia), injuring two people. Even though physical plant equipment was not damaged by the explosion, this event shows that this type of attack on industrial facilities is possible.

In case of pressurized storage units, no incidents collected in the database allowed the validation of any branch of the AT (see Table 6). However, this does not mean that it is not possible to cause loss of containment in such installations through the set of AMs adopted in the present study. In fact, a recorded incident, proves that equipment under pressure, even if not devoted to storage, may be damaged by security attacks. In this case, as a consequence of a terrorist attack (not further specified) on a petrochemical plant, a significant amount of flammable gas was released into the atmosphere from process equipment under pressure, forming an explosive cloud that was ignited resulting in an explosion (Major Accidents Hazards Bureau).

In the case of storage warehouses, an incendiary attack (AM#02) was by far the most common AM among all the cases concerning storage buildings (see Table 6): this is probably due to the high presence of flammable materials contained (e.g. paints, solvents) which can be ignited resulting in fires, as well as the presence of solids that can decompose at high temperature causing explosions. For example, in an incident which occurred on 26/06/1988 in Hungary, a former employee crawled into a warehouse storing 23 tons of flammable liquids (paints thinners, white spirit, toluene, and xylene) and lit a fire using a cigarette for ignition (French Ministry of Ecology). Despite the fact that only two incidents were found, deliberate interference with or w/o aids (AM#01) is deemed to be a very common attack mode for storage buildings. Attackers are required to perform only very simple actions such as removing caps from containers, opening manual taps or breaking bags. For example, in an incident which occurred on 02/10/2009 in France, attackers forced open containers of paint products (primarily acrylic resins and urethane in ethyl acetate) causing their release onto the ground and the consequent pollution of the Airaines watercourse (Category I) via the stormwater network (French Ministry of Ecology). On the contrary, the use of explosives lifted by a drone (AM#03-b), is deemed to be a very uncommon AM for these installations given the fact that storage buildings are typically enclosed areas and drones are not able to enter. Similarly, also shooting (AM#05) can be considered unlikely as releases of greater or equal intensity than those that can be triggered via this AM can be achieved through deliberate interference (AM#01) more easily.

6.3.4 Example of a bow tie (BT) diagram for the storage of flammable liquids

The third phase was aimed at the development and validation of security-related bow tie (BT) diagrams for reference substances.

The security-related BTs were built combining attack trees with event trees (see Figure 17) which were commonly available in the literature (in this specific case the ETs were adapted from MIMAH (Delvosalle et al., 2006)), and displaying primary,

secondary, and final scenarios triggered by such attacks. The ETs are tailored with respect to the specific hazardous and physical properties of each reference substance and the type of storage installation based on common approaches in safety assessment (e.g., MIMAH (Delvosalle et al., 2006)).

An example BT diagram for the storage of flammable liquids is shown in Figure 19.

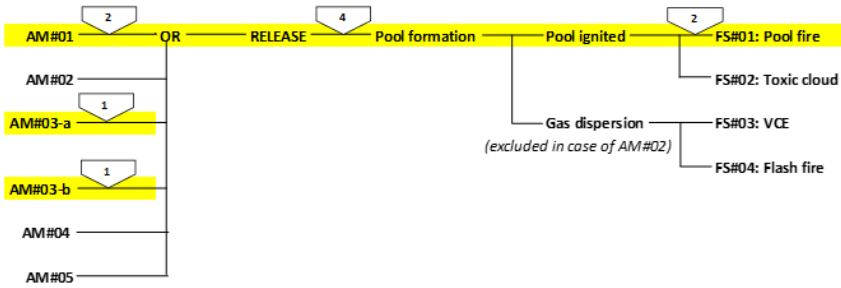


Figure 19. A bow tie diagram for the atmospheric storage of flammable liquids. The highlighted branches are those validated by past incident analysis. AM#-codes refer to the attack modes defined in Table 4; FS#-codes refer to the final scenarios defined in Table 7.

In the BT results above the primary event is the formation of a pool, which was validated by four incidents (see tags in Figure 19). A pool fire (FS#01, see definition in Table 7) is the final scenario that occurs in the case of immediate ignition of the pool. This happened in two events recorded in the database (Iaiani et al., 2020). In the first incident (14/07/2015 in France), 2,000 tons of naphtha and 1,000 tons of gasoline were released from their respective storage tanks resulting in pool fires after the detonation of explosive devices (AM#03-a) (Major Accidents Hazards Bureau); while in the second (14/09/2019 in Saudi Arabia) the pool fires were the result of a drone attack (AM#03-b) that caused the release of oil from 14 storage tanks (bbc.com, cnbc.com, nytimes.com).

If the combustion conditions produce large amounts of toxic compounds, a toxic cloud (FS#02) may be associated with the pool fire, and toxic effects are added to those related to the heat load.

As regards the secondary event “gas dispersion”, this is excluded in the case of low volatile liquids and in case of incendiary attacks (AM#02) given the presence of an immediate source of ignition (i.e., the arson intentionally triggered by the attackers). If a delayed ignition occurs after gas dispersion, a vapour cloud explosion (VCE, FS#03) or a flash fire (FS#04) may occur depending on several factors such as the reactivity of the substance involved, the turbulence of the gas cloud, the level of confinement, and the explosive gas mass.

Overall, the formation of a pool is deemed credible for all the AMs considered, and its ignition is highly probable in the case of incendiary attacks (AM#02) and can also occur in the case of attacks using explosives (AM#03 and AM#04). All the other scenarios are considered unlikely.

Table 7. Definitions of the final scenarios (FS) displayed in the BT of Figure 19, adapted from the "Yellow Book" of TNO (Van Den Bosh, and C.J.H. Weterings, 2005).

FS code	Final Scenario	Description
FS#01	Pool fire	The combustion of material evaporating from a layer of a flammable liquid.
FS#02	Toxic cloud	Atmospheric dispersion of a gas or aerosol, which is toxic to humans by inhalation.
FS#03	VCE	An explosion resulting from an ignition of a premixed cloud of flammable vapour, gas or spray with air, in which flame acceleration and partial confinement cause the formation of blast wave.
FS#04	Flash fire	The combustion of a flammable vapour and air mixture in which the flame passes through the mixture at less than sonic velocity, such that negligible damaging overpressure is generated.

7. Integrating safety and security management in Seveso plants

This chapter summarises the motivations and prerequisites for the integrated management of safety and security, the main similarities and differences between the concepts and management of safety and security, as well as the main challenges and possibilities for integration. This examination builds on the literature review of the concepts and management of safety and security, and on the interviews with the representative of Seveso establishments and regulators. In addition, this chapter provides a summary of the guidelines for the integrated management of safety and security in Seveso establishments.

7.1 Motivations for integrated management

There are several motivations for the integrated management of safety and security in process-industry and Seveso plants. These motivations are partly overlapping and closely connected to one another. We have identified five main motivations. These include: 1) economic reasons; 2) synergies based on mutual interactions and influences; 3) avoiding conflicts deriving from competing logics and related contradictions; 4) increasing resilience in chemical plants; and 5) inadequate approaches regarding new emerging risks.

1) Economic reasons refer to achieving cost-efficiency and cost benefits regarding aspects such as protection measures that are suitable for both safety and security domains (Kriaa et al. 2015; Reniers et al. 2011: Reniers and Amyotte 2012). For instance, using cameras to observe both safety and physical security risks is an example of cost-benefits and synergies between safety and security management.

2) Safety and security have mutual interactions and influences (e.g., Song et al. 2019; Chang et al. 2015; Kriaa et al, 2015; Pièrre-Cambacédès et al. 2013). An example would be an insider (security) threat, such as embittered employee, who intentionally leaves valves open and harms the industrial processes, and thus influences safety. Another example would be an external cyber-attack against the Seveso plant's operating system that could have severe process-safety 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.

3) Avoiding conflicts arising from competing logics and related contradictions, refers situations such as when the management of safety relies on openness and transparency, whereas the management of security requires the concealment of data. Reconciling these contradictory aspects requires coordination (Borodzicz 2005; Smith and Brooks 2012; Reniers and Khakzad 2017).

4) The goal of increasing resilience in chemical plants and the process-industry, means that systemic risks arising from the interconnectedness of technological systems and the related risks and human and organizational factor-related risks need to be identified and prevented, and that requires better understanding of

systemic risks and vulnerabilities of different systems and the whole plant (Young and Leveson 2014; Reniers et al. 2014; Harvey and Stanton 2014).

5) Pure safety or pure security approaches cannot identify and mitigate risks to the industrial automation and control systems (Boyes et al. 2018; Schulman 2020; Young and Leveson 2014; Kriaa et al. 2015; Reniers et al. 2014). Similarly, traditional safety and reliability approaches have not included cybersecurity risks. Therefore, the integrated management of safety and security risks is required.

7.2 Prerequisites for integration

Integration requires understanding of what is meant by integration, management, safety, and security. In addition to understanding of the contents of the concepts, also understanding the similarities and differences between the concepts is necessary for successful integration.

Integration can be divided into 3 levels: structural, functional, and cultural integration (Jorgensen et al. 2006). Structural integration can entail the integration of elements from different systems, such as elements from different standards, or the integration of organizational units, for example, a unit that takes care of environment, health, safety and security (EHS&S). Functional integration refers integrating processes and procedures, and here we refer again to EHS&S from the viewpoint of management system. This provides a framework that guides the evaluation, measurement, and continuous improvement of safety and security in an integrated manner. Cultural integration is the deepest level of integration. It entails shared understanding of the need for integration, and shared values that support safe and secure performance in an organization in a coordinated manner (Jorgensen et al. 2006; IAEA 2008; IAEA 2017; van Nunen et al. 2018).

The concepts of safety and security we have defined in Chapter 3.1. Regarding the differences and similarities between the safety and security risks, the different origin is evident. Security risks are intentional and derive from malicious human intent, whereas safety risks derive from the biophysical world (e.g., extreme weather conditions, or technical failures), but also from human and organizational factors and are unintentional by nature. Despite the different origins, safety and security risks can have similar consequences, i.e., incidents and accidents. In addition, safety and security management have similar goals that refer to the prevention of accidents and losses (Reniers et al. 2011).

Both safety and security risks can be divided into external and internal risks. External security risks include cyberattacks made by outsiders and physical security risks that consists of terrorism, sabotage, and thefts carried out by outsiders. Instead, internal security risks refer to insider threats, e.g., embittered employees. In the management of insider threats, different means can be utilised: colleagues can look after each other, supervisors play an important role in the prevention of insider threats, in addition, personnel management, HR, and occupational health care are also involved. Insider threats are a security question, but it is also a

question of mental well-being, and thus the management of insider threat exploits several means.

Similarly, safety risks can be divided into external and internal risks. External safety risks refer to risks related to the biophysical world, but also a poor safety culture of suppliers may create safety risks. External safety risks also include economic risks, such as economic depression, that may indirectly affect the company by creating pressures which company needs to answer, e.g., by cutting the budget regarding investments in safety or maintenance. Internal safety risks refer to technical deficiencies, human and organizational factors such as organizational changes, and poor safety culture within a company. From the point of view of integration, it is of great importance to examine the different management strategies, procedures, and processes in the safety and security domain and to reflect upon which strategies and processes could be combined.

Further differences between the safety and security domain can be found in the mindset and management. By mindset we refer to the main assumptions, and principles guiding safety and security activities as well as the understanding of what is valuable in terms of safety and security. In the safety domain, openness and transparency is seen as serving safety best. For instance, in the context of a safety culture, a questioning attitude and shared concerns are necessary for the improvement of safety (IAEA 1991; Reiman and Rollenhagen 2018). Instead in the security domain, the concealment of data is typical, and openness and transparency are possible only within a trusted community of experts dedicated to security issues (Borodzicz 2005; Smith and Brooks 2012). Furthermore, trust in colleagues, supervisors, and subordinates characterises the safety domain, whereas in the security domain continuous checks of trustworthiness are a crucial part of security (IAEA 2008). This does not mean distrust, but the reality is that this can be conceived as distrust by employees as shown in the aviation context (e.g., Pettersen and Bjornskau 2015).

Regarding the differences between safety and security management, it is not possible to manage security by a single company alone, whereas safety management is in the hands of one company (Borodzicz 2005; Smith and Brooks 2012; Jore 2019). Let us clarify this further. A single company does not have adequate information or means to manage security. For instance, in order to obtain situational awareness, security management is dependent on other companies and agencies, such as the police, border guards, intelligence agencies or companies providing security services. Instead, in the safety context, a company is not similarly dependent on others, even though in the high-risk industries, companies exchange information about good practices and incidents and accidents with other companies in the same sector. Even though there are differences in the management of safety and security, there is also a lot of potential for integration, e.g., in terms of risk analysis (Askeland et al. 2017; Amundrud et al. 2017; Cormier and Ng 2020) and attempts to create necessary organizational barriers to safety. By organizational barriers we refer to management and leadership, competencies, safety and security culture, and training, which all support attitudes and awareness relevant to safe and secure performance.

It is of great importance to understand the main differences and requirements regarding the safety and security domains regarding integration. In addition, there is a need for communication and the co-construction of an understanding of the integration-related needs and possibilities within the company. Moreover, the integration of safety and security management requires understanding the interfaces between safety and security. Regarding cybersecurity training, this could combine aspects from security culture, focusing on intentional harm, and aspects from safety culture focusing on ignorance and negligence.

7.3 Current state and development of integrated management of safety and security in Seveso establishments

This introduction to the current state and development of integrated management in Seveso establishment builds on the findings from the literature review and the interviews with the representatives of Seveso establishments. This presentation aims not to be exhaustive but provides indicative results and ideas for further development of integration. Apart from one, the companies interviewed represent multinational companies with headquarters in the USA and Europe, and several sites in different countries in Europe, and follow similar procedures and 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.

The Responsible Care management system is a well-known global declaration of sustainability, safety and security in the chemical industry context, and this system along with environment, health, safety and security (EHS&S) management systems have been adopted by Seveso establishments. The Responsible Care system and EHS&S represents structural integration in the sense that they integrate elements from different standards. In addition, Seveso establishments also have special organizational units or teams focused on EHS&S, which represent structural integration. Moreover, EHS&S refers also to functional integration in the sense that it provides a procedure and framework for evaluation and measurement of safety and security management. However, we could not get adequate information via the interviews concerning the status of cultural integration, which is the deepest level of integration and would mean that there would be a shared understanding and values regarding the integration in organizations.

There are several promising ongoing development processes in Seveso establishments in terms of integrated management. These entail the involvement of IT experts in discussions of process-safety and process-automation issues, as well as incident report systems that combine both safety and security incidents into the same system. In addition, there were separate developments, such as the development of methods for security vulnerability analysis and separate audits for process-safety. These separate developments are also essential, as special understanding of safety and security domains needs to be maintained and developed, even in the context of integration. However, integration is essential in

order to tackle systemic risks. Thus, from the integration viewpoint, it would be relevant to consider whether the development of methods for security vulnerability analysis could be integrated into safety risk analyses, and whether the separated audits for process-safety could include also cyber-security aspects.

Despite many good development processes in Seveso sites, it seems that integrated management is not yet adequately developed in terms of risk analysis and risk management. The potential for the examination of cybersecurity risks, physical security risks and process-safety risks and their significance together e.g., in Hazop studies or bow tie analyses is not yet fully exploited.

From the integrated management viewpoint, the clearest structural aspect that may create silos is that cybersecurity issues are handled by IT departments that are separated from departments that take care of EHS&S aspects. From the integrated management viewpoint, this is one important structural issue that does not contribute to integration optimally. Even though, the interviewees emphasized that the interaction between EHS&S and IT was good, the interaction may not be adequate to ensure a shared understanding of the convergence of cybersecurity, physical security, and process-safety risks.

Development of integrated management of safety and security

Despite the separation of IT and EHS&S units, we do not suggest incorporation of these units to avoid silos but establishing permanent forums where both the IT experts and process-safety experts can collaborate and co-construct better understanding of emergent cybersecurity, physical security, and process-safety risks. It would be of great importance to train IT experts to reflect upon how the cybersecurity risks might materialise in process-safety risks, and to train process-safety experts to reflect upon the potential of cybersecurity interference if there is a broken device or disturbance in the process.

It is possible to distinguish between the integration of safety and security in a single plant and the multi-plant context. What could the integrated management of safety and security mean in a multi-plant context, such as an industrial park?

The list of synergies below is not exhaustive, but it provides ideas of potential ways of collaborating in a multi-plant context. Some items from the list are already in use in industrial areas or industrial parks, but there is also room for improvement.

Integrated management in a multi-plant context

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

It is much easier to integrate management within a single company compared to a multi-plant context, as there are different goals, strategies and cultures that make integration more challenging. In addition, the sharing of costs regarding integrated management would be an issue (e.g., Reniers et al. 2014). However, in the multi-plant context it is important to understand the risks that other chemical installations in the same area may cause, as installations can be linked in terms of the danger they pose to each other. Often a small fracture of events may cause dramatic impacts. This is called power-law distribution (Reniers et al. 2014). Without knowing the power-law distribution, it is not possible to deal with systemic risks.

Single issues that relate to the integration of safety and security aspects which were raised by the interviewees in this study included the security of the transportation of hazardous chemicals, and security checks/clearance of safety process experts. There are currently language requirements for drivers and training that drivers need to pass before they gain access to a site. Even though the identity of the drivers is checked, a challenge exists in how to ensure that the person is who it says on their identity card. Another issue that arose from the interviews was the suggestion to make security clearance for process-safety personnel obligatory before they are employed, so that their backgrounds have been checked. This would be one way to tackle the insider threat. Furthermore, employees' use of drugs or alcohol was expressed as concern. This is not yet very big concern, but recently more cases have appeared.

7.4 Institutionalisation of IMSS and the role of regulators

Current laws and the Seveso directive do not require integration. However, a prerequisite for establishing an efficient IMSS system would include laws that support integration. However, amendments of existing laws and regulations would require broad acceptance by the industry, regulators, political decision-makers, and the public. Acceptance is dependent on the proper understanding of converging risks and the need to tackle them in an integrated way. Opposition to integration may be due to the fear of increasing duties while resources in the industries and regulators remain the same. Furthermore, IMSS would require new competences and expertise, and that would mean more financial and human resources.

If there were laws supporting IMSS, regulators could better contribute to IMSS. Without laws the regulators cannot do much. Furthermore, there are no ISO standards regarding the integrated management of safety and security. Thus, the institutional support for integration is rather weak.

There are ways in which regulators could contribute to IMSS. Regulators could create criteria for evaluating the quality of collaboration between the companies located in the same area. This collaboration could include common exercises regarding integrated safety and security risks, common safety and security strategies, sharing best practices, and targets for development in each company, sharing a system that includes both safety and security incidents, and the integrated

analysis of incidents. The benefits of close collaboration would be better common understanding of risks that the neighbouring organizations have, and proper understanding of safety and security vulnerabilities of the industrial area.

Furthermore process-safety regulators could make joint inspections with other regulators to single companies. This is occurring already now. However, these joint inspections could be made as a habit, as the interviewees reflected that joint inspections provide valuable knowledge to both sites and regulators. All participants benefit from them. In a multi-plant context, it could be possible to organize one joint meeting between all companies where the common issues, risks, and vulnerabilities could be handled so that better awareness could be formed, and this could contribute to better collaboration between the companies and better ways to mitigate the risks in a coordinated way.

7.5 Guidelines for integrating safety and security management in Seveso plants

One result of this research project are the guidelines for integrating safety and security management on Seveso plants. These are published on the website of the SAF€RA consortium https://projects.safera.eu/projects/ and the SAF€RA 4STER project www.vtt.fi/safera4ster

The guidelines provide guidance on what to consider when designing and implementing integrated safety and security management. The guidance covers different aspects of management including: a) recognition of the context of organization; b) leadership; c) planning; d) support; e) operation; f) performance evaluation; and g) improvement.

These aspects are derived from a high level structure, which was formulated by the International Organization for Standardization (ISO) in order to structure their management standards. The aspects comprise a continuous development cycle: plan - do - check - act, which is an important part of management.

In these guidelines integrated management means connecting, coordinating, and combining safety and security management activities in order to exploit synergies and to resolve conflicts between them. Understanding and recognizing their similarities and differences, and their intertwined nature is essential for carrying out integration. Integration may be implemented in structures and functions, and it promotes the creation of a new integrated culture, which also needs to be managed.

