VTT

beyond
the obvious

Guidelines

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

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

VTT TECHNOLOGY 385

VTT TECHNOLOGY 385

Guidelines

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

Jouko Heikkilä, Minna Nissilä, Marja Ylönen, 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 978-951-38-8745-2

VTT Technology 385

ISSN-L 2242-1211
ISSN 2242-122X (Online)
DOI: 10.32040/2242-122X.2021.T385

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

Executive Summary

This document provides guidance on what to consider when designing and implementing integrated safety and security management in Seveso plants. The guidance cover different aspects of management including a) recognition of the context of organisation, b) leadership, c) planning, d) support, e) operation, f) performance evaluation and g) improvement. These aspects are derived from High-Level Structure, which has been 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.

Integrated management refers to connecting, coordinating and combining safety and security management activities in order to exploit synergies and to resolve conflicts between them. Understanding and recognising 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 organisational units or documented integrated system (structures), forms a stabilising framework for the integration of operations, but it does not automatically create an integrated management. Integrated operations are formed by common activities, and interactions are required for integrated management; therefore, the promotion and improvement of the integrated operations are key tasks in integrated management. Integrated management also has an important role in the creation of integrated safety and security culture, which includes a shared understanding about the proper ways to integrate safety and security in operations. Integrated culture extends the effect of integration above the planned and instructed operations.

The effective integration of activities requires motivation. There is both a need for and expected benefits from integration. The need stems from increasing cybersecurity threats concerning the plants involving major chemical hazards, and the management of such threats requires an integrated approach. Increased threat is based on the rapid digitalisation, i.e., use of new digital technologies in chemical plants. The benefits of integration also include convenience, improved safety and security performance, resource optimisation, and increased resilience. It is important that

the management of an organisation 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. A joint risk assessment 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 may be used for reporting safety and security incidents and, moreover, both safety and security implications may be examined when the incidents are analysed. States of emergency and change are critical for both safety and security, and it is important to manage them while taking into account an integration aspect. Safety and security trainings may be combined, which makes it also natural to handle the integration viewpoint. There is plenty of information, which is relevant for both safety and security management. Conflict may arise due to different information management premises of safety and security management. Safety benefits from open information sharing, which is also required to a certain extent. On the other hand, security management controls and limits the availability of information. Integrated information management policy and practices are needed to avoid and overcome conflicts.

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 due to the intertwined and complex nature of present safety and security issues. A new integrative mind-set is required in the future.

Contents

List of Abbreviations

CCPS	Center for Chemical Process Safety
CIA	Confidentiality, Integrity & Availability
CISO	Chief Information Security Officer
DID	Defense in Depth
FAT	Factory Acceptance Test
HAZOP	Hazard and Operability studies
HLS	High Level Structure
HSEQ	Health, Safety, Environment & Quality
IACS	Industrial Automation and Control System
ICS	Industrial Control System
IEC	International Electrotechnical Commission
IMSS	Integrated Management of Safety & Security
ISAQ	Information Sharing and Analysis Centre
ISO	International Standardization Organization
IT	Information Technology
KPI	Key Performance Indicator
OEM	Operational Equipment Manufacturer
OSH	Occupational Safety & Health
OT	Operational Technology
PHR	Process Hazard Risk analysis
PID	Piping and Instrument Diagram
PLC	Program Logic Controllers

SCADA	Supervisory Control and Data Acquisition
SL	Security Level
SIL	Safety Integrity Level
SIS	Safety Instrumented Systems
VPN	Virtual Private Network
WEF	World Economic Forum

1. Introduction

The digitalisation of work and work processes in different industry sectors bring with them new safety and security challenges. Modern factories are constantly investing in automation, allowing factories to operate autonomously, without direct control of operators. Complicated automation and lack of operators present at a plant limit opportunities to find out what actually is happening at the plant. For a long time, chemical plants were not connected to networks, but now, in the interests of simplicity of management, certain installation parts are being connected to the internet (Steijn et al., 2016). As a result, cybersattacks within the safety-critical chemical industry can cause severe safety threats, such as explosions. The probability that a control system belonging to such sectors is attacked - and successfully so - is now higher than ever. These systems are historically not designed with cybersecurity in mind; in fact, it was not the intention to have them connected to the internet. Malicious cyber activities can exploit such unwanted and unforeseen vulnerabilities to damage the integrity of control systems in order to destroy data, shut down plants or to sabotage a firm's operations and, in the worst case, trigger an explosion that would likely harm workers and local residents.