Structural integration, for example combined organizational units or documented integrated system (structures), forms a stabilizing framework for the integration of operations, but it does not automatically create integrated management. Integrated operations are formed by common activities and interactions are required for integrated management. Therefore, the promotion and improvement of integrated operations are key tasks in integrated management. Integrated management also has an important role to play in the creation of an integrated safety and security

culture, which includes a shared understanding of proper ways to integrate safety and security in operations. An integrated culture extends the effect of integration above the planned and instructed operations.

The effective integration of activities requires motivation. There is both need for integration and expected benefits from it. The need stems from increasing cyber security threats concerning plants involving major chemical hazards and the management of such threats requires an integrated approach. The increased threat is based on the rapid digitalization, i.e., use of new digital technologies in chemical plants. Benefits of integration also include convenience, improved safety and security performance, resource optimization, and increased resilience. It is important that the management of an organization understands the need and benefits and communicates them to the personnel. Moreover, the importance of integration should be evident in different management activities.

The potential activities, in which safety and security management could be combined, include, for example, risk assessment, incident reporting, emergency management, change management, and informing the public. Joint risk assessments could include joint identification of security threats and major accident scenarios, joint risk evaluation including both aspects, and means of prevention affecting both safety and security. The same system could be used for reporting safety and security incidents and, moreover, both safety and security implications could be examined when incidents are analysed. States of emergency and change are critical for both safety and security, and it is important to manage them taking into account the integration aspects. Safety and security training could be combined, which would make it also natural to handle the integration viewpoint. There is plenty of information which is relevant to both safety and security management. Conflict may arise because of different information management premises of safety and security management. Safety also benefits from open information sharing, which is required to a certain extent. On the contrary, security management controls and limits the availability of information. Integrated information management policy and practices are needed to avoid and overcome conflicts arising from this duality.

Safety and security are intertwined topics comprising both common and different aspects. Both specific safety and security knowledge and integrated management are needed. Simply combining and communicating between safety and security domains is not sufficient because of the intertwined and complex nature of present safety and security issues and risks. A new integrative mind-set will be required in the future.

8. Discussion and conclusions

We will first summarise and discuss the results of the different subprojects of this study. Then we reflect upon the overall picture that the results together provide. We will reflect upon the impacts of this study for the industry and regulators, as well as further research needs regarding the integrated management of safety and security.

8.1 Summary and discussion of results

Survey results and interviews

The survey results, despite being only indicative due to the small response rate, can be examined together with other results, such as with the interviews. The survey respondents had a strong confidence in cybersecurity in their organizations. Cybersecurity is often managed by the IT department. Even though the survey showed little evidence of integration between safety and cyber security management—only one respondent referred to that safety and cybersecurity risks are managed in an integrated manner—the collaboration between safety and security managers was reported to occur at regular intervals, either weekly or monthly. Besides, the interviewees described collaboration with the IT department being good. The best example from the integrated management perspective included cybersecurity experts participating in meetings regarding process-safety and process-automation issues.

The survey results showed also that organizations report numerous interventions used to safeguard their cyber security on a human, policy, and technology level. These include awareness campaigns, enforcing strong passwords, and the use of VPN. In addition, the interviews showed that cybersecurity training has become more frequent over the last five years. In the multinational companies, employees are trained frequently against cybersecurity threats. However, the interviewees mentioned that knowing what cybersecurity would require and behaving in such a way in practice are two different things. Furthermore, large corporations have sent fake phishing mails to check their personnel's vigilance in terms of cybersecurity threats. According to one IT security expert, the result of a cybersecurity exercise was that all stakeholders including the city, first responders, representatives of regulatory body and industries all opened the "contaminated" mail. This indicates the need to continue with exercises. However, the result also leads us to reflect upon more efficient ways of affecting people's performance. For instance, we can make an analogy with smart homes and technologies that guide humans to sustainable energy consumption, without the need to think or choose it. Similarly, it is possible to design smart IT systems that guide humans to secure ways of acting without them needing to make choices. However, technological tools would not do away with the need for increasing of cybersecurity awareness.

All participants of the survey reported that no negative outcomes had been suffered as the result of a cybersecurity incident. Although this is possible, it also

aligns with the general attitude of secrecy surrounding this topic. Organizations are generally unwilling to share much about the status of their cyber security. This is because cybersecurity incidents are regarded as providing a bad image of the trustworthiness of the company. However, sharing information would boost learning and resilience towards future events and threats.

Another relevant aspect to reflect upon is that occupational safety incidents were seen as the least likely outcome of a cybersecurity breach. Unfortunately, there were no questions on the effects on process safety in the survey. However, as the current trend is towards growing digitalisation, automation and blurring boundaries between the IT and OT systems in high-risk industries (e.g., Boyes et al. 2018), both occupational safety risks and process-safety risks induced by cybersecurity interferences must be taken seriously. Therefore, raising the cybersecurity awareness in Seveso establishments is relevant.

Past incident analysis

The past incident analysis focused on physical security and cybersecurity induced incidents globally. The total number of cases was 369. Regarding the trend of both physical security- and cybersecurity-related incidents, two peaks were found one in the period of 2000-2004 (75 security related incidents) due to the high number of cyber-attacks in the world, and one occurred in 2010-2014 (80 security related incidents) due to a high number of physical attacks in the world. Instead in the last period of 2015-2019, there were fewer reported security related incidents compared to the earlier periods (see Appendix D). Obviously, companies have increasingly adopted cyber risk analyses in the management of their IT and operational technology (OT) systems but the decreasing trend might also be because of under reporting. In any case, the decreased trend in 2015-2019 should not be interpreted so that cybersecurity is seen not be a relevant issue currently or in the future. At least the recent news of cybersecurity attacks on government agencies in the US (https://news.cgtn.com/news/2020-12-14/U-S), as well as increasing digitalisation in industries provide strong hints at an increasing need for vigilance regarding cybersecurity attacks.

Terrorism was the most important security threat category (104 incidents) for industrial installations, and the outsider cyber threat (73 incidents) was the second most important threat category for all industrial sectors. In the chemical and petroleum sector, cyber-attacks (i.e., an attack via cyberspace on the IT-OT network of a facility) were the most common attack mode (34 incidents). However, in the case of infection of an OT system, the impacts on the facilities were the infection of the HMI workstations (12 incidents) and a local or process shutdown (5 incidents), and no major events occurred in chemical of petrochemical facilities due to cyber-attacks.

Even though, the most common cyber-security incidents reported entail external cyber-threats against process-facilities, the insider threat is also relevant to consider. Analysis of past incidents indicated that insider threats comprised about 10% of the total cybersecurity incidents recorded. Thus, insiders are potentially a

very relevant category of attackers to pay attention to. This is because insiders usually have comprehensive knowledge of the processes and the plant. Interviews with the representatives of Seveso plants also pointed to the relevance of insider threats, such as embittered employees. Insider threats are a security issue with potential safety implications. In addition, from the management viewpoint, other functions of the organization can participate in tackling insider threats, such as personnel management via HR departments. There are different means to manage insider threats, e.g., work colleagues can look after each other, supervisors play a relevant role in preventing insider threats, as well as occupational healthcare, as insider threats can also be a question of mental health and wellbeing, as our interviewees mentioned.

Furthermore, the results of the past incident analysis showed that intentional and unintentional cybersecurity incidents displayed equally credible patterns. These results lead us to reflect upon the relevance, interface, and integration of security and safety culture, as a security culture would focus on the prevention of intentional malicious acts, and a safety culture would focus on unintentional acts based on ignorance, negligence, or demotivation. We could say that cybersecurity belongs to both the domains of safety and security cultures. Therefore, the definitions and functions of both domains need to be defined, in addition to their interfaces (e.g., Van Nunen et al. 2018).

The past incident analysis provided insights into the characteristics of cyber-attacks as well as insights into key countermeasures regarding cybersecurity threats. It was noticeable that cybersecurity incidents with infections of IT systems alone, did not have impacts on process-systems. Thus, a perpetrator gaining access to the OT system would be critical in terms of negative impacts on process safety. Regarding cases in which OT system was infected (28 incidents), no severe effects were reported. However, the infection of a SCADA system, as well as the short loss of plant control, and the malfunction of the detection system for dangerous substances were reported. Despite the non-existence of severe effects on OT, we emphasise that the relevance of potentially severe effects needs to be taken into account. It is of major importance to acknowledge that when the IT and OT systems are closely connected, there is always the potential that the OT systems could be harmed via cyber-attacks.

The main countermeasures regarding cyber-attacks consist of network segmentation, which separates the corporate network and the control and supervision network enabling their communication only through properly controlled and configured devices. Furthermore, proper configuration of firewalls and installation of antivirus software were identified as relevant countermeasures.

In addition to technical countermeasures, organizational countermeasures, such as continuous and intensified training regarding cybersecurity issues, and training of the personnel in terms of identification of security threats were mentioned in interviews with the representatives of Seveso establishments. These measures show that physical security threats as well as cybersecurity threats are taken seriously in the Seveso plants.

Moreover, regarding the countermeasures against cybersecurity and physical security attacks, systems theory and a systems engineering approach have suggested the adoption of a high-level strategy and to focus on ensuring the critical functions and services that the networks and systems provide in the context of attacks and disruptions. The aim would be to identify and control system vulnerabilities, instead of focusing on the identification of all potential threats or intentions or avoiding threats (Young and Leveson 2014). This does not mean that the intentions or threats should not be dealt with, but that the focus on system vulnerabilities would be easier to control than various threats. The goal would be to assure the overall function of the whole enterprise by controlling system vulnerabilities. This would mean that safety and security would be handled at the strategy level, rather than a lower-level question of tactics. The benefit of this approach would be that it could tackle the disruptions deriving both from known and unknown sources. In addition, the benefit of this approach would be that it generates a systemic understanding of the whole enterprise context, which is relevant to controlling safety and security risks in a coordinated fashion.

Guidelines

The motivation for the guidelines—and this study—derives from the trend towards ever-increasing digitalisation and the increasing use of new, smart technologies in high-risk industries, including Seveso plants. Digitalisation, such as the use of monitoring sensors in the industrial processes, or the use of smart technologies, such as AI tools for analysing big data, have been justified for process-safety reasons. Obtaining real-time data from processes enhances the monitoring of disturbances and managing processes better. However, digitalisation also has potential negative effects on safety because historically closed industrial and automation control systems have become increasingly connected to public networks. This means that industrial automation and control systems, and OT systems have become more susceptible to cyber security attacks and human intrusion. This intensified development regarding digitalisation and automation and their impacts on safety and security needs to be understood properly. Furthermore, societal changes and the threat of terrorism are also increasing the physical security threats. These physical security and cybersecurity risks as well as process-safety risks can converge and lead to major accidents. Therefore, security and safety risks need to be managed together.

The goal of the guidelines for the integrated management of safety and security is to steer design and implementation of integrated management in Seveso establishments. The guidance follows the high-level structure of ISO standards, and thus provides a familiar framework to Seveso establishments in terms of managements structure.

Integrated management covers the following aspects of management, such as the context of the organization, leadership, planning, support, operation, performance evaluation, and improvement. These aspects constitute a continuous development cycle: plan - do - check - act, which is relevant to management.

Integration refers to the structural, functional, and cultural integration levels (Jorgensen et al 2006). Structural integration refers to how management is arranged in the organization, or to an increased compatibility of system elements, such as the similarities of standards to the structure of the management system. Hence, structural integration can refer to small and gradual, but necessary steps towards an integrated management system.

Functional integration refers to the coordination of generic processes, such as the management cycle, i.e., plan-do-check-act, or establishing relevant management tasks, such as performance measurements, evaluating and developing integrated safety and security management.

Cultural integration means that integrated management is embedded in a culture of learning and continuous improvement. Cultural integration entails shared values, norms, beliefs and understanding regarding the needs and benefits of integration, as well as values and norms that are beneficial to actual practices of integrated management of safety and security at different levels of the organization and in different tasks.

Interviews with the representatives of Seveso plants showed that despite the development of integrated management, there is still lot to do in terms of common risk assessment, common evaluation of incidents, and the integration of cyber-security aspects into process-safety considerations. Furthermore, especially in the multi-plant context integration would be needed in order to understand the power-law distribution, i.e., the risks that other companies can create to one's own company, so that one could better attenuate the risks in the industrial area (Reniers et al. 2014). This contributes to understanding the context in which the companies operate and is relevant to the safety and security.

In the context of systemic risks, risk assessment would benefit from integrated assessment. This could happen for instance by integrating physical security risks, cybersecurity risks and process-safety risks into the same Hazop or bow tie analysis. To our understanding, risk assessments that combine all risks have not been adopted much in the Seveso plants. This type of combined risk assessment would require incorporating physical security and cybersecurity experts into the same team to take care of safety and the assessment of process-safety risks.

The tendency towards the increasing interconnectedness of IT and OT systems requires vigilance from the Seveso plants. The guidelines provide a general level structure for better design and implementation of integrated management. However, the guidelines aim not to be an exhaustive guide on the management of safety and security in an integrated and coordinated way. Thus, in each context one needs to reflect upon the suggested aspects and tailor them to be suitable for the industry and company contexts in question.

8.2 Implications for the industry and regulators

The integrated management of safety and security would require new safety and security thinking and an appropriate mindset that includes an adequate understanding of the need for integration based on knowledge regarding digitalisation and the convergence of safety and security risks, as well as motivation for integration.

The motivation for integration would require also understanding the potential benefits of integration, which refer to better means to identify, anticipate, prevent, mitigate, respond, and learn from safety and security risks in a coordinated way. In addition, the benefits include better internal coordination and the reduction of possible trade-offs, competitive advantages, as well as reduction of administration and audit costs.

New safety and security thinking requires thinking “beyond the box” or going beyond one’s own area of expertise. One challenge is that in the Seveso establishments it is common that cybersecurity risks are dealt with in the IT department. Furthermore, there are experts dedicated to process-safety issues, other experts are dedicated to industrial automation and control aspects, and some experts focus on physical security risks, or occupational safety risks. Obtaining a clear understanding of these different types of risks and the systemic nature of risks, i.e., their interconnectedness, would require close collaboration between different experts.

Collaboration could be enhanced by establishing permanent forums where different experts could co-construct a common understanding of systemic risks, and the needs and means for integration. Only this way will new safety and security thinking would be achieved. Nobody is an expert on systemic risks. The creation of this form of expertise requires multidisciplinarity and the co-construction of knowledge.

Attention needs to be paid to interfaces regarding IT and OT systems. IT experts, and cybersecurity experts should be trained to reflect upon the potential effects of cyber-attacks on process-safety, and process-safety engineers should be trained to reflect upon the potential cybersecurity interferences if there are disturbances in the process, or faults in devices.

Situational awareness regarding cybersecurity and physical security aspects is relevant. This requires inter-organizational collaboration. In addition, attention needs to be paid to building a common understanding of safety and security risks regarding business partners, or other companies located in the same industrial area. This power-law distribution (referring to the idea that a small fraction of companies can have a relevant safety or security impact on the other companies located in the same area) is necessary to understand and examine in order to tackle systemic risks, and this would require inter-organizational collaboration.

In the multi-plant context, integration could concretely involve the following aspects: common guarding, common emergency exercises, common fire brigades, common incidence reporting systems, integrated incidence analyses, integrated risk analyses, common safety and security cultures, common understanding of risks and

possible impacts that neighbouring organizations may have on your company and vice versa. Lastly, inspectors from different domains could make inspections jointly.

Regarding the importance of insider threats as a relevant physical security and cybersecurity threat category, the security clearance of those persons who are responsible for process-safety is highly important. This could be one means among others to tackle insider threats. Furthermore, the transportation of hazardous chemicals has received more attention recently, and the identification of the drivers. This is relevant from the perspective of tackling external threats. Similarly, attention should be paid to the identification of workers in outages, as workers can be hired by contractors and subcontractors. It is the multi-tier subcontracting chain that makes the identification of workers difficult.

Seveso sites are developing their practices in terms of security and cybersecurity and integrated management of safety and security. At the same time, there is still a lot to do. Seveso plants are willing to learn in terms of security, cybersecurity, and integrated management of safety and security. However, Seveso sites are not necessarily willing to share information about the cybersecurity disturbances, or cybersecurity aspects. This may partly relate to the need to limit information regarding security aspects, but also that cybersecurity disturbances or cyber-attacks can be seen as counter-productive to the image of the company and thus may be viewed as sensitive information.

Management and leadership are relevant for the improved and integrated safety and security. Visionary leadership would be needed in the integration of safety and security. Similarly, an effective management that could design integrated safety and security management systems and which would coordinate and solve problems regarding the integration would be needed.

The guidelines in this study can be seen as providing a frame of reference for assessing the robustness of integrated management. At the same the guidelines are not the final presentation of the management of safety and security in a coordinated way but should be taken as a starting point for further development.

Implications to the regulator

We will reflect on some implications of the integrated management of safety and security on regulators. As regulators are dependent on the existing laws in their oversight work, the support and mandate that the law provides to the oversight of integrated management of safety and security is critical. Currently the Seveso III Directive does not require integrated management from companies. Similarly, laws in many European countries do not support the oversight of integrated management of safety and security. The oversight of process-safety is arranged differently depending on the country.

What could regulators do, if the law would support them in the oversight of integrated management of safety and security? First, regulators could create criteria which the regulatory body could use to assess the quality of integrated management both in single companies and in the multi-plant context. This could include creating criteria for evaluating the quality of collaboration between companies in the

industrial area. This collaboration could entail common exercises regarding integrated safety and security risks, common safety and security strategies, sharing best practices and targets of development in each company, sharing a system that includes both safety and security incidents, and an integrated analysis of these incidents. The benefit of close collaboration would be a better common understanding of risks that neighbouring organizations create to one's own company, and a proper understanding of safety and security vulnerabilities of the complete industrial area.

Furthermore, process-safety regulators could make joint inspections with other regulators to single companies. Even though this practice is already in use, it could be made a prevailing practice. The benefit of the joint inspections is that they provide valuable knowledge to both the sites and the regulators. In the multi-plant context, all companies could participate in the final meeting, where regulators could go through issues that are common to all companies in the area.

Regulators could also demand that public safety reports required by Seveso directives should not include information that would compromise the security aspects. An abridged version of the safety reports, not containing major accident scenarios, should be mandatory.

Similarly, as Seveso establishments, also regulators would need a shared understanding of the needs for and benefits of integrated management of safety and security, but also support from law. The latter aspect broadens the integrated management of safety and security to an issue that would require support from industry, political decision-makers, and the public.

The relevant, broad discussion topic would be the following: which actors in the society are and which actors should be responsible for the emergent risks and their effects on society? Whose responsibility is to protect humans and environment and future generations from the effects of systemic risks?

8.3 Conclusions

The results of this study provided support for the relevance of paying attention to physical security and cybersecurity threats in Seveso establishments, (as well as the convergence of different security, cybersecurity, and process-safety risks). Terrorism was the main security threat category for all industries, and outsider cyberattacks were the second most important threat category. Even though, past incident analysis showed that no major events occurred in chemical or petrochemical facilities due to cyber-attacks, they remain a relevant threat category, and worth paying attention to. This is because of the current trend towards growing digitalisation, automation and blurring boundaries between IT and operational technology (OT) systems in high-risk industries (e.g., Boyes et al. 2018), which means that cybersecurity incidences have the potential to create negative impacts in OT and industrial automation and control systems (IACS), and thus could lead to major accidents. Therefore, raising the awareness of cybersecurity and the

convergence of cybersecurity risks, physical security risks and process-safety risks, and the potential for major accidents in Seveso establishments is relevant.

Cybersecurity awareness in Seveso plants was reported to be at a good level. Companies have increased training and exercises regarding cybersecurity over the last years. However, a warning example was a case in which a cybersecurity exercise resulted in all stakeholders opening a “contaminated” message. Furthermore, survey respondents mentioned that they had seen ignorance and negligence in their companies regarding cybersecurity. Thus, both continuous training, and raising the motivation to act securely are needed, because awareness of cybersecurity requires both.

It is possible to create technological barriers, e.g., to design IT systems so that they guide people to act securely without the need for people to make their own choices. Furthermore, technological barriers, such as firewalls, anti-virus software, but also the design of IT and OT systems are relevant in terms of protecting these systems. In addition to technological barriers, human and organizational barriers are needed, and these refer to an integrated management and safety and security culture. It is good to remember that decisions, investments, and updates regarding technological barriers are dependent on organizational factors, such as management and leadership.

Institutional support to integrated management is weak. The Seveso directive does not require integration. The Responsible Care programme and Environment, Health and Safety and Security (EHS&S) management system adopted by many Seveso plants, do combine different standards into the same management system and thus represent structural integration. However, they are not sufficient to tackle systemic risks, deriving from interconnectedness of technological and organisational systems and related risks.