Where chemical plants are concerned, the dangers of cyberattacks on physical infrastructure, including SCADA (Supervisory Control and Data Acquisition) and ICS (Industrial Control Systems), are very real, growing and frightening. One example is an attack on a plant of a Saudi Arabian petrochemical company (Perlroth & Krauss 2018). The attack was deliberately targeting the plant to trigger an explosion. The only thing that prevented an explosion was "a mistake in the attackers' computer code", one which the investigators believe the hackers have "probably fixed by now". It is more important than ever, as these examples show us, that companies handling dangerous chemicals have better knowledge of the security implications for the safe operation of their work processes and functioning of its assets.

The aim of an attacker may be to cause damage for terroristic purposes or for revenge because of experienced mistreatment. On the other hand, the primary aim might not be to cause damage, but to threaten damage purely for financial benefit by blackmailing. Blackmailing for money seems to be an increasingly more potential motivation for a cyberattack, since the knowledge and tools enabling anonymous hacking are easily available for anyone who wants to get "easy money". So far,

blackmailing as a result of cyberattacks has mostly been focused on sensitive information that has been threatened to be exposed to competitors, for example. However, when the sensitive information is better protected, blackmailers may move to use the threat of physical harm. Causing some minor harm to show that the threat is real is a part of the blackmailing concept. If the blackmailers are not real experts of the plant, they may cause more severe harm than they actually aim to. Instead of just stopping the plant, they may cause actual damage, e.g., an explosion.

This publication presents guidelines for the integration of safety and security management in high-risk chemical industries. Integration of management systems is not a new topic. Health, safety, environment and quality management have commonly been integrated as an HSEQ management system. Many chemical plants have committed to the Responsible Care® programme, which combines health, safety, security and environmental topics under the company responsibility theme. They have produced, for example, a specification for a Responsible Care Management System® and Responsible Care Security Code. However, these guidelines aim to provide guidance for a more profound and knowledgeable integration of safety and security management.

Safety and security issues may very much intertwine, especially in chemical and process plants having major accident potential. Such plants are regulated by the so-called Seveso directive (Directive 2012/18/EU). Since any of these so-called Seveso plants have the potential to cause extensive harm to their environment (safety issues), they are also potential targets for intentional attacks (security issues). The main goal of both safety and security management is to prevent unwanted events. Therefore, to a certain extent, integrated management is essential. In addition, safety and security management apply similar means and practices. Integrating and coordinating these practices may make overall safety and security management more effective by improving the impact and saving the resources.

Safety and security issues and management also have a very essential difference in their nature: security deals with intentional attacks towards the plant, while safety deals with accidental incidents. Therefore, certain means and activities of safety and security management are very different, and they will remain as such. In such cases, the integration means connection of different means and activities as an effective overall safety and security management, taking into account both aspects. In some cases, the difference between safety and security causes conflicts in management activities, for example in information sharing and in leadership based on trust and an open atmosphere. The integration of safety and security management should also identify these conflicts and resolve them as effectively as possible.

Reasons why cybersecurity should be considered an important topic, especially on the agenda of safety-critical sectors, e.g., Seveso plants, include:

1. Increase in threat: cyberattacks are increasing every year and they are rapidly becoming more sophisticated and focused on specific purposes.

2. Changes in the sector: innovations, such as internet of things (IoT), artificial intelligence and collaborative robots, may create new cyber risks and vulnerabilities.

The benefits of integration include improvements to security performance and risk management, increased compliance, accountability for cybersecurity issues, the institution's ability to function properly in unsafe environments, increased process efficiency (lower costs), increased confidence and morale among staff and students, improved reputation among the public, legislators and financers, and lastly, increased security awareness. The costs of integration mostly involve time investments.