Regarding the current state of integrated management of safety and security in Seveso plants, there are several promising developments ongoing. However, there is also space for improvements, e.g., integrated management would benefit from risk assessments, in which process-safety risks, physical security risks and cybersecurity risks and their significance would be examined together e.g. in the same hazop study. The integrated management of safety and security is the best means to better identify, manage and mitigate systemic risks.

Integrated management requires a deep understanding of systemic risks, and new safety and security thinking, and collaboration between different safety and security experts. Only this way will better insights into the emerging risks and motivation for integration be obtained. Furthermore, tensions between safety and security management e.g. in term of openness and transparency, needs to be understood and dealt with. In the security domain concealment of data is typical and necessary, instead in the safety domain openness and transparency are relevant for the improvement of safety.

The separate Guidelines report, see https://projects.safera.eu/projects provides guidance on what to consider when designing and implementing integrated safety and security management in Seveso plants. The potential activities, in which safety and security management could be combined include e.g., risk assessment,

incident reporting and analysis, emergency management, change management, and informing the public.

In the future it would be worth studying the robustness of companies in terms of integrated management of safety and security; as well as different forms and manifestations of integration on Seveso sites (both in single plant and multi-plant contexts); in addition to interfaces between safety and security cultures, and limitations regarding their integration; as well as the way current integrated management approaches such as EHS&S enhance or constrain the integrated management of safety and security.

Acknowledgements

We thank for SAF€RA consortium, and Finnish Work Environment Fund (FWEF), Finnish Safety and Chemicals Agency (TUKES) and the Italian National Institute for Insurance against Accidents at Work (INAIL) for funding this project. We thank for representatives of all organizations and Seveso plants who participated in this project.

References

Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50, 179–211.

Aldawood, H., Skinner, G. (2019) Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review. Proceedings of 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering, TALE 2018, art. no. 8615162, pp. 62-68.

Amundrud, O., Aven, T. and Flage, R. 2017. How the definition of security risk can be made compatible with the safety definitions? Journal of Risk and Reliability, 231, 3, 286-294.

Appelbaum J, Potras L. The NSA and Its Willing Helpers. Edward Snowden Interview.2013. https://scholar.google.com/scholar?q=Appelbaum%20J,%20Potras%20L.%20The%20NSA%20and%20Its%20Willing%20Helpers.%20Edward%20Snowden%20Interview.%202013.

Argenti F., Salzano E., Cozzani V. (2019) A comparative analysis of security risk assessment methodologies for the chemical industry. Reliability Engineering and System Safety 2019;191. https://doi.org/10.1016/j.ress.2018.03.001.

Askeland, T., Flage, R. and Aven, T. 2017. Moving beyond the probabilities - Strength of knowledge characterisations applied to security. Reliability Engineering and System Safety, 159, 196-205.

van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. International Journal of Human-Computer Studies, 123, 29-39.

Baybutt, P. (2017). Security vulnerability analysis: protecting process plants from physical and cyber threats. In Security Risk Assessment: In the Chemical and Process Industry, ed. Reniers, G. et al., De Gruyter, Inc., 2017. ProQuest Ebook

Becker, M., H. (1974). The health belief model and personal health behavior. Health Education Monographs, 2, 324–473.

Becker, M., H., & Rosenstock, I. M. (1987). Comparing social learning theory and the health belief model. In W. B. Ward (Ed.), Advances in health education and promotion (Vol. 2, pp. 245-249). Greenwich, CT: JAI.

Bieder, C. and Pettersen Gould, K. (2020). The Coupling of Safety and Security. Exploring interrelations in Theory and Practice. Springer Open. 484809_1_En_Print.indd (oapen.org)

Blythe, John (2015) Information security in the workplace: A mixed-methods approach to understanding and improving security behaviours. Doctoral thesis, Northumbria University.

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

Boudriga, N. (2010) Security of mobile communications. Boca Raton: CRC Press. 2010.

Boyes, H., Hallaq, B., Cunningham, J. and Watson, T.(2018). The Industrial Internet of things (IIoT): An analysis framework. Computers in Industry, 101, 1-12.

Brooks, D.J. What is Security: Definition through knowledge categorization. 2010 Security Journal, 23, 3, 225-239.

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

CCPS (2003). Center for Chemical Process Safety (CCPS). Guidelines for investigating chemical process incidents 2003..

Chowdhury, N. H., Adam, M.T.P. and Skinner G. (2019) The impact of time pressure on cybersecurity behaviour: a systematic literature review. Behaviour and Information Technology, 38, (12), 1290-1308.

Cozzani, V. (2017). Safety and security of Seveso sites: Stepping towards research synergies and an integrated framework. Journal of Integrated Security Science 2017 (1) 32-34.

Davis, F. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly, 13(3), 319-340. doi:10.2307/249008

Dekker, S., Cilliers, P. and Hofmeyr, J.H. (2011) The complexity of failure: implications of complexity theory for safety investigations. Safety Science, 49 (6), 939-945.

Ethical Hacking - Phases of Hacking, Comput Sci (2019). http://cybersecurity.jhigh.co.uk/ethicalHacking/attackPhases.html (accessed July 18, 2019)

Falliere, N. O., Murchu, L., Chien, E. (2011).W32.Stuxnet Dossier 2011.

Fogg, B., J. (2009). A behavior model for persuasive design. In Proceedings of the 4th International Conference on Persuasive Technology (Persuasive '09). Association for Computing Machinery, New York, NY, USA, Article 40, 1–7.

Fischer, R.J and Green, G. (2004). Introduction to Security. Boston, MA: Butterworth-Heinemann.

Franke, U., Brynielsson, J. (2014). Cyber situational awareness - A systematic review of the literature. Computers and Security, 46, pp. 18-31.

Garcia, M. L. (2007). The Design and Evolution of Physical Protection Systems. 2nd ed. Butterworth-Heinemann; 2007.

Gibbs, J. (1975). Crime, Punishment, and Deterrence. Elsevier, New York, NY.

Greenacre M. (2016) Correspondence Analysis in Practice. 3rd ed. Chapman and Hall/CRC; 2016.

Hanus, B., & Wu, Y. A. (2016). Impact of users' security awareness on desktop security behavior: a protection motivation theory perspective. Information Systems Management, 33(1), 2-16.

Henrie M. (2013) Cyber Security Risk anagement in the SCADA Critical Infrastructure Environment. Eng Manag J 2013;25:38–45. https://doi.org/https://doi.org/10.1080/10429247.2013.11431973.

Hollnagel, E., Pariès, J., Woods, D.D. and Wreathall, J. (2011) Resilience Engineering in Practice. A guidebook. Ashgate, Surrey.

Hollnagel, E. (2012) A Tale of Two Safeties. https://www.entrypointnorth.com/wp-content/uploads/sites/3/A-tale-of-two-safeties-V8.pdf

IAEA, 2008. Nuclear Security Culture. IAEA Nuclear Security series No. 7. Implementing Guide. International Atomic Energy Agency, Vienna.

IAEA. 2017. Self-assessment of nuclear security culture in Facilities and Activities. IAEA Nuclear Security series No 28-T. Technical guidance.

Iaiani, M., Tugnoli, A., Casson Moreno, V., Cozzani, V. (2020) Analysis of past cybersecurity-related incidents in the process industry and the like. Chem Eng Trans 2020; 83:163–8.

INSAG-4. 1991. Safety Culture. A report by the International Nuclear Safety Advisory Group. Safety Series, No 75, INSAG-4. International Atomic Energy Agency. Vienna.

Ishikawa K. Guide to Quality Control. 2nd ed. Tokyo: Asian Productivity Organization; 1982.

Jorgensen T.H., Remmen A. and Mellado M.D. (2006) Integrated management systems - three different levels of integration. Journal of Cleaner Production, 14 (8), 713-722.

Jore, S.H. (2019) The Conceptual and Scientific Demarcation of Security in Contrast to Safety. Eur J Secur Res (2019) 4:157–174.

Khakzad, N., Su Martinez, I.; Kwon; H.M., Stewart, C., Perera, R. and Reniers, G. (2018): Security Risk Assessment and Management in Chemical Plants: Challenges and New Trends: Process Safety Progress Vol.37, No.2

Karanikas, N. (2018) Revisiting the relationship between safety and security. Int. J. of Safety and Security Eng., Vol. 8, No. 4 (2018) 547–551.

Kriaa, S., Pietre-Cambacedes, L., Bouissou, M., Halgand, Y., (2015) A survey of approaches combining safety and security for industrial control systems. Reliability Engineering and System Safety139(2015)156–178.

Krippendorff, K. H. (2013). Content analysis: An introduction to its methodology (3rd ed.). California; CA: Sage Publications

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & H. Breitner, M. (2014). Information security awareness and behavior: a theory-based literature review. Management Research Review, 37(12), 1049-1092.

Mannan, M.S., Sachdeva,s., Chen, H., Reyes-Valdes, O., Liu, Y. & Laboureur, D.M. 2015. Trends and Challenges in Process Safety. AIChE Journal November 2015 Vol. 61, No. 11, 3558-2569.

Martens, M., De Wolf, R., & De Marez, L. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. Computers in Human Behavior, 92, 139-150.

Michie, S., van Stralen, M. M., & West, R. (2011). The behaviour change wheel: A new method for characterising and designing behaviour change interventions. Implement Science, 6, 42.

Casson Moreno, V., Reniers, G., Salzanoa, E. & Cozzani, V. (2018). Analysis of physical and cyber security-related events in the chemical and process industry Process Safety and Environmental Protection 116 (2018) 621–631.

van Nunen, K., Sas, M., Reniers, G., Vierendeels, G., Ponnet, K., Hardyns, W. (2018) An integrative conceptual framework for physical security culture in organizations. Journal of integrated security science 2 (1), 25-32.

OPCW (2016). Needs and Best Practices on Chemical Safety and Security Management. Available at: https://www.opcw.org/sites/default/files/documents/ICA/ICB/OPCW_Report_on_Needs_and_Best_Practices_on_Chemical_Safety_and_Security_ManagementV3-2_1.2.pdf

Paltrinieri, N., Tugnoli, A., Buston, J., Wardman, M., Cozzani, V (2013). Dynamic Procedure for Atypical Scenarios Identification (DyPASI): A new systematic HAZID tool. J Loss Prev Process Ind 2013; 26:683–95. https://doi.org/https://doi.org/10.1016/j.jlp.2013.01.006.

Piètre-Cambacédès, L. & Bouissou, M. 2013.Cross-fertilization between safety and security engineering. Reliability Engineering and System Safety 110 (2013) 110–126.

Piquero, N., & Tibbetts, S. (1996). Specifying the Direct and Indirect Effects of Low Self-Control and Situational Factors in Offenders Decision Making: Toward a More Comparative Model of Rational Offending, Justice Quarterly, 13(3), pp. 481-510.

Rahim, N. H. A., Hamid, S., Mat Kiah, M. L., Shamshirband, S., & Furnell, S. (2015). A systematic review of approaches to assessing cybersecurity awareness. Kybernetes, 44(4), 606-622.

Rathnayaka, S., Khan, F., Amyotte, P. (2011). SHIPP methodology: Predictive accident modeling approach. Part I: Methodology and model description. Process Saf Environ Prot 2011;89:151–64. https://doi.org/10.1016/j.psep.2011.01.002.

Reiman, T. and Rollenhagen, C. (2018) Safety culture. In: Möller, N., Hansson, S.O., Holmberg, J-E. and Rollenhagen, C. (eds.) Handbook of Safety Principles. John Wiley & Sons, pp. 647- 676.

Reniers, G. and Khakzad, N. 2017. Revolutionizing Safety and Security in the Chemical and Process Industry: Applying the CHESS concept. Journal of integrated Security Science 2017.

Reniers, G.L.L, Sörensen, K, Khan, F. and Amyotte, P. 2014. Resilience of chemical industrial areas through attenuation-based security. Reliability Engineering and System Safety 131, 94-101.

Reniers, G. and Amyotte, P. (2012): Prevention in the chemical and process industries: Future directions. Journal of Loss Prevention in the Process Industries 25, 227-231.

Rouse, M. (2010). Definition: privilege escalation attack. SearchSecurity n.d. https://searchsecurity.techtarget.com/definition/privilege-escalation-attack.

Smith C. and Brooks, D.J. (2012) Security Science: The theory and practice of security. Butterworth-Heinemann.

von Solms, R. and van Niekerk, J. (2013). From information security to cybersecurity. Computers and Security, 38, 97-102.

SRA 2018 Glossary Society for Risk Analysis, www.sra.org/resources.

Stacey, R. (2012). Tools and Techniques of Leadership and Management. Meeting the challenge of complexity. Routledge, London and New York.

Steijn, W., J. van der Vorm, E. Luiijf, R. Gallis, and F. van der Beek, D. (2016). Opkomende risico's voor arbeidsveiligheid als gevolg van IT-koppelingen van en tussen arbeidsmiddelen (Emerging occupational safety risks associated with IT links from and between work equipment). TNO report, TNO 2016 R10096

Stouffer, K., Falco, J., Scarfone, K. (2008) Guide to Industrial Control Systems (ICS) Security.

Torten, R., Reaiche, C., & Boyle, S. (2018). The impact of security awarness on information technology professionals' behavior. Computers & Security, 79, 68-79.

Woods, D. D. 2006. Essential Characteristics of Resilience. In Hollnagel, E., Woods, D.D, and Leveson, N.G. (eds.) Resilience Engineering: Concept ad precepts. Aldershot: UK: Ashgate.

Young, W and Leveson, N.G. (2014). Insider risks: An integrated approach to safety and security based on systems theory. Communications of the ACM, vol. 57, 2, 31-35.

Appendix A: Themes of the expert interviews

Each theme includes examples of questions. In each interview the themes were dealt with. However, the expert area of an interviewee had impacts on answers. Some themes were emphasized, whilst other themes got minor attention, depending on the expert area of the interviewee.

I BACKGROUND

- (Interviewee's education, experience, how long interviewee has worked in the organization)
- Field of industry
- Please describe your work (position, tasks, roles, responsibilities)
- What is the size of your organization (in terms of employees, budget etc.)
- How is your work related to safety/security/cybersecurity? (Please, specify, also interconnections between safety/security/cybersecurity in your work)

II SAFETY & SECURITY ASPECTS

- How does your organization keep itself aware of the actual safety/security/cyber security situation?
- What kind of external (governmental) organizations, consultants, etc. do you collaborate with in order to get proper understanding of the security situation?
- What kind of practices, forums, or methods do you use for maintaining security situation awareness?
- What are the specific safety risks/threats that are acute in this field of industry? /in your own organization?/ (e.g., process safety related questions)
- How are these safety threats taken into account in your organization?
- How have you anticipated and prepared for the safety threats? Please, provide some examples.
- How are (cyber)security induced threats to (process) safety managed by your organization?
- How does your organization keep itself aware of the actual safety/security/cyber security situation?

III SECURITY & CYBER SECURITY RISKS

- How do you define security? (e.g., intentional or unintentional act, or both?).
- How is security (physical security or cyber security) taken into account in risk assessment? (methods?)
- What are typical security risks in your company?/ or in the industry to which your company belongs?
- What are the main concerns related to security risks in your company?
- Is cyber security regarded as a relevant threat in your company?
- What do you understand the term OT-security to include?

- What do you think is the main cyber threat to OT security?
- What kinds of cyber security threats or vulnerabilities you have identified? Below the list:
- Information security
- Spying (e.g. attacks through the IT service provider, e.g. IT service provider is contaminated so that via IT service provider it is possible to get access to clients information, e.g. spying by own employees)
- Outsourcing of services and concentration of services (definition of responsibilities in contracts is essential)
- Security breach - and information leakages
- Malware (e.g. malware is identified as relevant cyber security observations in Finland, in general)
- Confidence trick, Fishing
- Internet of Things and automation (e.g. devices connected to internet, or open internet) Organization's capacity to manage the internet (net's situation)
- How have you prepared for cyber security threats? Below the list:
- Information security related responsibilities have been included in contracts
- Updating of equipment ("Equipment hygiene"; e.g. software patches)
  - Education, training and testing (own employees, contractor personel)
  - Familiarity with the systems and services (from external service providers)
  - Information security is a relevant part of the organization's everyday practices
- What would better preparedness require from employees/organizations?
  - Opennes? etc…
- Do the members of your organizations have the courage to inform the IT department if they (unintentionally) breached the systems security (e.g. have opened a suspicious link)? Does your IT department monitor employees security behavior (e.g. logging systems, downloading files, etc.)?
- How would you estimate the significance of cyber security threats compared to other physical security threats?
- Are there any IT interfaces between physical security measures and cybersecurity (e.g. use of passes to entrance gates)? How are these interfaces protected?
- Do you think a major cyber-attack with catastrophic effects will take place?

IV INCIDENTS AND NEAR MISSES

- What kinds of safety/security/cybersecurity incidents or near misses have you had? Could you provide examples?
- How would you estimate the companies' willingness to report safety/security related incidents?
- How do you identify security threats? What kinds of procedures/methods do you use? (risk matrices, scenarios, predictions)?

- Does your company exchange information about the security threats or near misses with other companies? If not, why?
- Does your company exchange information about the security threats or near misses with governmental institutions? Is this voluntary or obliged by regulation? If not, why?
- Who investigates security incidents? Who should investigate them?
- How are security threats investigated (e.g. in combined teams, including process control engineers, IT specialists, safety specalists)?
- Do you get information of incidents or near misses from your company/from other companies or governmental institutions?
- How do you learn from security incidents of near misses?
- Is there a formalized learning process within your company (e.g. acquiring incident information by registration and report, actual investigation itself including fact finding and analysis, planning interventions, performing and monitoring actions and evaluation of the effectiveness of actions and the learning process itself).
- Does your company learn from incidents only (reactive) or do you learn from experience as well (proactive) based on success stories, near misses, best practices and early warnings/ weak signals?

V INTEGRATION OF SAFETY AND SECURITY MANAGEMENT

- How are security, cyber security and safety aspects managed in your company? (separate department? specific experts?)
- Are safety and security management integrated in your company? How is this done?
- What are the biggest obstacles as regards the integration of safety and security management (e.g. different expertise, lack of resources)?
- What are the drivers to integrate safety and security?
- What are the reasons to keep management of safety and security separated?
- Could you identify some features in safety management, which would not be possible/desirable in management of security and vise versa?
- How to improve the management of safety and security?
- Could you please describe the national level or regional level activities regarding management of safety and security in integrated way?

VI REGULATION, REGULATORY BODY'S SUPERVISION,

- How does the regulatory body supervise safety and security management?
- Are security threats discussed with the regulatory body during their inspection visits?
- What are your expectations concerning regulatory body's supervision of security?

VI LEARNING FROM OTHER COUNTRIES

- What are your observations concerning safety and security management in the process industry in your country?/in small facilities vs. big facilities?/ in different industries?/ Abroad?
- What is learnt from other countries regarding integrated management of safety and security?
- How is safety and security managed in industrial parks? Collaboration?
- What kinds of pros and cons are related to industrial park regarding management of safety and security?
- What are the needs and the gaps within the current and future cybersecurity landscape in Europe?
- In order to address the identified needs or gaps in future, what should be the top priorities for cybersecurity?

Thank you for the interview!

Appendix B: Survey on attitudes and awareness of cyber-physical security threats

Index

Report Summary	3
For which department do you work within your organisation?	4
What is your role in your department?	5
Please indicate below with what kind of technology (IT or OT) you come into contact with most during your daily activities. Please answer the subsequent questions with your answer here in mind.	6
How often do you see the employees in your organisation behave as follows?	7
How likely do you think it is that the following consequences occur in your organisation as a result of a cyber security breach?	9
Have any of the following consequences occurred as a result of a cyber security breach within your organisation?	11
What are the likely consequences that the following types of misuse can have? (multiple answers possible)	13
What are the likely cyber security breaches that the following types of misuse may cause or enable? (multiple answers possible)	15
What are the likely consequences that the following security breaches can have? (multiple answers possible)	17
Do you feel confident with the level of cyber security of your company?	19
Who in your organisation is responsible for the cyber security? (multiple answers possible)	20
Do you feel the cyber security policy of your organisation has an impact on your daily activities?	21
Do you think employees in your organisation are aware of the potential impacts of cyber security risks?	22
What activities or tools do you employ to integrate (occupational and process) safety and cybersecurity management in your organization?	23
How often do safety and security managers have meetings together?	24
To what extent do you believe that management of (occupational and process) safety and cyber security are interdependent?	25
Please elaborate your answer.	26
Does your organisation implement cyber security interventions aimed at how employees work with systems? Can you indicate which interventions are used within your organisation? (multiple answers possible)	27
Does your organisation implement cyber security interventions focused on organisational policy? Can you indicate which interventions are used within your organisation? (multiple answers possible)	29
Does your organisation implement cyber security interventions aimed at IT-systems? Can you indicate which interventions are used within your organisation? (multiple answers possible)	31
How many people does your organisation employ?	33
How long ago was your organisation established?	34

Which sector does your organisation operate in? 35
Which level of obligations does the site have under the Seveso regulation? 36
How would you describe the structure of your organization? 37

Report Summary

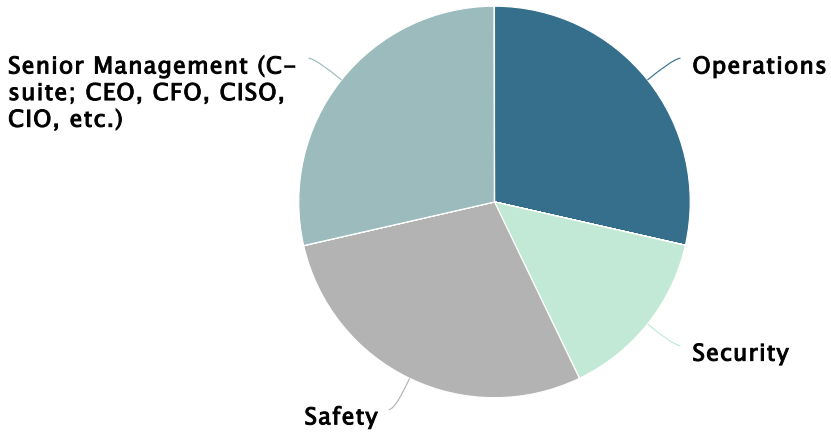
Safera SecSafMan (def)
Survey period: from 25 Feb 2020

Response Statistics

	Unfiltered		Filtered	
Group	**Count**	**in %**	**Count**	**in %**
Completed	11	22	7	100
In progress	39	78	0	0
Not responded	0	0	0	0

For which department do you work within your organisation?

7 Answers



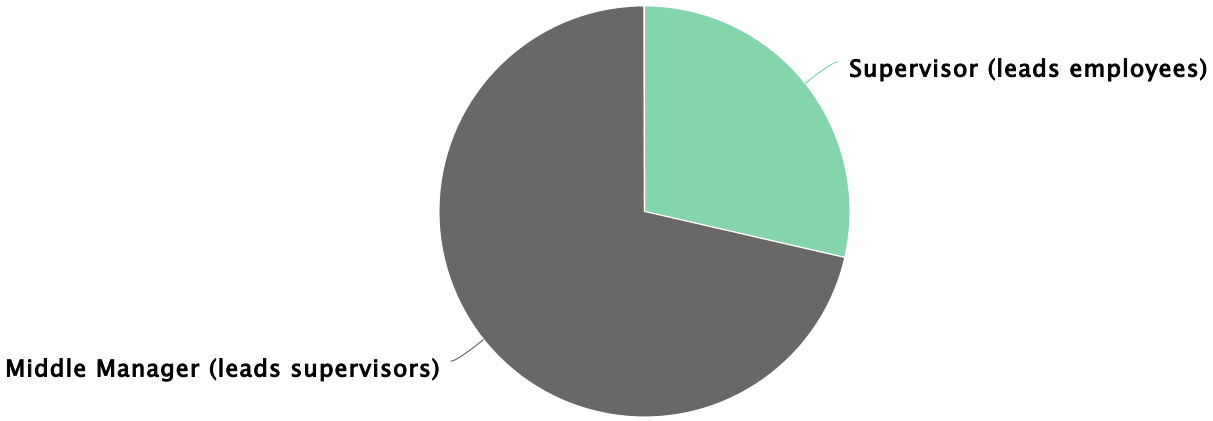
Value	All cases
Total	⌀ 7.1 (n=7)
Operations	29% (2)
Maintenance	0
Marketing & Communication	0
Legal	0
Risk & Compliance	0
Engineering	0
IT	0
Security	14% (1)
Safety	29% (2)
Proces control	0
Senior Management (C-suite; CEO, CFO, CISO, CIO, etc.)	29% (2)
Other (please elaborate)	0

Other (please elaborate)

All cases

What is your role in your department?

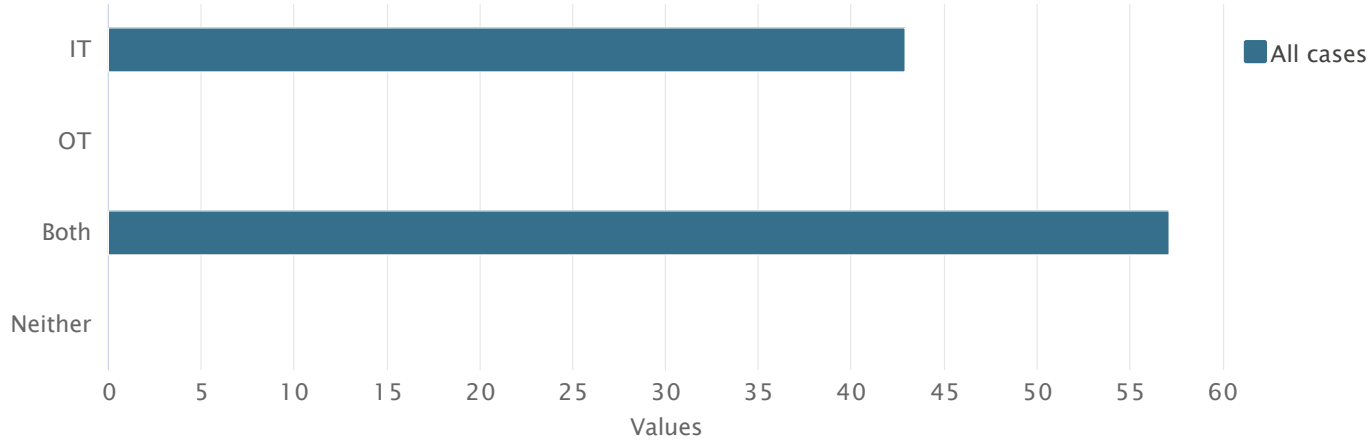
7 Answers



Value	All cases
Total	⌀ 2.7 (n=7)
Employee	0
Supervisor (leads employees)	29% (2)
Middle Manager (leads supervisors)	71% (5)
Senior Manager (leads company)	0

Please indicate below with what kind of technology (IT or OT) you come into contact with most during your daily activities. Please answer the subsequent questions with your answer here in mind.

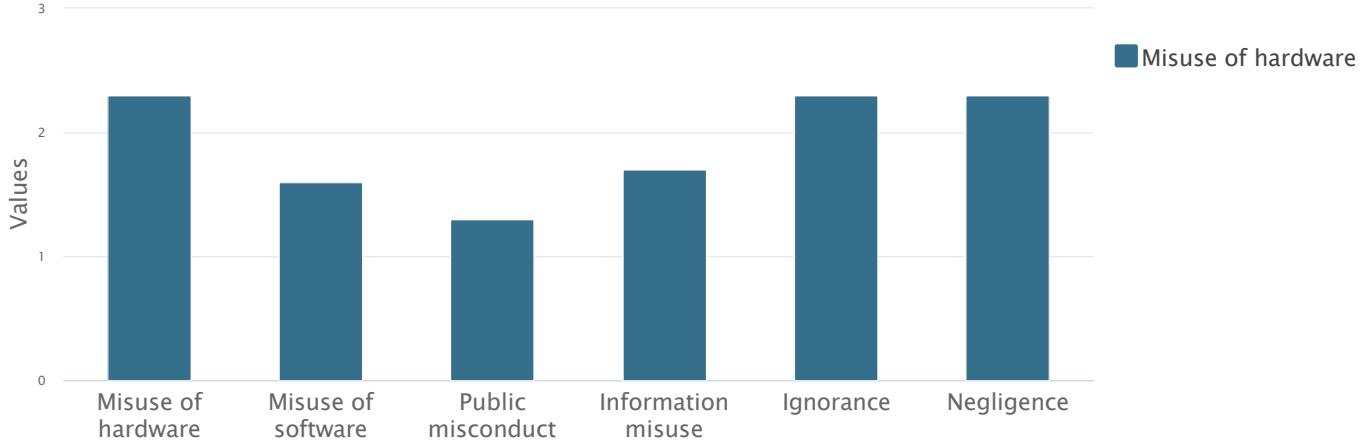
7 Answers



Value	All cases
Total	⌀ 2.1 (n=7)
IT	43% (3)
OT	0
Both	57% (4)
Neither	0

How often do you see the employees in your organisation behave as follows?

7 Answers

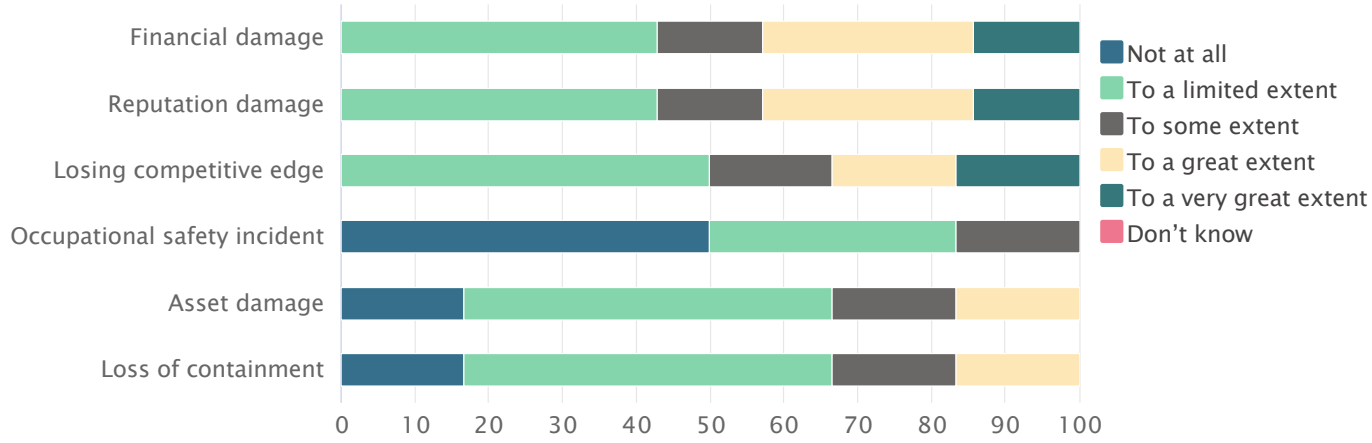


Value	All cases
Misuse of hardware	⌀ 2.3 (n=7)
Never	29% (2)
Sometimes	57% (4)
Regularly	0
Often	0
Always	0
Do not know	14% (1)
Misuse of software	⌀ 1.6 (n=7)
Never	43% (3)
Sometimes	57% (4)
Regularly	0
Often	0
Always	0
Do not know	0
Public misconduct	⌀ 1.3 (n=6)
Never	67% (4)
Sometimes	33% (2)

Regularly	0
Often	0
Always	0
Do not know	0
Information misuse	⌀ 1.7 (n=6)
Never	67% (4)
Sometimes	17% (1)
Regularly	0
Often	17% (1)
Always	0
Do not know	0
Ignorance	⌀ 2.3 (n=6)
Never	17% (1)
Sometimes	67% (4)
Regularly	0
Often	0
Always	17% (1)
Do not know	0
Negligence	⌀ 2.3 (n=6)
Never	17% (1)
Sometimes	67% (4)
Regularly	0
Often	0
Always	17% (1)
Do not know	0

How likely do you think it is that the following consequences occur in your organisation as a result of a cyber security breach?

7 Answers

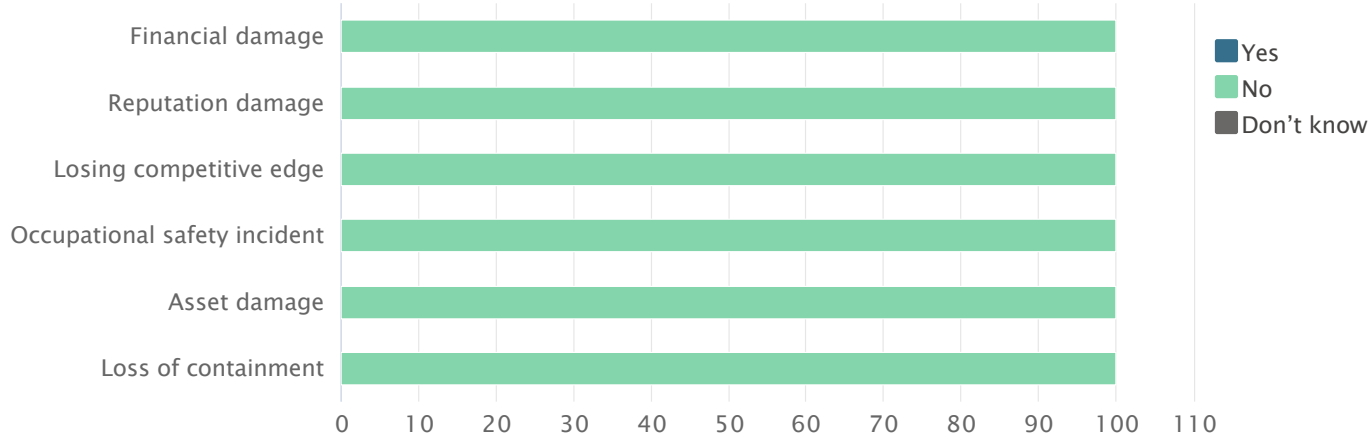


Value	All cases
Financial damage	⌀ 3.1 (n=7)
Not at all	0
To a limited extent	43% (3)
To some extent	14% (1)
To a great extent	29% (2)
To a very great extent	14% (1)
Don't know	0
Reputation damage	⌀ 3.1 (n=7)
Not at all	0
To a limited extent	43% (3)
To some extent	14% (1)
To a great extent	29% (2)
To a very great extent	14% (1)
Don't know	0
Losing competitive edge	⌀ 3 (n=6)
Not at all	0
To a limited extent	50% (3)

To some extent	17% (1)
To a great extent	17% (1)
To a very great extent	17% (1)
Don’t know	0
Occupational safety incident	⌀ 1.7 (n=6)
Not at all	50% (3)
To a limited extent	33% (2)
To some extent	17% (1)
To a great extent	0
To a very great extent	0
Don’t know	0
Asset damage	⌀ 2.3 (n=6)
Not at all	17% (1)
To a limited extent	50% (3)
To some extent	17% (1)
To a great extent	17% (1)
To a very great extent	0
Don’t know	0
Loss of containment	⌀ 2.3 (n=6)
Not at all	17% (1)
To a limited extent	50% (3)
To some extent	17% (1)
To a great extent	17% (1)
To a very great extent	0
Don’t know	0

Have any of the following consequences occurred as a result of a cyber security breach within your organisation?

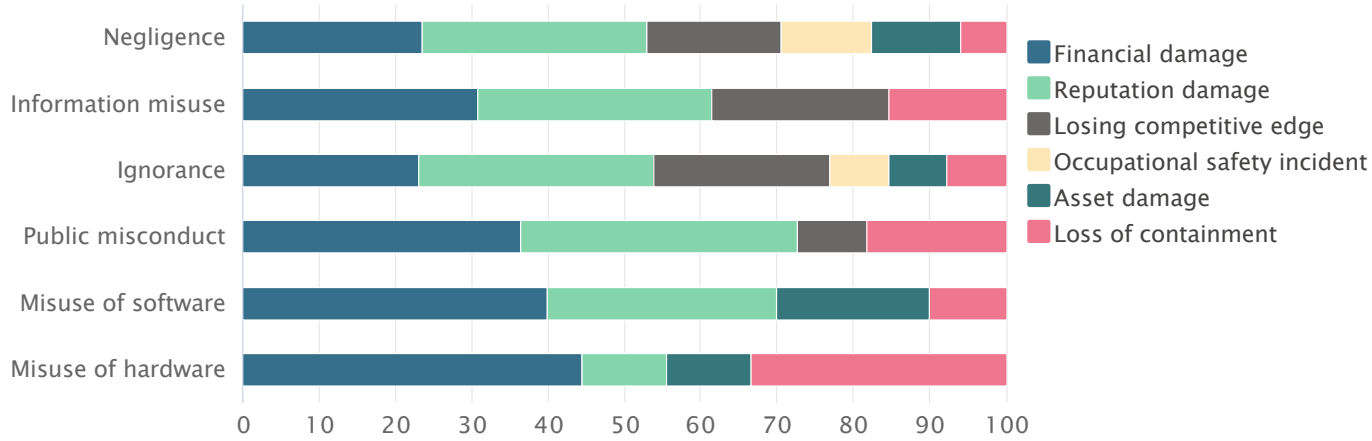
6 Answers



Value	All cases
Financial damage	⌀ 2 (n=6)
Yes	0
No	100% (6)
Don’t know	0
Reputation damage	⌀ 2 (n=6)
Yes	0
No	100% (6)
Don’t know	0
Losing competitive edge	⌀ 2 (n=6)
Yes	0
No	100% (6)
Don’t know	0
Occupational safety incident	⌀ 2 (n=6)
Yes	0
No	100% (6)
Don’t know	0
Asset damage	⌀ 2 (n=6)
Yes	0
No	100% (6)
Don’t know	0
Loss of containment	⌀ 2 (n=6)
Yes	0
No	100% (6)
Don’t know	0

What are the likely consequences that the following types of misuse can have? (multiple answers possible)

7 Answers

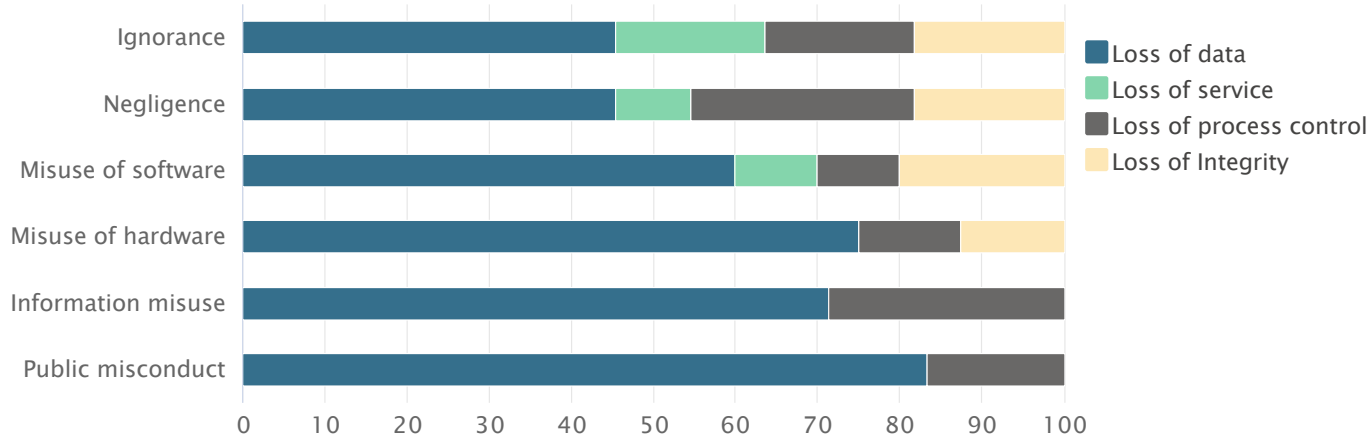


Value	All cases
Negligence	⌀ 2.4 (n=7)
Financial damage	57% (4)
Reputation damage	71% (5)
Losing competitive edge	43% (3)
Occupational safety incident	29% (2)
Asset damage	29% (2)
Loss of containment	14% (1)
Information misuse	⌀ 1.9 (n=7)
Financial damage	57% (4)
Reputation damage	57% (4)
Losing competitive edge	43% (3)
Occupational safety incident	0
Asset damage	0
Loss of containment	29% (2)
Ignorance	⌀ 1.9 (n=7)
Financial damage	43% (3)
Reputation damage	57% (4)