2. Scope

This document provides guidance on what to consider when designing and implementing integrated safety and security management (IMSS), with a specific focus on key technological, individual or human, and organisational aspects that are necessary to create and maintain optimal safety and security. It is specifically aimed for Seveso plants, but can be applied by any organisation to improve their safety and security management system to enhance major accident prevention. These guidelines are not mandatory and do not negate obligations on license holders pursuant to the Seveso Directive or national legislation, nor any other regulatory obligations and any individual license conditions.

The primary target group for IMSS guidelines comprises Executive Boards and line managers in the area of safety and security. The integration aspects presented here also offer viewpoints for development of legislation and supervision practices where it seems appropriate. Furthermore, IMSS potentially provides a basis for internal and third-party assessments (based on self-audits, peer reviews and external audits).

It is important to emphasise that this document does not provide a complete integrated safety and security management (system) framework, but identifies some of the success factors intended as footholds for chemical companies to enable structured, integrated safety and security management. In this view, the organisations should strive for introducing a suitable management system based on established standards and requirements of legislation, for both cybersecurity and safety in general, and ICS security in particular.

The scope of these guidelines is to support the integration of safety and security management in Seveso plants by highlighting relevant topics and introducing practical solutions. It builds on current practices of safety management and (physical and digital) security management, which currently are typically more or less separate.

The management subjects handled in this guideline document are derived from the ISO High Level Structure (HLS)1 for management systems' standards. The HLS is intended for all future management systems standards to ensure consistency and smooth integration with other management systems. The underlying philosophy of the HLS structure is the existence of a plan-do-check-act cycle at both the operational and strategic levels. HLS includes the following management topics: 1.

[1] HSL was introduced in 2008 for ISO standards in line with further harmonisation purposes of standards, such as ISO 9001 (quality), ISO 14001 (environment), ISO 27001 (information security) and ISO 45001 (occupational safety and health). HSL is introduced in Annex SL and Appendix 2 of the ISO/IEC Directives, Part 1 (Consolidated ISO Supplement – Procedures specific to ISO).

Scope, 2. Normative references, 3. Terms and definitions, 4. Context of the organisation, 5. Leadership, 6. Planning, 7. Support, 8. Operation, 9. Performance evaluation and 10. Improvement. This forms a framework for these guidelines.

The guidelines have three premises:

1. Merged scenarios, in which process disruptions or unsafe situations are the result of cyber disruptions (i.e., through hacking, malware or signal disruptions). These have become increasingly more likely and require integrated risk management.

2. A similar nature of safety and security management as prevention of unwanted incidents and harm have led to the use of similar approaches, tools, means and practicalities in both safety and security management. Integrating these provides the possibility to improve both the impact and resource efficiency of safety and security management

3. A very essential difference between safety and security in their nature is that security deals with intentional attacks towards the plant, while safety deals with accidental incidents. Therefore, 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 is implemented by connecting different means and activities as effective overall safety and security management and resolving conflicts by taking into account both aspects.

Integration includes connecting, coordinating and combining safety and security efforts, looking for synergies and resolving conflicts.

Safety and security issues may very much intertwine, especially in chemical and process plants having major accident potential. Since any of these plants have the potential to cause extensive harm to their environment (safety issues), they are also potential targets for intentional attacks (security issues), thus merging accident and security attack scenarios. Similarities in safety and security management make this merging of scenarios and risk assessment possible and reasonable.

Safety and security management have certain similarities. Security and safety do share the common aim of protecting people, the environment and assets. Safety-critical assets tend to be also security-critical assets (but not necessarily vice versa). Moreover, where security measures are applied for their protection against a range of credible attack scenarios, the same approach is followed in safety cases for assessing and mitigating the risk across a range of major accident scenarios. Similarities form a basis to look for benefits by applying synergies in integration. Having a common approach to security and safety would introduce consistency and, if integrated, would naturally identify and manage conflicts, as well as realising efficiency savings. An integrated management aims to avoid ambiguity and to deliver efficiency savings for those barriers that deliver a combination of safety and security measures.

Safety and security have also profound differences though. Safety is about preventing unwanted events as a result of natural anomalies and disasters, or technical, organisational or human failures. Security is about preventively resisting deliberate disruption. This intentional character determines the distinction between security and safety. It has also led to different approaches taken by safety and security practitioners. Security tends to be more prescriptive than the risk-based practice of safety, and communication around security tends to be on a need-to-know basis, whereas safety emphasises widespread, open communication based on trust and sharing best practices. Integration includes reconciling these differences. Differences between safety and security are presented in Table 1.

Table 1. Overview of different characteristics attached to safety and to security (Reniers et al., 2011)

Safety	Security
The nature of an incident is an inherent risk	The nature of an incident is caused by a human act
Non-intentional	Intentional
No human aggressor	Human aggressor
Quantitative probabilities and frequencies of safety-related risks are available	In the case of less-common security risks (e.g., terrorism), only a qualitative (expert-opinion-based) likelihood of security-related risks may be available
Risks are of rational nature	Threats may be of symbolic nature

These differences have implications to integration. The implications are briefly introduced below, and the rest of this document provides guidelines on how to take these differences – as well as synergies – into account in different management subjects.

Both safety and security management require continuous work, but the nature of this work is different. Continuous safety management is fighting against natural deterioration of human and technical systems and management of changes. Once the hazards have been identified, they are often considered to be relatively stable over time. Security management is fighting against a potential intelligent attacker, who actively searches for vulnerabilities and means to by-pass any newly established protection. The attacker may search vulnerabilities from the target they have especially selected for some reason, or the vulnerable target in general.

Both safety and security management use risk assessment but with certain differences. For security-based events, only qualitative probabilities of occurrence are available. But for safety-related events, quantitative probabilities and frequencies are available through databases for different scenarios. (Villa, Reniers, Paltrinieri & Cozzani, 2017). In a safety assessment, the likelihood of specific technical and - even - human failures can be estimated on quite a reliable basis, and the related risk level can be assessed even quantitatively. Security risk assessment needs to

focus more on the most serious consequences and the most critical vulnerabilities. It monitors changes in all kinds of security threats on a more general level regionally. National and international prevention of terrorist attacks greatly rely on the identification of potential activists and the monitoring of them. The interaction between security risk parameters (Khakzad,et al. 2018) are depicted in Figure 1.

Figure 1. The interaction among the security risk parameters

The same information may be relevant for safety and security management. Information confidentiality is both a specific aim of security and a strong component of its culture. The malicious nature of the risks under consideration, including the fact that threats can have their origins from outsider attacks and insider sabotage, explains this. In safety, transparency and broad access to information are most often sought (Pietre-Cambacedes & Bouissou, 2013). This difference may cause conflicts. Resolving such conflicts is included in the agenda of integration.

3. Normative references

The structure of this document is derived from ISO High-Level Structure for ISO management standards. However, the aim of this document is not to set such structure as norm, but to make it easier for the companies who follow the ISO standards to apply these guidelines.

There are standards concerning several aspects safety and security management available. Appendix A includes a non-comprehensive list of such standards.

Requirements of effective legislation should definitely be followed, and they override any guidance presented in this document in case of conflict. The Seveso directive, and the related national regulation, is especially relevant in this context.

4. Terms and definitions

For the purposes of this document, the following terms and definitions apply:

Escalation factors (CGE): conditions that lead to increased risk by defeating or reducing the effectiveness of barriers.

Hazard is the intrinsic property of a dangerous substance or physical situation, with a potential for creating damage to human health or the environment (Seveso III Directive)

Incident: unwanted event related to either safety or security

Information technology (IT): the technology involving the development, maintenance, and use of computer systems, software, and networks for the processing and distribution of data (Merriam-Webster, 2021)

Integrated Safety & Security Management: connecting, coordinating and combining safety and security management activities in order to exploit synergies and to resolve conflicts.

Integrated Safety & Security Culture: the dimension of organisational culture, which deals with integrated safety and security management.

Leadership is a process of social influence in which a person can enlist the aid and support of others in the accomplishment of a common task (Chemers 1997).

Major accident: an occurrence, such as a major emission, fire, or explosion, resulting from uncontrolled developments in the course of the operation of any establishment covered by the Seveso III Directive, and leading to serious danger to human health or the environment, immediate or delayed, inside or outside the establishment, and involving one or more dangerous substances. (Seveso III Directive)

Management system: a system composed by management activities for an organisation. Management is a set of activities directed at the efficient and effective utilisation of resources in the pursuit of one or more goals (Van Fleet and Peterson, 1994). Safety management is for the pursuit of safety and security management respectively for security.