Losing competitive edge	43% (3)
Occupational safety incident	14% (1)
Asset damage	14% (1)
Loss of containment	14% (1)
Public misconduct	⌀ 1.6 (n=7)
Financial damage	57% (4)
Reputation damage	57% (4)
Losing competitive edge	14% (1)
Occupational safety incident	0
Asset damage	0
Loss of containment	29% (2)
Misuse of software	⌀ 1.4 (n=7)
Financial damage	57% (4)
Reputation damage	43% (3)
Losing competitive edge	0
Occupational safety incident	0
Asset damage	29% (2)
Loss of containment	14% (1)
Misuse of hardware	⌀ 1.3 (n=7)
Financial damage	57% (4)
Reputation damage	14% (1)
Losing competitive edge	0
Occupational safety incident	0
Asset damage	14% (1)
Loss of containment	43% (3)

What are the likely cyber security breaches that the following types of misuse may cause or enable? (multiple answers possible)

7 Answers

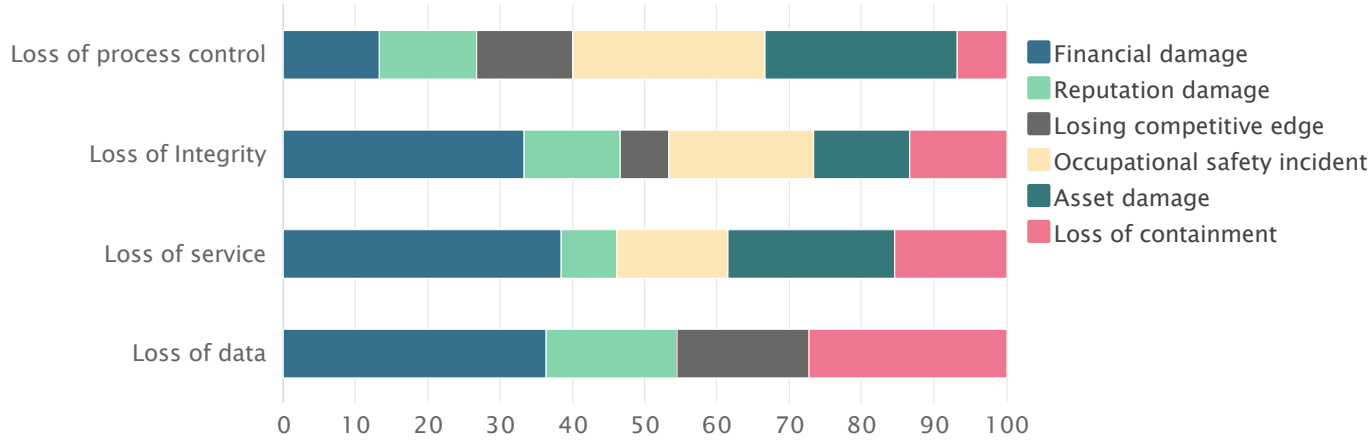


Value	All cases
Ignorance	⌀ 1.6 (n=7)
Loss of data	71% (5)
Loss of service	29% (2)
Loss of process control	29% (2)
Loss of Integrity	29% (2)
Negligence	⌀ 1.6 (n=7)
Loss of data	71% (5)
Loss of service	14% (1)
Loss of process control	43% (3)
Loss of Integrity	29% (2)
Misuse of software	⌀ 1.4 (n=7)
Loss of data	86% (6)
Loss of service	14% (1)
Loss of process control	14% (1)
Loss of Integrity	29% (2)
Misuse of hardware	⌀ 1.1 (n=7)
Loss of data	86% (6)

Loss of service	0
Loss of process control	14% (1)
Loss of Integrity	14% (1)
Information misuse	⌀ 1 (n=7)
Loss of data	71% (5)
Loss of service	0
Loss of process control	29% (2)
Loss of Integrity	0
Public misconduct	⌀ 0.9 (n=7)
Loss of data	71% (5)
Loss of service	0
Loss of process control	14% (1)
Loss of Integrity	0

What are the likely consequences that the following security breaches can have? (multiple answers possible)

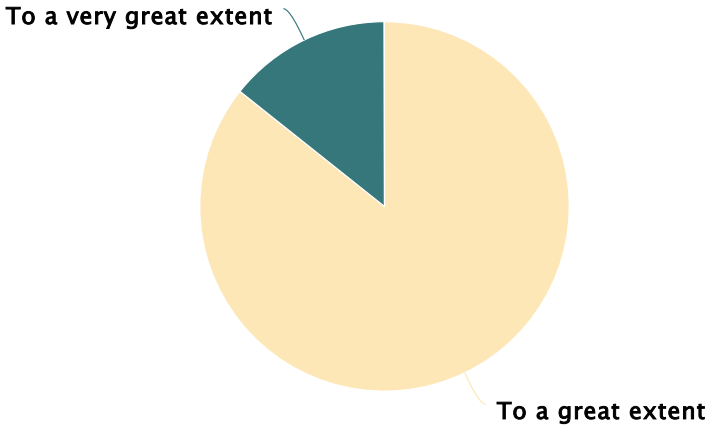
7 Answers



Value	All cases
Loss of process control	⌀ 2.1 (n=7)
Financial damage	29% (2)
Reputation damage	29% (2)
Losing competitive edge	29% (2)
Occupational safety incident	57% (4)
Asset damage	57% (4)
Loss of containment	14% (1)
Loss of Integrity	⌀ 2.1 (n=7)
Financial damage	71% (5)
Reputation damage	29% (2)
Losing competitive edge	14% (1)
Occupational safety incident	43% (3)
Asset damage	29% (2)
Loss of containment	29% (2)
Loss of service	⌀ 1.9 (n=7)
Financial damage	71% (5)
Reputation damage	14% (1)
Losing competitive edge	0
Occupational safety incident	29% (2)
Asset damage	43% (3)
Loss of containment	29% (2)
Loss of data	⌀ 1.6 (n=7)
Financial damage	57% (4)
Reputation damage	29% (2)
Losing competitive edge	29% (2)
Occupational safety incident	0
Asset damage	0
Loss of containment	43% (3)

Do you feel confident with the level of cyber security of your company?

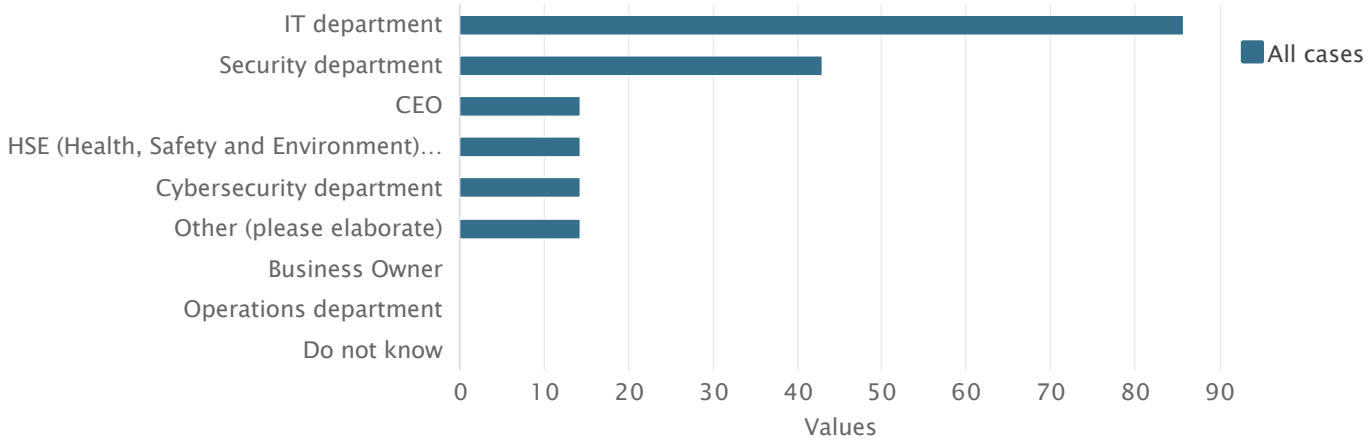
7 Answers



Value	All cases
Total	⌀ 4.1 (n=7)
Not at all	0
To a limited extent	0
To some extent	0
To a great extent	86% (6)
To a very great extent	14% (1)
Do not know	0

Who in your organisation is responsible for the cyber security? (multiple answers possible)

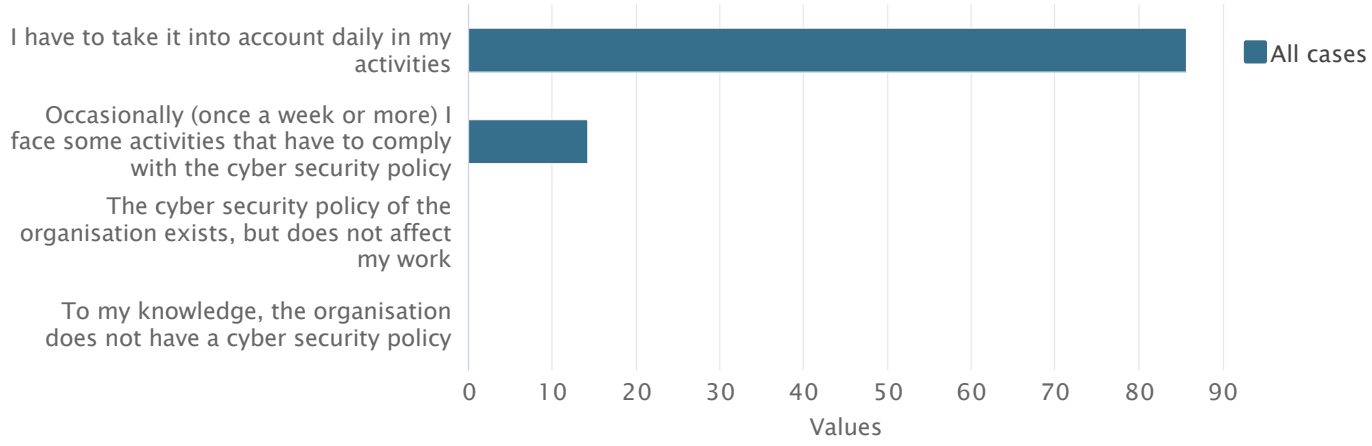
7 Answers



Value	All cases
Total	⌀ 1.9 (n=7)
IT department	86% (6)
Security department	43% (3)
CEO	14% (1)
HSE (Health, Safety and Environment) department	14% (1)
Cybersecurity department	14% (1)
Other (please elaborate)	14% (1)
Business Owner	0
Operations department	0
Do not know	0

Do you feel the cyber security policy of your organisation has an impact on your daily activities?

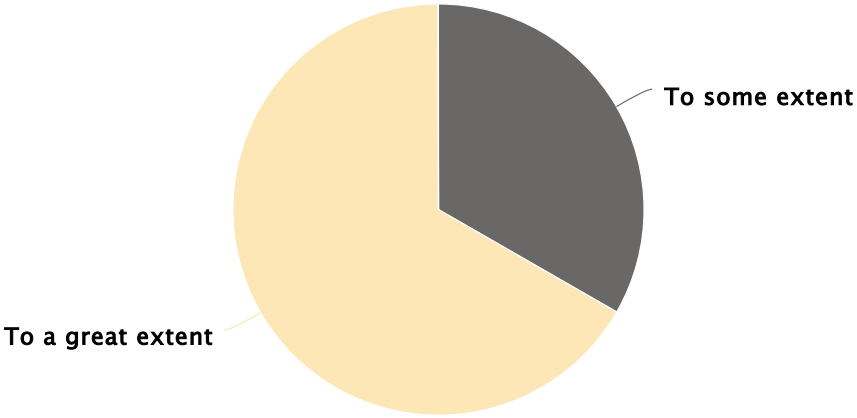
7 Answers



Value	All cases
Total	⌀ 1.1 (n=7)
I have to take it into account daily in my activities	86% (6)
Occasionally (once a week or more) I face some activities that have to comply with the cyber security policy	14% (1)
The cyber security policy of the organisation exists, but does not affect my work	0
To my knowledge, the organisation does not have a cyber security policy	0

Do you think employees in your organisation are aware of the potential impacts of cyber security risks?

6 Answers



Value	All cases
Total	⌀ 3.7 (n=6)
Not at all	0
To a limited extent	0
To some extent	33% (2)
To a great extent	67% (4)
To a very great extent	0
Don’t know	0

What activities or tools do you employ to integrate (occupational and process) safety and cybersecurity management in your organization?

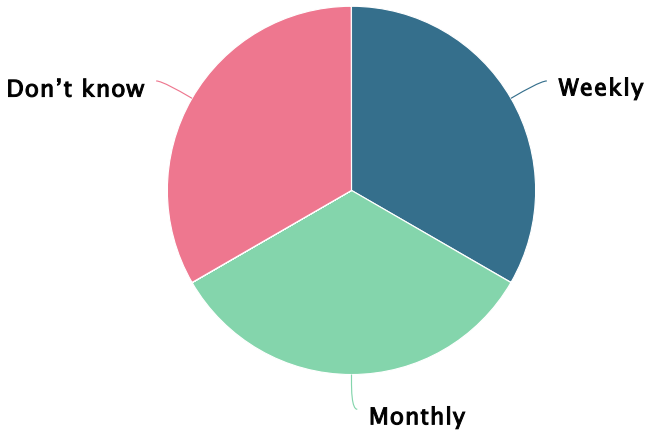
3 Answers

All cases

La gestione di entrambi questi rischi avvengono in maniera integrata e supervisionata dal Chief Risk Officer. Molt e BIA (Business Impact Analisys) vengono svolte congiuntamente dalle rispettive funzioni.
Turvallisuuden mittarit ja niiden seuranta, Läheltä piti -tilanteiden seuranta ja korjaavien toimenpiteiden määritt ely, henkilöstön koulutus, muutoksen hallintajärjestelmien käyttö, turvallisuus- ja prosessiturvallisuusriskinarviot, juurisyyanalyysit
firewall, limitazione accesso ineternet, cirpatzione, server posta esterni al dominio aziendali

How often do safety and security managers have meetings together?

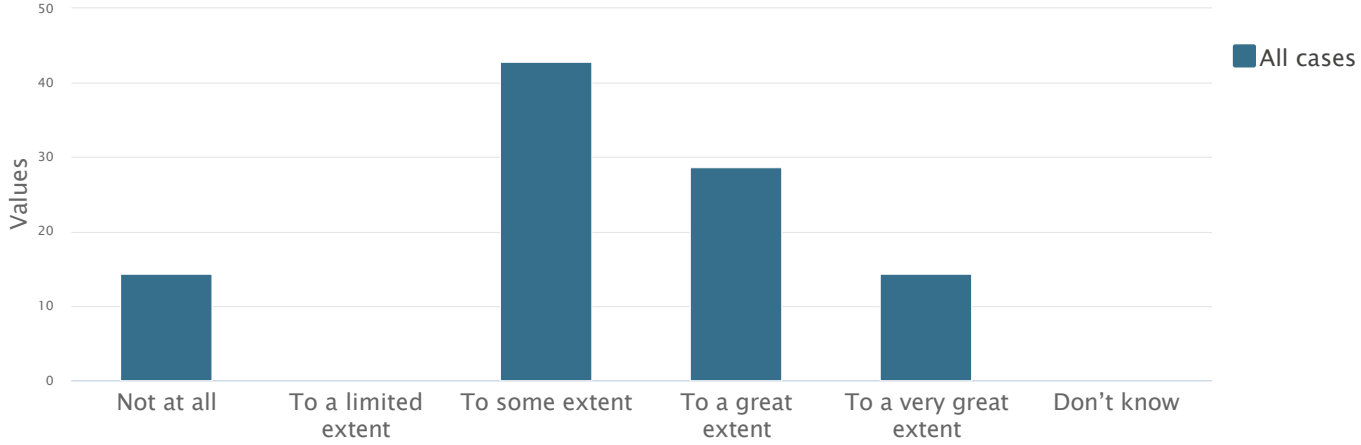
6 Answers



Value	All cases
Total	⌀ 3 (n=6)
Weekly	33% (2)
Monthly	33% (2)
Yearly	0
In relation to specific needs/events	0
Never	0
Don’t know	33% (2)

To what extent do you believe that management of (occupational and process) safety and cyber security are interdependent?

7 Answers



Value	All cases
Total	⌀ 3.3 (n=7)
Not at all	14% (1)
To a limited extent	0
To some extent	43% (3)
To a great extent	29% (2)
To a very great extent	14% (1)
Don’t know	0

Please elaborate your answer.

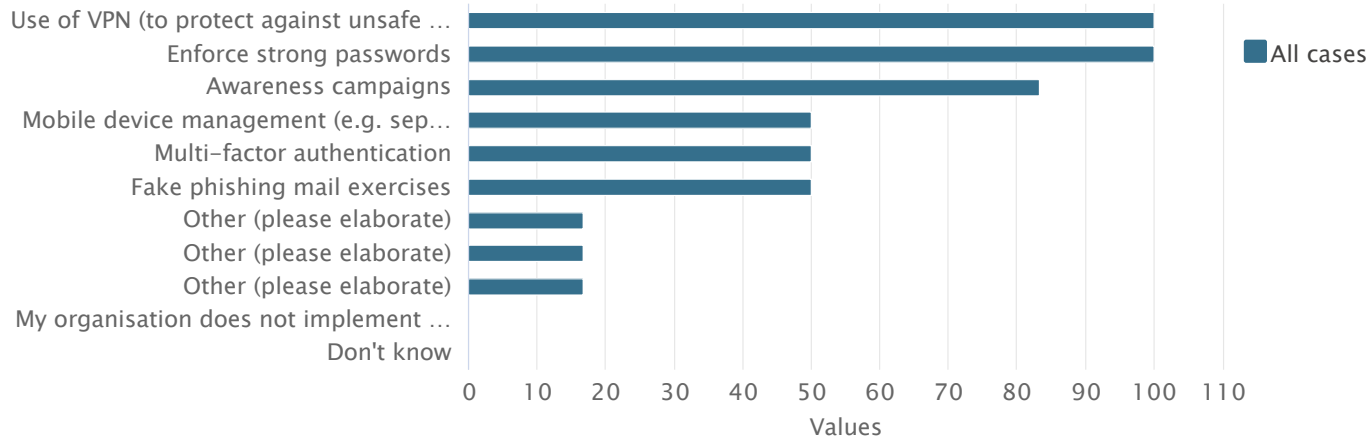
5 Answers

All cases

La risposta a questa domanda varia ovviamente in funzione del business principale del rispondente. Nel nostro ca so sono relativamente pochi gli impatti di un incidente cyber che vedono un coinvolgimento della funzione HSE.
osittain hoidetaan eri osastoilta
Ovat eri osastoja organisaatioineen, mutta tekevät yhteistyötä
Meillä ovat täysin erillisiä asioita.
Misure organizzative controllo accessi e qualificazione appaltatori

Does your organisation implement cyber security interventions aimed at how employees work with systems? Can you indicate which interventions are used within your organisation? (multiple answers possible)

6 Answers



Value	All cases
Total	⌀ 4.8 (n=6)
Use of VPN (to protect against unsafe use of networks)	100% (6)
Enforce strong passwords	100% (6)
Awareness campaigns	83% (5)
Mobile device management (e.g. separating work use and private use of devices)	50% (3)
Multi-factor authentication	50% (3)
Fake phishing mail exercises	50% (3)
Other (please elaborate)	17% (1)
Other (please elaborate)	17% (1)
Other (please elaborate)	17% (1)
My organisation does not implement interventions aimed at how employees work with systems	0
Don't know	0

Other (please elaborate)

All cases

Esercitazioni

Other (please elaborate)

All cases

Misure di protezione degli end point

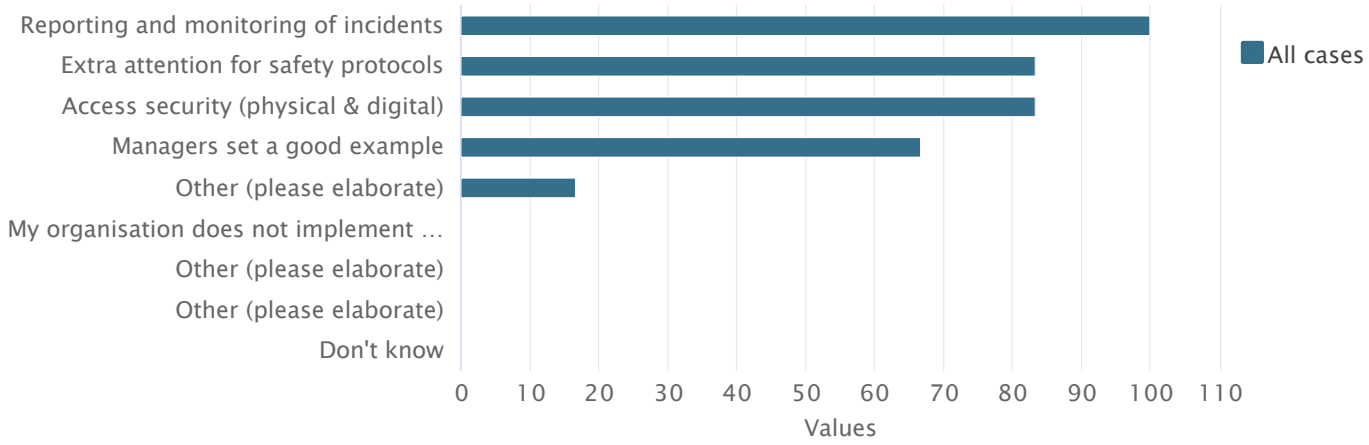
Other (please elaborate)

All cases

Linee guida strumenti di social network

Does your organisation implement cyber security interventions focused on organisational policy? Can you indicate which interventions are used within your organisation? (multiple answers possible)

6 Answers



Value	All cases
Total	⌀ 3.5 (n=6)
Reporting and monitoring of incidents	100% (6)
Extra attention for safety protocols	83% (5)
Access security (physical & digital)	83% (5)
Managers set a good example	67% (4)
Other (please elaborate)	17% (1)
My organisation does not implement interventions focused on organisational policy	0
Other (please elaborate)	0
Other (please elaborate)	0
Don't know	0

Other (please elaborate)

All cases

Relazione periodica della funzione cybersecurity agli Organismi di Vigilanza

Other (please elaborate)

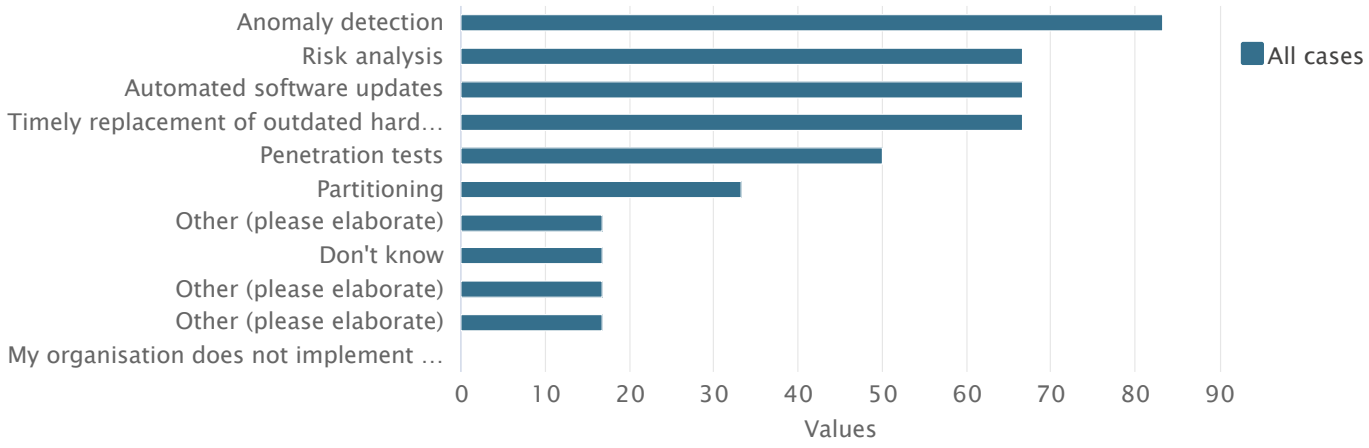
All cases

Other (please elaborate)

All cases

Does your organisation implement cyber security interventions aimed at IT-systems? Can you indicate which interventions are used within your organisation? (multiple answers possible)

6 Answers



Value	All cases
Total	⌀ 4.3 (n=6)
Anomaly detection	83% (5)
Risk analysis	67% (4)
Automated software updates	67% (4)
Timely replacement of outdated hardware	67% (4)
Penetration tests	50% (3)
Partitioning	33% (2)
Other (please elaborate)	17% (1)
Don't know	17% (1)
Other (please elaborate)	17% (1)
Other (please elaborate)	17% (1)
My organisation does not implement interventions aimed at IT-systems	0

Other (please elaborate)

All cases

BIA

Other (please elaborate)

All cases

Monitoraggio di cybersecurity H24

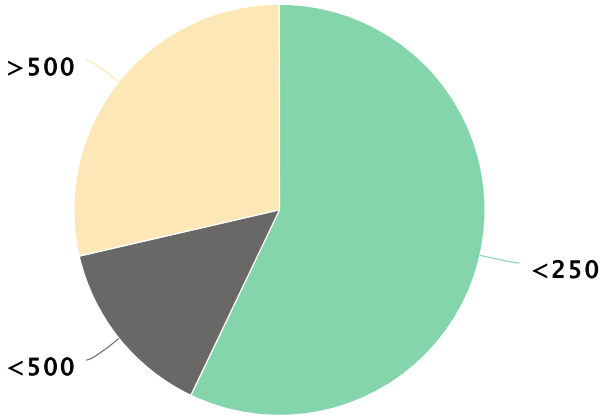
Other (please elaborate)

All cases

Audit di terza parte

How many people does your organisation employ?

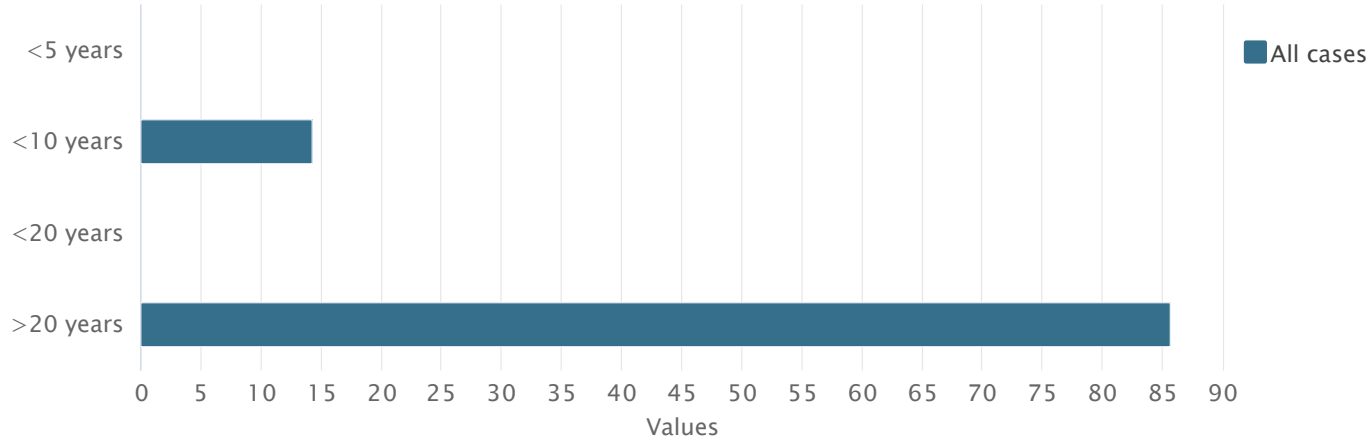
7 Answers



Value	All cases
Total	⌀ 2.7 (n=7)
<50	0
<250	57% (4)
<500	14% (1)
>500	29% (2)

How long ago was your organisation established?

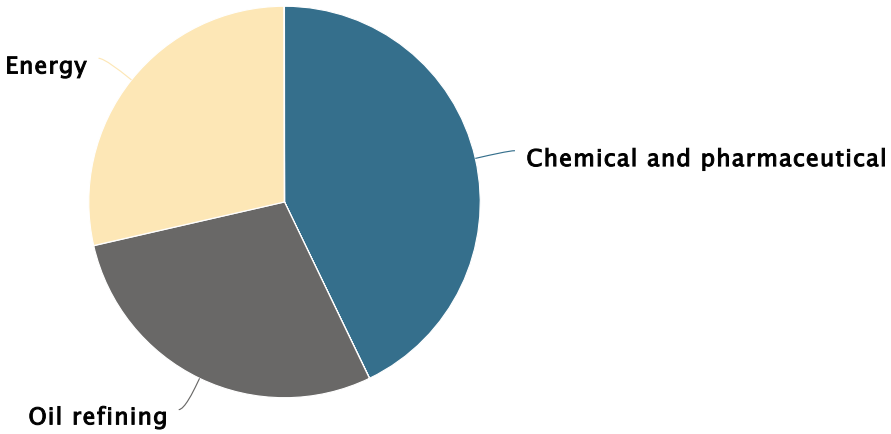
7 Answers



Value	All cases
Total	⌀ 3.7 (n=7)
<5 years	0
<10 years	14% (1)
<20 years	0
>20 years	86% (6)

Which sector does your organisation operate in?

7 Answers



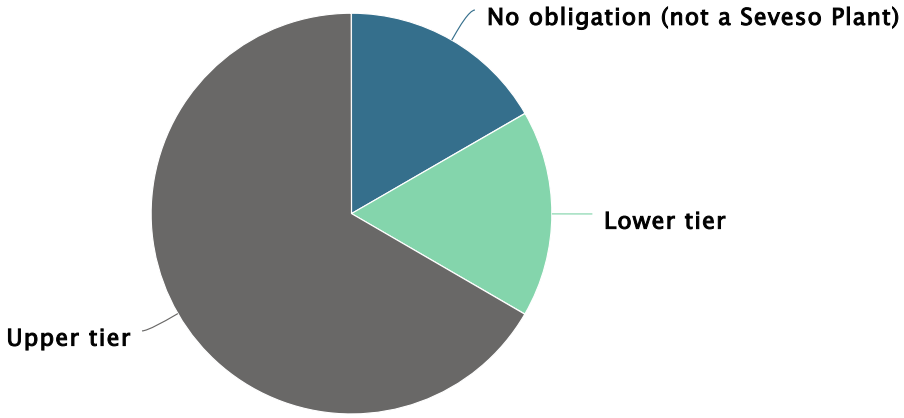
Value	All cases
Total	⌀ 2.4 (n=7)
Chemical and pharmaceutical	43% (3)
Oil & Gas production	0
Oil refining	29% (2)
Energy	29% (2)
Mining	0
Other (please elaborate)	0

Other (please elaborate)

All cases

Which level of obligations does the site have under the Seveso regulation?

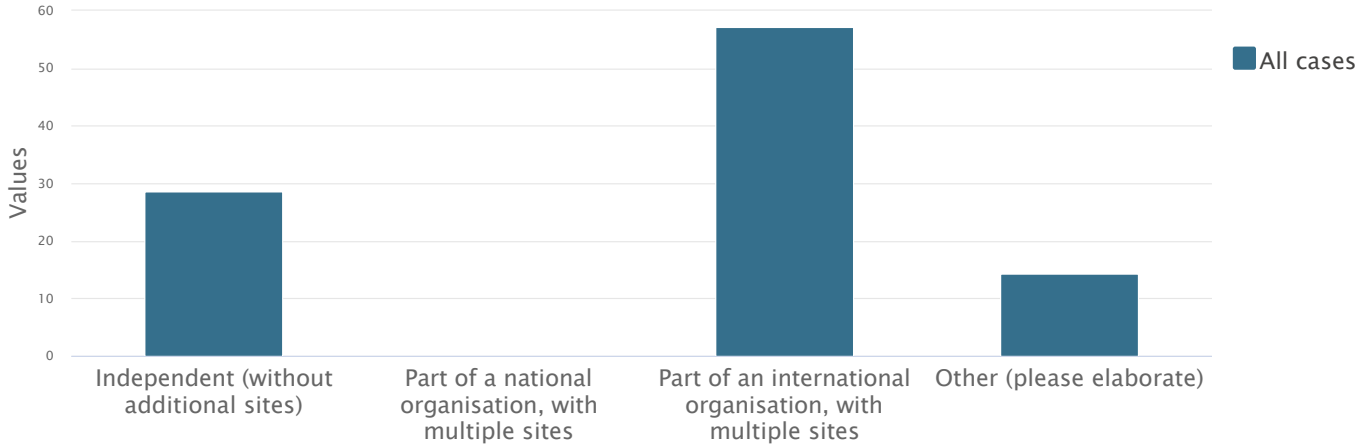
6 Answers



Value	All cases
Total	⌀ 2.5 (n=6)
No obligation (not a Seveso Plant)	17% (1)
Lower tier	17% (1)
Upper tier	67% (4)

How would you describe the structure of your organization?

7 Answers



Value	All cases
Total	⌀ 2.6 (n=7)
Independent (without additional sites)	29% (2)
Part of a national organisation, with multiple sites	0
Part of an international organisation, with multiple sites	57% (4)
Other (please elaborate)	14% (1)

Appendix C: Data and definitions for analysis of past security incidents

Data for the past security incidents was gathered from different sources: scientific literature, the web and specific open-source databases reporting industrial accidents/incidents and near misses:

- The ARIA Database - La référence du retour d'expérience sur accidents technologiques n.d. https://www.aria.developpement-durable.gouv.fr/the-barpi/the-aria-database/?lang=en (accessed December 23, 2020).
- ProcessNet - eine Initiative von DECHEMA und VDI-GVC n.d. https://processnet.org/en/ (accessed December 23, 2020).
- Home - Concawe n.d. https://www.concawe.eu/ (accessed December 23, 2020).
- About EGIG » EGIG n.d. https://www.egig.eu/about-egig (accessed December 23, 2020).
- EUROPA - eMARS Dashboard - European Commission n.d. https://emars.jrc.ec.europa.eu/en/emars/content (accessed December 23, 2020).
- GTD Search Results n.d. https://www.start.umd.edu/gtd/search/Results.aspx?search=&sa.x=54&sa.y=3 (accessed December 23, 2020).
- Infosis / ZEMA n.d. https://www.infosis.uba.de/index.php/de/site/12981/zema/index.html (accessed December 23, 2020).
- RISI - The Repository of Industrial Security Incidents n.d. https://www.risidata.com/Database/Search_Results/search&keywords=Salt+River+Project+Hack/ (accessed December 23, 2020).
- Pipeline and Hazardous Materials Safety Administration n.d. https://www.phmsa.dot.gov/ (accessed December 23, 2020).
- Significant Cyber Incidents | Center for Strategic and International Studies n.d. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (accessed December 8, 2020).

Table 1. Definitions of the classes associated to the itemized fields "Industrial Sector", "Security Threat" and "Final Scenario" used in the collection of all the SRIs.

INDUSTRIAL SECTOR	
Bioprocesses	Treatment of organic waste and waste fermentation juices. Food industry.
Chemical & Petroleum	Chemical production and storage installations, including pesticides production, pharmaceutical industry, production of basic chemicals. Petrochemical production and storage installations, including refineries.
Energy production	Electric power production plants using hydrocarbons (petroleum and natural gas-based fuels), hydroelectric and nuclear plants.
Pipelines	Oil and Gas transportation via pipelines.
Transportation	Transportation of hazardous materials via road, rail, water.
Water / Waste water treatment	Water and wastewater treatment for industrial and domestic purposes, including water supply systems (excluding bioprocesses-related waters and slurries).
SECURITY THREAT	
Outsider cyber-threat (cybersecurity)	Events collected in this category are characterized by an attack, via cyberspace, targeting the IT-OT system of the target facility with the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. Usually, the malwares used by the attackers were not tailored for industrial control systems, but they breached the company network protection compromising operations.
Insider threat (physical security and cybersecurity)	The attacker is an insider, i.e., an individual who normally has authorized access to the assets of the company (e.g., employee, contractor, business partner, vendor, etc.). The motivation is related to working dissatisfaction or possibility of gaining personal advantage (e.g., stealing items or materials). Insider threat refers both to physical security and cybersecurity.
Sabotage (physical security)	Events collected in this category are characterized by an attack mode aimed to disrupt normal operations, but not defined in their threatening agent, as well as in their driving motivations.
Terrorism (physical security)	Terroristic organizations/groups, highly capable, well organized and equipped. Events included in this category have a terroristic matrix, often focused on targeting a facility with the aim of causing a high-impact event, not only in terms of casualties, but also on media.

Theft (physical security)	Criminal groups or individuals attacking facilities with the intent of stealing material. It includes both events of attempted theft that caused an accident and cases of intrusion without reaching the target.
Vandalism (physical security)	Poorly equipped groups or individuals with low level of preparedness and usually no tactic in attack execution.
Unknown (physical security and cybersecurity)	An interference in normal production activities has been achieved via certainly intentional acts, but no more details were given concerning attackers or motivations of the act. This category refers both to physical security and cybersecurity.
FINAL SCENARIO	
Release	Event consisting in the discharge of a chemical from its containment, i.e. the process and storage equipment in which it is kept, without any further consequence such as an explosion or a fire.
Explosion	Event consisting in a physical and/or chemical explosion.
Fire	Event consisting in a pool fire, jet fire, fireball, flash fire, or flame.
Loss of process control/monitoring	Event consisting in the physical or cyber interference with the OT system (software and hardware), without the occurrence of a release of hazardous substances, a fire, or an explosion.
Other	Event that does not result in a release of substances, a fire, an explosion, or a loss of process control/monitoring (e.g. infection of the IT system of a process facility, use of explosives without involving chemical equipment).
Near miss	An event that does not result in an actual final scenario such those described above, but the attack perpetrated by the attackers has the potential to do so. This can be due to the intervention of the security forces to stop the attack and/or the effectiveness of the physical protection system in place.

Table 2. Definitions of the classes associated to the itemized fields “Attack Mode” and “Final Outcome” used in the collection of the SRIs occurred in the Chemical & Petroleum sector.

ATTACK MODE	
Cyber-attack	An attack via the cyberspace to the IT-OT network of a facility that can be accidental (i.e. it is not directed towards a specific target, but that infects any vulnerable host) or intentional (i.e. it is carried out against a specific target and designed to exploit specific weaknesses of the target system).
Armed assault	An armed attack that involves people with guns or other carrying weapons.
Arson	An attack that deliberately consists in setting a fire (e.g. using incendiary weapons or improvised sources of ignition).
Explosive device	An attack that involves explosives, i.e. devices that relies on the exothermic reaction of an explosive material to provide a violent release of energy (e.g. dynamite). The explosive device can be placed directly on the target asset or it can be launched from a point far from it.
Grenade rocketing	An attack that consists in the shooting of missiles launched by a rocket launcher or by remotely controlled drones.
VBIED	Vehicle Borne Improvised Explosive Device. An attack that consists in an improvised explosive device placed and detonated inside a car or other vehicle.
FINAL OUTCOME	
Damage to people	Injury or fatality.
Property damage / economic loss	Physical and economic damages due to loss of an asset for the affected facility, whether it is a loss of production capability, loss of equipment and property, including loss of sensitive data. Loss of life is not included.
Environmental damage	Damages to the ecosystems due to air and/or water pollution, or land contamination.

Table 3. Definitions of the classes associated to the itemized fields “Attacker Type”, “System Infected”, and “Impact” used in the collection of the cyber-SRIs.

ATTACKER TYPE	
Accidental attacker	A cyber-attack not directed towards a specific target, but that infects any vulnerable host, the attacker is generally unknown.
Intentional internal attacker	A cyber-attack carried out against a specific target and designed to exploit specific weaknesses of the target system. The attacker is an insider, i.e., an individual who normally has authorized access to the assets of the company (e.g., employee, contractor, business partner, vendor, etc.). The attacker is generally identified by an investigation.
Intentional external attacker	A cyber-attack carried out against a specific target and designed to exploit specific weaknesses of the target system. The attacker is not an insider, i.e. he has not authorized access to the assets of the company. The attacker generally claims the attack.
SYSTEM INFECTED	
IT system	The hardware and software dedicated to store, retrieve, transmit, and manipulate data, or information.
OT system	The hardware and software dedicated to detect or cause changes in physical processes through direct monitoring and/or control of physical devices such as valves, pumps, compressors, etc.
IMPACT	
Major event	Loss of containment of hazardous material, fire, explosion, toxic dispersion, soil contamination etc.
Economic loss	The attacked company suffers serious economic losses due to e.g., the loss of productivity (downtime), the collapse of the company shares on the stock exchange.
PSD/LSD	PSD (Process Shut Down) or LSD (Local Shut Down) originated either directly or by inducing an anomalous condition or abnormal mode of operation.
OT infection	Infection of the OT system (e.g., infection of HIM workstations, OT servers, etc.)
Data loss or corruption	Theft and/or corruption of sensitive information regarding the company knowhow, employee data, process data (e.g., equipment data sheets, PFDs, P&IDs, historical data, etc.), economic data, etc.
IT infection	Infection of the IT system (e.g., infection of IT server, PCs, etc.)