Operation: an organised activity that involves several people (Oxford Dictionary). In this context, it especially refers to how the activity actually comes true as a distinction with the related plans, instructions or process descriptions. As a management approach, *operation* means putting the plans into practice.

Operational Technology (OT): hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events.

Organisation: in this document, an organisation refers to a Seveso plant consisting of a group of people that has its own functions with responsibilities, authorities and relationships to achieve their objectives.

Policy: a deliberate system of principles to guide decisions and achieve rational outcomes. A policy is a statement of intent and is implemented as a procedure or protocol. Policies can assist in both *subjective* and *objective* decision making. Policies to assist in subjective decision making usually assist senior management with decisions that must be based on the relative merits of a number of factors, and as a result are often hard to test objectively, e.g., work–life balance policy. In contrast, policies to assist in objective decision making are usually operational in nature and can be objectively tested, e.g., password policy. (Wikipedia)

Risk: the effect of uncertainty on objectives (ISO 31000). In the cases of safety and security risks, objectives are to manage safety and security. (The ISO definition of risk is problematic in the sense that it does not distinguish the risk concept from how it is measured. The concept is so tied to the formulation of objectives. However, risk exists despite the formulation of objectives, and risk should be possible to define and describe without referring to objectives. (Aven and Ylönen 2019)). Risk is the possibility of an unfortunate occurrence (SRA Glossary 2018). The SRA Glossary states that the risk concept needs to be distinguished from how it is measured.

Risk assessment: the overall process of risk identification, risk analysis and risk evaluation. *Risk identification* includes description of issues that might help or prevent an organisation in achieving its objectives - in this context, safety- and security-related issues. *A risk analysis* defines the risk level of identified risks. *A risk evaluation* involves comparing the results of the risk analysis with the established risk criteria to determine where additional action is required (ISO 31000). Alternatively, risk assessment is a systematic process to comprehend the nature of risk, express and evaluate risk, with the available knowledge (SRA Glossary 2018). Definitions of the previous terms and their relationships vary in different contexts. Terms in this document are used according to ISO definitions, but they are not in conflict with the definition by the SRA presented above.

Safety: the expectation that a system does not, under defined conditions, lead to a state in which human life, economics or the environment are endangered (CCPS). Safety risks comprise the events, which are unintentional by their nature.

Safety Barrier (Sklet, 2006): physical and/or non-physical means planned to prevent, control or mitigate undesired events or accidents

Process safety: a disciplined framework for managing the integrity of operating systems and processes handling hazardous substances by applying good design principles, engineering and operating practices. (CCPS)

Security: a condition that results from the establishment and maintenance of protective measures that enable an organisation to perform its mission or critical functions despite risks posed by threats to its use of systems. Protective measures may

involve a combination of deterrence, avoidance, prevention, detection, recovery and correction that should form part of the organisation's risk management approach. **(**NIST SP 800-37 Rev. 2). Security threats are intentional by nature.

Cybersecurity: a body of technologies, processes and practices designed to protect networks, devices, programs and data from attack, damage or unauthorised access. Cybersecurity may also be referred to as information technology security (De Groot, 2020).

Information Security: protecting information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction in order to provide— (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity; (B) confidentiality, which means preserving authorised restrictions on access and disclosure, including the means for protecting personal privacy and proprietary information; and (C) availability, which means ensuring timely and reliable access to and use of information (NIST SP 800-66 Rev. 1).

Physical Security: refers to the physical protection afforded to an organisation's functions and resources, including their employees, information, assets and clients in the context of security.

Security breach: when the physical site or the digital system is accessed without authorisation.

Vulnerability: a state of a certain system or installation which increases a threat success probability.

5. Context of the organisation

Guiding principle: "Both external and internal issues that influence the organisation need to be determined. External issues include things such as legal, technological or cultural, and may be international, national or local. The internal includes things like values, culture and knowledge. The interested party needs are to be understood as well as the scope of the management system."