Table 4. Description of the key elements of Correspondence Analysis (CA)

CONCEPT	DESCRIPTION
Correspondence Analysis	A method of displaying the rows and columns of a table as points in a spatial map, with a specific geometric interpretation of the positions of the points as a means of interpreting the similarities and differences between rows, the similarities and differences between columns and the association between rows and columns.
Contingency table	A table with row and column labels filled with the combined frequencies of two variables; hence the grand total of the table is the number of individuals/events.
Profile	A row or a column of the contingency table divided by its total (i.e. a set of relative frequencies); the profiles are the points visualized in CA, elements of a multidimensional space. Such sets, or vectors, of relative frequencies have special geometric features because the elements of each set add up to 1. In particular, if the profiles are points in a m-dimensional space, they actually occupy a limited region of that space, i.e. a (m-1)-dimensional subspace.
Mass	The marginal total of a row or a column of a table, divided by the grand total of the table; used as weights in CA.
Centroid	The average profile of a row or a column: its elements are respectively the column or row masses.
Vertex	A unit profile, i.e. a profile with all elements zero except one with value 1.
Principal coordinates	Coordinates of a set of points projected onto a principal axis, such that their weighted sum of squares along an axis equals the principal inertia on that axis.
Standard coordinates	Coordinates of a set of points such that their weighted sum of squares along an axis equals 1.
Chi-square distance	Weighted Euclidean distance measure between profiles, where each squared difference between profile elements is divided by the corresponding element of the average profile.
Inertia	Weighted sum of squared distances of a set of points to their centroid; in MCA the points are profiles, weights are the masses of the profiles and the distances are chi-square distances. The inertia can assume zero as minimum value (i.e., all the row or column profiles coincide with the centroid), to a maximum value coinciding with the size of the (m-1)-dimensional subspace (i.e., all the row or column profiles lie exactly on the vertices).

CONCEPT	DESCRIPTION
Reduction of dimensionality	Profiles consisting of m elements are situated exactly in spaces of dimensionality m – 1. Hence, profiles with more than four elements are situated in spaces of dimensionality greater than three that cannot be observed directly. The reduction of dimensionality is the process consisting in the identification of a subspace of lower dimensionality (2D or 3D) which lies close to all the profile points so that it is possible to project the profiles onto such a subspace and look at their projected positions in this subspace as an approximation to their true higher-dimensional positions. What is lost in this process of dimensionality reduction is the knowledge of how far and in what direction the profiles lie "off" this subspace. What is gained is a view of the profiles that would not be possible otherwise.
Percentage of inertia	It is the measure of the accuracy of the reduction of dimensionality (For example, if 85% of the inertia of the profiles is represented in the subspace, then the residual inertia, or error, which lies external to the subspace, is 15%).

Appendix D: Results from analysis of the total number of SRIs

The time trend and the location

Figure D1 a shows the quinquennial time trend of the physical- and cybersecurity-related incidents (respectively 291 and 78 incidents) included in the database. After year 2000, there was a significant increase (almost quadruple) in the number of the incidents recorded, considering both physical-SRIs and cyber-SRIs. In particular, only five cybersecurity-SRIs occurred before 1999, which started to be significant in the last 20 years. This can be justified by the fact that cybersecurity was not a significant threat for process facilities at the time (lower attractiveness, lower level of digitalization and network connection).

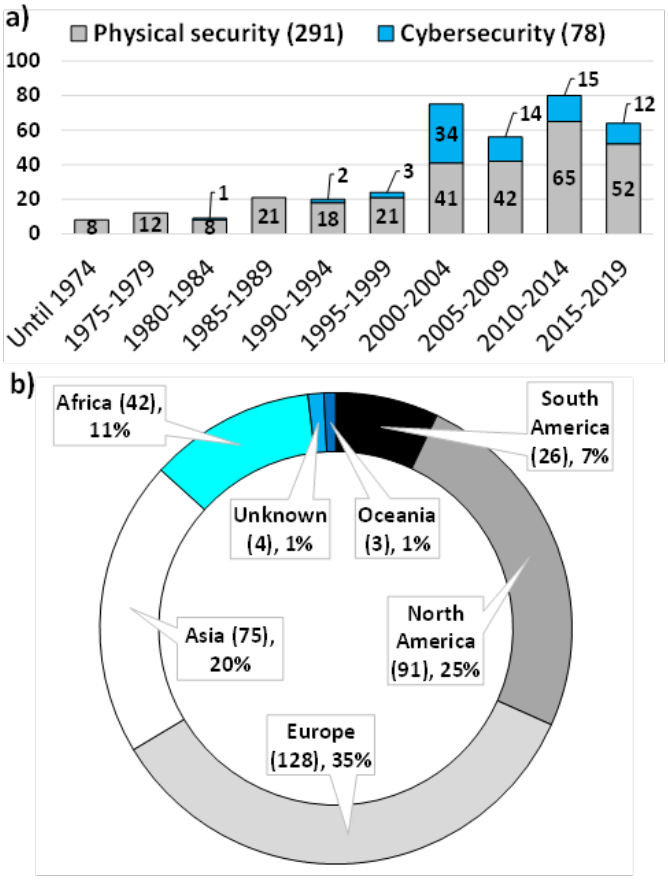


Figure D1 (a) Time trend of the total SRIs recorded; (b) Geographical distribution of the total SRIs recorded.

The time trend of the records shows two peaks: one during the five-year period 2000-2004 (75 SRIs), due to a high number of cyber-attacks all over the world, and one during the five-year period 2010-2014 (80 SRIs), due to a high number of physical attacks. The latter peak might be due to the greater attention paid to the topic in the last decades, promoting incident reporting. For instance, for what concerns cybersecurity, in the last years, companies have increasingly implemented cyber risk analysis (CRA) in the management of their IT-OT systems.

This was supported by the international standards, such as the ISO/IEC 27000 series for IT systems and the ISA/IEC 62443 for the industrial automation and control systems (IACSs). Moreover in 2016 in Europe, the NIS Directive was issued by the European Parliament and Council, setting several goals in the direction of security of IT-OT systems that all EU countries must achieve with specific national regulations. In this context, an increase in cybersecurity awareness by companies and a decrease of cyber-attacks are expected in the coming years.

The geographical distribution of the entries recorded in the database is shown in Figure D1 b. Most of the events took place in Europe (128 SRIs, 35% of the total), followed by America (117 SRIs, 32%, 91 of which in North America and 26 in South America), Asia (75 SRIs, 20%), Africa (42 SRIs, 11%) and Oceania (3 SRIs, 1%). For 4 SRIs (1% of the total) the location is unknown. This result could be in part ascribed to the different reporting practices of each geographic area. For instance, in Australia, accidental events have to be reported when entailing a "serious risk", defined as “the death of a person, a serious incident or illness, or an incident that exposes any person to a serious risk (even if no one is injured)” [1]. A similar legislation is present in U.K. [2]. Differently in U.S., reporting is included in the National Incident Management System, which requires reporting “for all the departments and agencies as well as for the private sector, regardless of cause, size or complexity of the incident” (Department of Homeland Security). A probable under-reporting concerns Asia, as the continent has the greatest number of industrial establishments (UNIDO Statistic Data Portal [3]), but only the 20% of the incidents recorded took place in such continent.

The industrial sectors affected

Figure D2 reports the number of the SRIs recorded in the database with respect to the industrial sectors considered in the present study (defined in the “Methodology” section). Pipelines for crude oil and gas transportation resulted to be the most affected industrial installation by security attacks (132 SRIs, 36% of the total). This can be ascribed to the relatively easy accessibility of pipelines and the inherent difficulties and related cost in protecting them. Moreover, cyber-attacks to the IT-OT systems that manage pipelines can be motivated by the possibility to obtain proprietary information important for the business such as production statistics, market strategies, drilling plans and pricing sheets. However, physical attacks to Oil &Gas pipelines outnumber by far the cyber-attacks (respectively 125 and 7).

The facilities belonging to the Chemical & Petroleum sector turned to be the second most affected by security attacks (100 SRIs, 27 % of the total). This fact is

mainly due to the following reasons: i) the high socio-political impact of the events, first of all for those facilities owned by multinational companies and/or located in critical contexts; ii) the potential severity of consequences in facilities processing or storing large amounts of hazardous materials (e.g., Seveso establishments in Europe). Furthermore, as for pipelines, cyber-attacks to such companies, can be motivated by the possibility of obtaining proprietary information, important for business (e.g., patents of specific processes).

A total of 66 SRIs was recorded for the energy production sector (18% of the total) and 42 SRIs for transportation via road, rail and water (11%). Only 19 entries involved facilities belonging to the water/wastewater treatment sector (5% of the total) and 6 belonging to the sector of bioprocesses (2%). These are relatively small numbers considering the fact that the worldwide number of water/wastewater and bioprocesses plants is by far higher compared to that of chemical and petrochemical plants as reported by UNIDO Statistical Data Portal [3]. This can be justified considering two factors that stoke each other. Firstly, the security level of water/wastewater treatment plants is high because of the severe consequences on humans and the environment that can potentially be generated by malicious acts aiming at polluting water [4]. Secondly, the attractiveness of these facilities is low due to the limited amount of hazardous materials processed. This makes them target of few threat actors, only those that aim at polluting water and are able to perform such attack (e.g. terrorist groups).

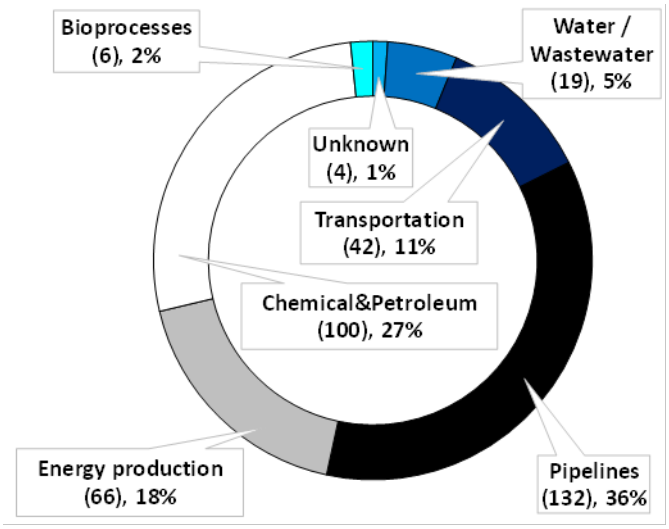


Figure D2. Distribution of the events with respect to the industrial sectors.

Security threats

The share of the 369 SRIs recorded in the database with respect to the security threats (defined in the “Methodology” section) is presented in Figure D3. Terrorism resulted to be the most important threat category for the industrial installations with 104 SRIs recorded, the 27% of the total. In particular. It plays an important role for the pipelines for oil and gas transportation, for the chemical and petrochemical facilities and for the energy production sector, whose attractiveness has been previously discussed. Groups of terrorists can be motivated by political and/or monetary gain, revenge or destruction [5]. The figure also reveals that terrorism is not a relevant security threat for transportation via road, rail or water, for water/wastewater plants and bioprocesses companies, due to their lower attractiveness.

Outsider cyber threat, with 73 SRIs recorded (20%) is among all, the second most important threat category. It is relevant for all the industrial sectors considered in the present study with the logical exception of the transportation sector. Typically, there is no possibility to connect remotely to the networks managing the operations of such transportation systems (it may be possible for a train [6, 7], but difficultly for a truck. Nevertheless, transportation is an easy target for vandals (35 of the total 56 SRIs of vandalism occurred in this sector).

Fifty (50) SRIs (14% of the total) were characterized by theft of materials: most of them occurred in the oil and gas pipelines (e.g. theft of crude oil or natural gas). However, this class of security threat is affected by under-reporting, since thefts are very common events [8].

Sabotage (40 SRIs, 11% of the total) is common to almost all the industrial sectors, as well as the insider threat, the latter being less common (14 SRIs, 4%). Insiders are potentially a very critical category of attackers since they usually have extensive knowledge of both the process and the plant, and they usually have physical and/or remote authorized access to the assets of the facility they work for (they do not need to bypass all the security barriers in place as for outsider attackers).

For a high number of incidents (32 SRIs, 9% of the total) it was not possible to identify the threat category, which fell into the category “unknown”.

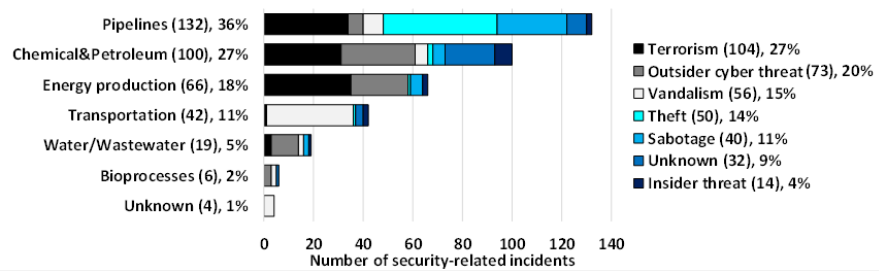


Figure D3. Share of security threats with respect to the industrial sectors.

Results of Correspondence Analysis

Correspondence Analysis (CA) was used to looking for correlations among the different itemized fields considered in the database. In particular, CA was used to test the presence of correlations among the type of security threat, the geographical area, the industrial sector, and the final scenario triggered by the threat actor. More specifically, four couples of itemized fields were investigated through MCA:

1. "Location" – "Security Threat";
2. "Industrial Sector" – "Security Threat";
3. "Industrial Sector" – "Final Scenario";
4. "Security Threat" – "Final Scenario".

Due to both a low inertia (i.e. the behaviour of the profiles is similar to the average profile) and a low quality of the 2D-map of the profiles (i.e. the percentage of inertia – see definition in Appendix C – that resulted less than 80%,), the outputs of the CA for the couples "Location" vs. "Security Threat" and "Industrial Sector" vs. "Final Scenario" resulted of scarse interest and therefore were not reported below. On the contrary, strong correlations were found for the other two couples of itemized fields ("Industrial Sector" vs. "Security Threat" and "Security Threat" vs. "Final Scenario").

Figure D4 a shows the contingency table of the couple "Industrial Sector" vs. "Security Threat". The numbers outside the brackets correspond to the combined numbers of SRIs that were collected in the updated database for each couple of labels "sector - scenario", while the numbers in brackets correspond to the relative frequencies in the row (i.e. the number of events divided by the total in the row). Each of the six row frequency vectors is a row profile, i.e. a point in a 5-dimensional subspace, as explained in Appendix C. It may be remarked that the grand total of SRIs in the table (i.e. 333) does not coincide with the total number of the SRIs recorded in the database (i.e. 369), as the incidents with unknown security threat or unknown industrial sector were not considered in the CA.

Figure D4 b shows the 2D-map of the CA based on the contingency table discussed above. The graph represents the row analysis and displays the security threats in principal coordinates (i.e. those deriving from the row profiles) and the industrial sectors in standard coordinates (i.e. as unit vectors). It is important to remark that the map contains the projections of the real points in the best-fitting 2D-plane (see reduction of dimensionality in Appendix C): this means that some information is missing. In particular, the percentage of inertia shown by the map is 95.1% and, consequently, the information loss is 4.9%: this means that the correlations that can be obtained from the analysis are a very good representation of reality. The origin of the graph represents the centroid, i.e. the average row profile of the entire dataset, considering all the security threats. The points representing the security threats that are close to the centroid are those that differ the least from the average profile, while the points that are more distant from the origin are those for whom it is possible to find correlations with a specific industrial sector, as they have a different behaviour with respect to the average profile.

a)

	Bioprocesses	Chemical&Petroleum	Energy Production	Pipelines	Transportation	Water/Wastewater	TOTAL
Outsider cyber threat	3 (0,041)	30 (0,411)	23 (0,315)	6 (0,082)	0 (0,000)	11 (0,151)	73
Insider threat	0 (0,000)	7 (0,500)	2 (0,143)	2 (0,143)	2 (0,143)	1 (0,071)	14
Sabotage	0 (0,000)	5 (0,125)	5 (0,125)	28 (0,700)	0 (0,000)	2 (0,050)	40
Terrorism	0 (0,000)	31 (0,298)	35 (0,337)	34 (0,327)	1 (0,010)	3 (0,029)	104
Theft	0 (0,000)	2 (0,040)	1 (0,020)	46 (0,920)	1 (0,020)	0 (0,000)	50
Vandalism	2 (0,038)	5 (0,096)	0 (0,000)	8 (0,154)	35 (0,673)	2 (0,038)	52
TOTAL	5 (0,015)	80 (0,240)	66 (0,198)	124 (0,373)	39 (0,117)	19 (0,057)	333

b)

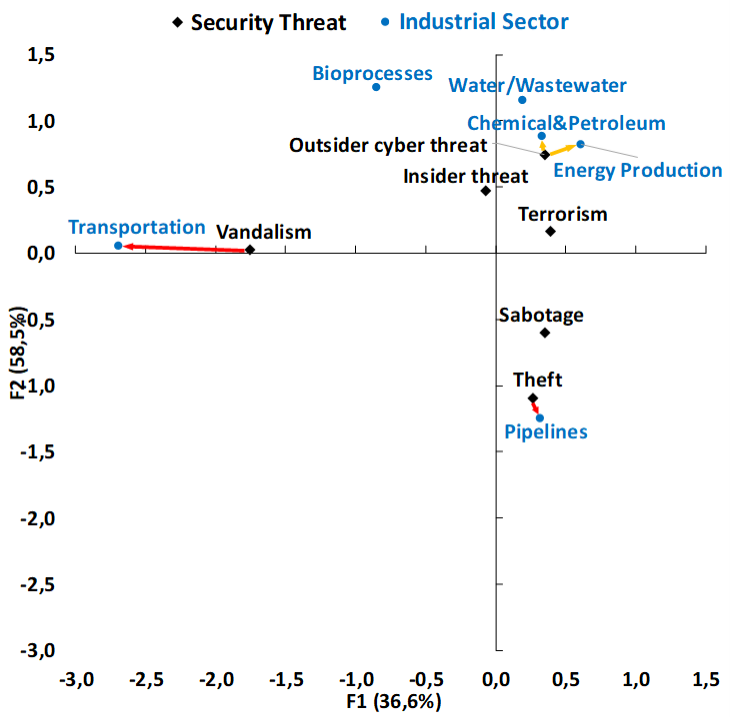


Figure D4 a). Contingency table reporting the combined number of SRIs and row relative frequencies; (b) 2D-map reporting the results of Correspondence Analysis for the couple of itemized fields “Security Threat” and “Industrial Sector” (percentage of inertia of the map is 95.1%).

The correlation between security threats and industrial sectors is shown in the 2D-map by the distance between the two respective points: a smaller the distance indicates a higher correlation. In particular, two strong correlations were found (red shaded in the contingency table of Figure D4 a): one between "Vandalism" and "Transportation", and the other between "Theft" and "Pipelines". This means that the infrastructures for transport via road, rail or water such as trucks, trains and ships, are those which are mainly affected by acts of vandalism, and that the trend of vandalism strongly differs from the average behaviour of all the threats with respect to the industrial sectors. In other words, there is a correlation. In the same way, thefts are closely correlated with pipelines.

Moreover, a weak correlation between "Outsider cyber threat" with both “Chemical & Petroleum” and “Energy Production” sectors, was found (orange shaded in the contingency table shown in Figure D4 a. This correlation is weak because the point corresponding to "Outsider cyber threat", despite being at a very small distance from the points representing “Chemical & Petroleum” and “Energy Production”, is not so far from the origin of the graph (i.e. the centroid).

Finally, it was not possible to find correlations between "Insider threat", "Terrorism", "Sabotage" and the industrial sectors. From the contingency table it is possible to notice that these security threats mainly affect the Chemical & Petroleum sector, the energy production sector and the pipelines, but this trend is similar to that of the average profile of the security threats (i.e. corresponding points are close to the centroid).