These guidelines focus on plants, where dangerous chemicals may be present (e.g., during processing or storage) in quantities that can cause major accident risk for their environment. Safety management of those plants are regulated by the so-called Seveso Directive (Directive 2012/18/EU). This Directive forms a strict boundary for the management and operation of Seveso plants. The focus of the Seveso directive is on the prevention of accidents; intentional security threats are not included in its scope. However, there is a debate between regulators in different countries and at the EU level on whether intentional major hazards should be included in the regulation under the Seveso Directive. Different EU countries also have different practices on how major accident-related security issues are taken into account in inspections.

In the EU, there is not a similar regulation concerning security management – neither physical, nor cybersecurity. The security-related regulation, which obliges industries, focuses on the protection of employees' or citizens' physical integrity and privacy. These are relevant for safety and security management integration, but they are not the main focus of these guidelines.

There are different standards specifying and guiding security management, such as the ISO 27000 series concerning information security management. Other relevant norms and standards are listed in Appendix A.

5.1 Understanding the organisation and its context

Due to its dangerous chemicals, the Seveso plant always has the potential for major damage. This can be caused both unintentionally and intentionally, and the consequences to human health or the environment can be severe. This makes the plant an attractive target for terrorism or blackmailing. However, the Seveso directive defines the potential hazard only according to the amount and degree of hazardousness of the chemicals at the plant.

In order to take into account the overall risk of intentional incidents, the plant management should identify and assess how the operational surroundings affect the likelihood of such an incident. A wide variety of factors should be taken into account in predicting the likelihood of an attack, including, but not limited to, (i) the general history of threats and attacks to similar targets – locally, regionally, nation-

ally and internationally – (ii) site-specific record of attacks, (iii) capability and potential actions of attackers (threats), (iv) motivation and intent of attackers and (v) attractiveness of the chemical facility in the eyes of attackers (Khakzad, et al. 2018). Factors affecting attractiveness include, for example:

- Size and importance of the company: media visibility and financial standing
- Reputation of the company: who are the “enemies”
- Location near residential area or other potentially vulnerable, important and valuable targets
- Political environment and general safety and security culture
- True and believed strength of protection: attackers look for easier targets
- Common knowledge and awareness of the chemical and its hazardousness: is the chemical itself a subject of common fear, and is it recognised by potential attackers?

The University of Bologna has reviewed 369 security-related incidents recorded in open source databases[2]. **Error! Reference source not found.** presents different attack modes, which have caused 35 realised loss of containment incidents in the chemical and petroleum sector.

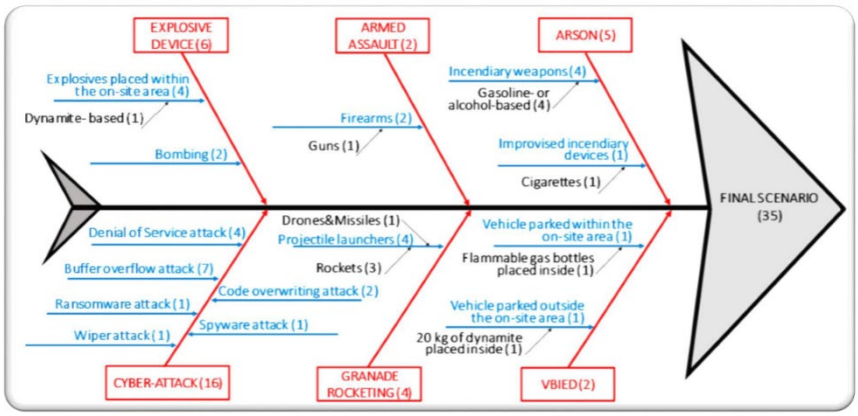

Figure 2. Fishbone diagram showing attack modes which have caused 35 realised final scenarios (loss of containment) (Iaiani & Tugnoli, 2020).

[2] Repository of Industrial Security Incidents (RISI database); Analysis, Research and Information on Accidents (ARIA database); Major Accident Reporting System (eMARS database); E.U. Concawe; Dechema ProcessNet; Infosis ZEMA; E.U. EGIG and the Global Terrorism Database (GTD).