Figure D5 a shows the contingency table of the couple of itemized fields “Security Threat” and "Final Scenario". The grand total of the contingency table is equal to 309 since for 60 out of 369 SRIs collected in the updated database the threat and/or the final scenario triggered by the threat actor was unknown. The 2D-map of CA resulted from this table is shown in Figure D5 b. The graph represents the row analysis and displays the security threats in principal coordinates and the final scenarios in standard coordinates. The percentage of inertia shown by the map is 97.7% and, consequently, the information loss is 2.3%. Thus, the correlations obtained from the analysis are an extremely good representation of reality.

Five strong correlations (red shaded in the contingency table shown in Figure D5 a and a weak correlation (orange shaded) were identified. "Vandalism" and "Theft" results to be strongly correlated with "Release". This means that a loss of containment of a hazardous substance can be considered as a reference scenario triggered by security attacks performed by vandals and thieves. Since from the analysis of the correlation among "Security Threat" and “Industrial Sector” reported in Figure D4 “Theft” resulted correlated with “Pipelines” and “Vandalism” with “Transportation”, a release turns out to be a scenario that should be considered in a security risk assessment (SRA) of such industrial infrastructures.

a)

	Explosion	Fire	Loss of process C/M	Near miss	Other	Release	TOTAL
Outsider cyber threat	2 (0,027)	0 (0,000)	40 (0,548)	0 (0,000)	31 (0,425)	0 (0,000)	73
Insider threat	4 (0,286)	1 (0,071)	6 (0,429)	0 (0,000)	2 (0,143)	1 (0,071)	14
Sabotage	21 (0,619)	5 (0,147)	1 (0,029)	0 (0,000)	1 (0,029)	6 (0,176)	34
Terrorism	73 (0,848)	6 (0,070)	1 (0,012)	2 (0,023)	3 (0,035)	1 (0,012)	86
Theft	7 (0,143)	0 (0,000)	0 (0,000)	0 (0,000)	0 (0,000)	42 (0,857)	49
Vandalism	1 (0,019)	3 (0,057)	0 (0,000)	0 (0,000)	0 (0,000)	49 (0,924)	53
TOTAL	108 (0,350)	15 (0,049)	48 (0,155)	2 (0,006)	37 (0,120)	99 (0,320)	309

b)

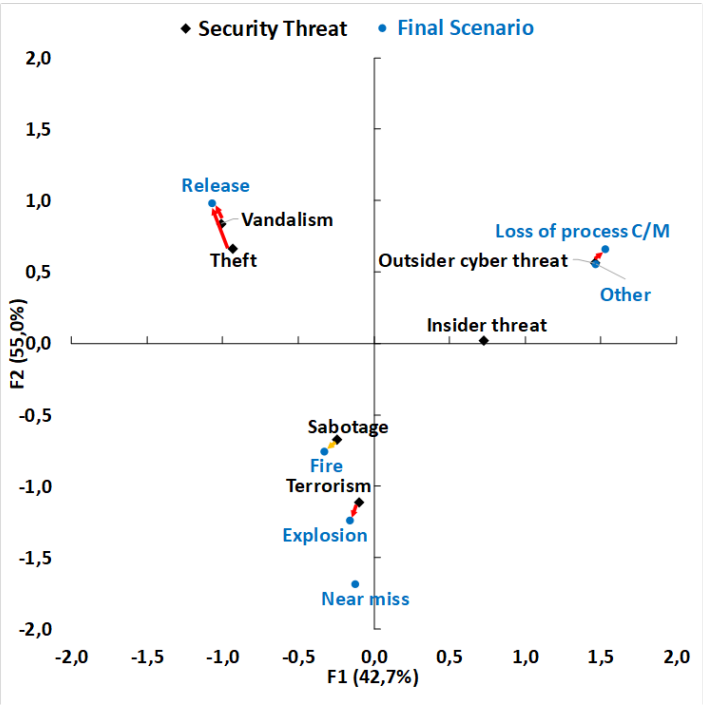


Figure D5 (a) Contingency table reporting the combined number of SRIs and row relative frequencies; (b) 2D-map reporting the results of Correspondence Analysis for the couple of itemized fields “Security Threat” and “Final Scenario” (percentage of inertia of the map is 97.7%).

Similarly, "Outsider cyber threat" resulted strongly correlated with both the final scenarios "Other" (the two points coincide) and "Loss of process control/monitoring". This means that these two scenarios should be considered when cyber threats are assessed in the framework of a SRA. Since this threat has a weak correlation with the chemical, petrochemical and energy production facilities (see Figure D4 b), a malicious interference with the Basic Process Control System (BPCS) and/or the Safety Instrumented System (SIS) should be taken into account in the security analysis of these facilities.

Moreover, "Terrorism" turned out to be closely correlated with the final scenario "Explosion", which therefore can be considered as a reference scenario when terrorism is assessed in a SRA. Finally, “Sabotage” resulted weakly correlated with "Fire": the correlation is weak because of both the small distance from the origin of the graph (i.e. the centroid) of the point corresponding to "Sabotage" and the small number of events labeled as "Fire" (14). No correlation with final scenarios was evidenced by the data analysis for the “Insider threat” security threat.

[1] Safe Work Australia. Incident Reporting 2008.

[2] Health and Safety Executive (HSE). RIDDOR - Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 2003.

[3] UNIDO - United Nations Industrial Development Organization. INDSTAD 2 2019, ISIC Revision 3 database 2019.

[4] Water Security Agency. EPB 363- Security at Water Treatment Plants n.d.

[5] American Petroleum Institute (API). Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries. Washington: API Publication; 2003.

[6] Kour R, Karim R, Thaduri A. Cybersecurity for railways - A maturity model. Proc Inst Mech Eng Part F J Rail Rapid Transit 2019.

[7] Pawlik M. Railway Safety and Security Versus Growing Cybercrime Challenges. Commun Comput Inf Sci 2019;1049:57–68.

[8] Casson V, Reniers G, Salzano E, Cozzani V. Analysis of physical and cyber security-related events in the chemical and process industry. Process Saf Environ Prot 2018;116:621–31. https://doi.org/10.1016/j.psep.2018.03.026.

Appendix E: Definitions of key terms for cyber-attack characterization

Term	Definition	Ref.
Vulnerability	Flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's integrity or security policy.	[1]
Cyber-threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image or reputation), organizational assets, individuals, other organizations or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.	[2]
Impact	Result of an incident, usually described in terms of health and safety effects, environmental impacts, loss of property, loss of information, and/or business interruption costs, that occurs from a particular incident.	[1]
Countermeasure	Device, procedure, or technique that reduces a threat, a vulnerability, or the impacts of an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.	[1]

[1] International Society of Automation (ISA), International Electrotechnical Commission (IEC). ISA/IEC 62443 Series of Standards: Industrial Automation and Control Systems Security 2018.

[2] National Institute of Standards and Technology (NIST). Glossary of Key Information Security Terms. 2nd ed. Gaithersburg: 2013.

Appendix F: Selected cybersecurity-related incidents used in the discussion of the phases of intentional attack and countermeasures

Cyber-SRI	Year	Continent	Industry type	Attack	Type of attack	Impact
A	1982	Asia	Petro-chemical	A trojan horse was introduced into the control system of the Trans-Siberian gas pipeline.	Intentional, external	The pressure inside the pipeline increased, giving rise to an explosion which caused huge economic losses. There were no fatalities.
B	1992	Europe	Energy production	A computer programmer introduced a malware into one of the computer stations in order to sabotage a nuclear reactor.	Intentional, internal	The cooling system in the first reactor broke down resulting in the reactor LSD.
C	1999	Asia	Petro-chemical	A trojan horse was introduced into the SCADA system of a Russian pipeline.	Intentional, external	Loss of process control/monitoring.
D	2003	Europe	Chemical	Blaster worm entered the OT system of a chemical plant through a poorly configured firewall. It was later discovered by the AV software.	Accidental	Infection of a couple of HMIs.
E	2003	Europe	Petro-chemical	A corporate user installed an unpatched software. After contracting Slammer worm, the	Accidental	Data loss.

Cyber-SRI	Year	Continent	Industry type	Attack	Type of attack	Impact
				user connected the infected machine to the historicization network (in violation of company policies), causing a small outbreak of the worm.		
F	2003	Europe	Petro-chemical	The MUMU worm entered the OT system of a petrochemical plant exploiting a weak admin password.	Accidental	Infection of the fiscal metering system.
G	2003	USA	Petro-chemical	SQL Slammer worm entered the OT system of a petrochemical plant and was able to perform a Denial of Service (DoS) attack.	Intentional, external	Traffic was intermittent between HMIs, PLCs and the SCADA servers.
H	2003	Americas	Energy production	SQL Slammer worm entered the IT system of an energy production plant and was able to perform a Denial of Service (DoS) attack. The infection also took the OT system due to the absence of a firewall between the corporate and control and supervision networks.	Accidental	Data overload resulting in the inability of the computers to communicate with each other.
I	2004	Europe	Petro-chemical	Sasser worm entered the OT system of a petrochemical plant through a poorly configured firewall. The spread of the worm was favoured by the absence of AV	Accidental	A couple of HMIs became infected.

Cyber-SRI	Year	Continent	Industry type	Attack	Type of attack	Impact
				software and of patched software on the devices connected to the network.		
J	2004	Americas	Water / Waste-water	A trojan backdoor was accidentally installed on an HMI workstation by an operator browsing external hot-mail websites.	Accidental	An HMI workstation became infected.
K	2005	Asia	Energy production	An unknown file-swapping worm infected a worker's computer.	Intentional, external	Loss of confidential data regarding Japanese nuclear plants.
L	2007	Unknown	Energy production	An employee was victim of a phishing attack that gave the attackers access to the employee's computer which was later connected to the control and supervision network.	Intentional, external	Infection of the SCADA system without severe consequences.
M	2008	Europe	Petro-chemical	Attackers intentionally shut down alarm systems, cut off communications and pressurized a section of the BTC crude oil pipeline.	Intentional, external	The attack resulted in an explosion, in the release of more than 30,000 barrels of oil in an area above a water aquifer, in a fire lasting more than two days, and in losses for BP and its partners of $5 million a day.

Cyber-SRI	Year	Continent	Industry type	Attack	Type of attack	Impact
N	2008	Americas	Petro-chemical	A disgruntled employee accessed and disabled the system that monitors the detection of pipeline leaks for three oil derricks.	Intentional, internal	The leak detection system was shut-down.
O	2010	Asia	Energy production	Stuxnet worm entered the network of the Natanz nuclear power plant by un infected USB stick, then bypassed all the safety barriers until reprogramming the PLC logics.	Intentional, external	The spinning speed of the centrifuges was modified, damaging thousands of them. The uranium enrichment process was stopped for about one week, causing huge economic losses.
P	2012	Unknown	Petrochemical	An unknown worm entered the IT system of a petrochemical plant through an infected USB stick.	Accidental	Infection of a local IT operator panel.
Q	2014	Americas	Energy production	Attackers entered the IT system exploiting a weak password by means of a brute force attack.	Intentional, external	No significant impacts at IT level.
R	2014	Americas, Europe	Energy production	The industrial espionage group Dragonfly entered the IT systems of many energy production plants by means of infected emails, compromised websites and malware inserted in third-party software packages.	Intentional, external	Loss of confidential data.

Cyber-SRI	Year	Continent	Industry type	Attack	Type of attack	Impact
S	2016	Americas	Water / Waste-water	Attackers entered the IT system of a water utility by means of a phishing attack. Then they obtained access to the OT system and were able to reprogram the PLCs that manage the plant devices such as valves and pumps.	Intentional, external	The levels of chemicals used to treat tap water were changed.
T	2019	Americas	Chemical	Ransomware attacks hit the chemical companies Momentive and Hexion.	Intentional, external	Files were encrypted and the IT system was shutdown.

Series title and number

VTT Technology 386

Title	**Integrated Management of Safety and Security Synergies in Seveso plants (SAF€RA 4STER)** Final report
Author(s)	M Ylönen, M Nissilä, J Heikkilä, N Gotcheva, A Tugnoli, M Iaiani, V Cozzani, G Oliva, R Setola, G Assenza, D van der Beek, W Steijn, H Young, M Roelofs
Abstract	This is the final report summarises the main results of the research project on Integrated Management of Safety and Security Synergies in Seveso plants (SAF€RA 4STER). The objectives of the research project were the following: 1) To gain insights into synergies and tensions related to the management of safety and security in Seveso plants. 2) To find a solution to the challenge of managing safety and security in a coordinated manner. 3) To provide guidelines for managing safety and security in an integrated way in Seveso plants. 4) To provide tools for the identification of security scenarios triggered by malicious human intentions. The research data included literature reviews on concepts and management of safety, security, cybersecurity; interviews with regulators and safety and security experts on Seveso sites; analysis of past accidents induced by malicious human intent both in the form of physical security violence and cybersecurity interference, and survey on cybersecurity awareness and physical security awareness in companies. Past incident analysis showed that terrorism and cyberattacks were the most important threat categories for Seveso plants. Even though, past incident analysis showed that no major events occurred in chemical or petrochemical facilities due to cyber-attacks, they remain a relevant threat category, and worth paying attention to. This is because of the current trend towards growing digitalisation, automation and blurring boundaries between IT and operational technology (OT) systems in high-risk industries, makes OT systems vulnerable to cybersecurity attacks. Cybersecurity awareness in Seveso plants was reported to be at a good level. However, survey respondents had seen ignorance and negligence in their companies regarding cybersecurity. It is possible to create technological barriers, e.g., firewalls, anti-virus software, and to design IT systems so that they direct people to act securely without the need for people to make their own choices. Furthermore, human and organizational barriers, such as integrated management and safety and security culture, are needed. Institutional support to integrated management is weak. The Seveso directive does not require integration. Often cybersecurity is dealt with by IT department, and process-safety and cybersecurity risks are handled separately. These do not contribute to integration. The Responsible Care programme and Environment, Health and Safety and Security (EHS&S) management system adopted by many Seveso plants, do combine different standards into the same management system and thus they represent structural integration. However, they are not sufficient to tackle systemic risks, deriving from interconnectedness of technological and organisational systems and related risks. Integrated management would benefit from risk assessments, in which process-safety risks, physical security risks and cybersecurity risks and their significance would be examined together, e.g. in the same Hazop study. The integrated management would require deep understanding of systemic risks, and new safety and security thinking, and close collaboration between different safety and security experts. Both single plants and industrial parks would benefit from Integrated management.
ISBN, ISSN, URN	ISBN 978-951-38-8746-9 ISSN-L 2242-1211 ISSN 2242-122X (Online) DOI: 10.32040/2242-122X.2021.T386
Date	April 2021
Language	English, Finnish abstract
Pages	84 p. + app. 66 p.
Name of the project	
Commissioned by	
Keywords	Digitalisation, cybersecurity, physical security, safety, risks, security scenarios, integrated management, Seveso plant
Publisher	VTT Technical Research Centre of Finland Ltd P.O. Box 1000, FI-02044 VTT, Finland, Tel. 020 722 111, https://www.vttresearch.com

Julkaisun sarja ja numero

VTT Technology 386

Nimeke	**Integrated Management of Safety and Security Synergies in Seveso plants (SAF€RA 4STER)** Final report
Tekijä(t)	M Ylönen, M Nissilä, J Heikkilä, N Gotcheva, A Tugnoli, M Iaiani, V Cozzani, G Oliva, R Setola, G Assenza, D van der Beek, W Steijn, H Young, M Roelofs
Tiivistelmä	Tämä raportti esittää Integrated Management of Safety and Security Synergies in Seveso plants (SAF€RA 4STER) -tutkimusprojektin keskeiset tulokset. Tutkimuksen tavoitteena oli 1) saada ymmärrys turvallisuuden (safety) ja turvauhkien (security) hallintaan liittyvistä synergioista ja jännitteistä Seveso-laitoksilla, 2) löytää ratkaisu turvallisuuden ja turvauhkien hallintaan koordinoidulla tavalla, 3) tuottaa ohjeistus turvallisuuksien turvallisuuden ja turvauhkien integroituun hallintaan Seveso-laitoksilla, 4) tuottaa välineitä tunnistaa turvauhkaskenaarioita (security). Aineisto koostuu turvaa (security) ja turvallisuutta (safety) sekä niiden hallintaa koskevasta kirjallisuuskatsauksesta, kyberturvatietoisuutta koskevasta kirjallisuuskatsauksesta, Seveso-laitosten turva-asiantuntijoiden haastatteluista, Tapahtuneiden onnettomuuksien analyyseista sekä kyberturvatietoisuutta ja turvauhkatietoisuutta koskevasta kyselystä. Tapahtuneiden onnettomuuksien analyysi osoitti, että terrorismi ja kyberhyökkäykset ovat suurimmat turvauhkakategoriat Seveso-laitoksille. Kyberhyökkäyksiin tulee varautua, vaikka ne eivät olekaan aiheuttaneet vakavaa onnettomuutta kemian- ja petrokemianlaitoksilla. Tämä siksi, että lisääntyvä digitalisaatio- ja automaatiokehitys sekä hämärtyvät rajat informaatioteknologiajärjestelmien (IT) ja tuotantoon liittyvien järjestelmien (OT) välillä tekevät OT:n haavoittuvaksi kyberhyökkäyksille. Haastattelujen ja tehdyn kyselyn perusteella kyberturvatietoisuus on Seveso-laitoksilla hyvällä tasolla. Toisaalta kyselyyn vastaajat olivat havainneet yrityksissään tietämättömyyttä ja välinpitämättömyyttä kyberturvallisuuden suhteen. Turva- ja turvallisuusriskeiltä suojautumiseksi on mahdollista luoda teknologisia suojauksia, esimerkiksi suunnitella IT-järjestelmä siten, että ne ohjaavat ihmisiä toimimaan turvallisesti ilman, että heidän tarvitsee tehdä valintoja. Lisäksi palomuurit, anti-virus -ohjelmat sekä IT- ja OT-järjestelmien suunnittelu ovat tärkeitä suojaamiskeinoja. Teknologisten suojausten lisäksi tarvitaan organisatorisia suojauksia. Näillä tarkoitetaan esimerkiksi integroitua turvallisuusjohtamista ja turvallisuuskulttuuria. Institutionaalinen tuki integraatiolle on heikko siinä mielessä, että nykyiset lait ja Seveso-direktiivi eivät vaadi integraatiota. Usein kyberturvallisuutta hoitaa erillinen IT-osasto ja prosessiturvallisuutta ja kyberturvallisuutta tarkastellaan erikseen. Tällainen eri turvallisuuksien hallinnan siiloutuminen ei tue integraatiota. Myöskään Seveso-laitoksilla yleinen Responsible Care -ohjelma ja yhdistetty ympäristö- terveys- ja turvallisuusjohtamisjärjestelmä (EHS&S), jotka yhdistävät erilaisia standardeja ja edustavat rakenteellista integraatiota, eivät ole riittäviä systeemisten riskien hallitsemiseksi. Systeemisillä riskeillä tarkoitetaan erilaisten teknologisten ja organisatoristen järjestelmien tiivistä yhteenkietoutumista ja näistä syntyviä riskejä. Integroitu hallinta hyötyisi esimerkiksi riskiarvioinneista, joissa prosessiturvallisuusriskejä, kyberturvallisuusriskejä ja fyysisiä turvallisuusriskejä ja niiden merkitystä tarkasteltaisiin yhdessä. Systeemisten riskien integroitu hallinta edellyttää uutta turvallisuusajattelua ja yhteistyötä erilaisten asiantuntijoiden kanssa, jotta voidaan paremmin tunnistaa, hallita ja lieventää riskejä. Turvallisuuden ja riskien integroidusta hallinnasta hyötyvät sekä yksittäiset laitokset että laitosryppäät, kuten teollisuuspuistot.
ISBN, ISSN, URN	ISBN 978-951-38-8746-9 ISSN-L 2242-1211 ISSN 2242-122X (Verkkojulkaisu) DOI: 10.32040/2242-122X.2021.T386
Julkaisuaika	Huhtikuu 2021
Kieli	Englanti, suomenkielinen tiivistelmä
Sivumäärä	84 s. + liitt. 66 s.
Projektin nimi	
Rahoittajat	
Avainsanat	Digitalisaatio, kyberturvallisuus, turvauhka, turvallisuus, riskit, integroitu hallinta, Seveso-laitos
Julkaisija	Teknologian tutkimuskeskus VTT Oy PL 1000, 02044 VTT, puh. 020 722 111, https://www.vtt.fi/

Integrated management of safety and security synergies in Seveso plants

Final report

ISBN 978-951-38-8746-9
ISSN-L 2242-1211
ISSN 2242-122X (Online)
DOI: 10.32040/2242-122X.2021.T386

VTT beyond the obvious