The incidents include 16 cyberattacks with six different attack mechanisms:

- Buffer overflow attacks: an attack aimed at overwriting parts of memory data;
- Denial of Service attack: an attack aimed at making a machine or a network resource unavailable;
- Code overwriting attack: an attack aimed at reprogramming parts of the software code (e.g., attack to program logic controllers - PLCs);
- Ransomware attack: an attack aimed at publishing the data contained in the target machine or perpetually block access to it unless a ransom is paid;
- Wiper attack: an attack aimed at wiping the hard drive of the target machine;
- Spyware attack: an attack aimed at gathering information about a person or organisation.

The reference of these 16 incidents is given in Appendix B. Cyber threats on process facilities are confirmed as an actual risk and credible attack scenario within current publicly available databases. The number of these seem to have significant growth after the year 2000. Process shutdown is a frequent scenario; though only two major events were recorded. Economic losses due to asset damage and/or interruption of productivity is by far the more frequent final outcome suffered by the affected chemical and petrochemical facilities. No injuries and fatalities are reported for cybersecurity-related incidents. The scenarios mentioned here describe actual cases proving a real connection between cybersecurity and process safety. These scenarios require an integrated management approach especially, but an integrated risk assessment should not be limited only within the realised cases.

Industrial Control System (ICS) is a matter of life and death in most modern chemical plants - it is the key to all process operations. They are increasingly exposed to external cyber threats because of the increasing connections outside of the plant. ICS includes safety systems preventing harm in the case of technical failures or human errors. The safety systems need to be overridden if intentional harm is aimed to be caused. Those ICS infrastructures need to be protected against direct and indirect attacks to prevent major accidents.

Industrial Control Systems are often put into use for decades. As a result, many older systems still contain limited or very few cybersecurity measures. At the time they were developed, there was no threat of cyberattacks on these industrial environments. Moreover, given the often-high requirements with regard to stability and continuity of ICS for the production process, it is often difficult, if not impossible, to roll out patches and updates on these systems. Additionally, ICS are increasingly connected to the internet for remote management and monitoring purposes without adequate security measures being implemented in all cases. This fact, together with the major impact that a successful attack can cause, makes ICS in chemical plants an attractive and relatively easy target for cyberattacks. The purpose of cyberattacks ranges from theft of intellectual property to sabotage from state interests or disgruntled employees. The Federal Office for Information Security in Germany, in

cooperation with industry partners, has compiled a list of the top 10 security threats for industrial control systems (BSI 2016). The threats include:

- Social Engineering and Phishing
- Infiltration of Malware via Removable Media and External Hardware
- Malware Infection via Internet and Intranet
- Intrusion via Remote Access
- Human Error and Sabotage
- Control Components Connected to the Internet
- Technical Malfunctions and Force Majeure
- Compromising of Extranet and Cloud Components
- (D)DoS Attacks
- Compromising of Smartphones in the Production Environment.

Starting from a primary attack, an attacker can penetrate further into the systems with subsequent attacks using and creating new vulnerabilities.

5.2 Understanding the needs and expectations of the related parties

It is worthwhile to understand the needs and expectations of relevant parties concerning safety, security and their integration. The relevant parties in the case of a Seveso plant include, at least:

- Societal viewpoint and authorities
- Persons working and visiting a plant
- All (other) involved parties (citizens, municipality, industrial, commercial and non-commercial parties, etc.)

Involved parties include those, who may affect safety or security of the plant, or who may be affected (directly) by the plant – typically neighbouring parties and the parties with whom the plant interacts. If the needs and expectations about integration of safety and security management differ from the implementation of the integration, this may lead to misconceptions or conflicts threatening safety or security. Thus, it is good to take into account the different needs and expectations in integration or, at least, in communication and interaction with these parties.

In Europe, the control of major-accident hazards involving dangerous substances is regulated by the Seveso III directive (Directive 2012/18/EU), related national legislations and supervision by national authorities. This represents societal safety requirements but not requirements against intentional actions related to major accident hazards (at the moment). Obviously, the requirements for safety management can’t be compromised when integrating safety and security management. Even

though the management of an intentional origin of a major accident is not so evidently regulated, it is by no means meaningless for society.

For safety, the EU Machine Directive (Directive 2006/42/EC) requirements should also be applied. This includes specified safety integrity level (SIL) or performance level (PL) as part of the design phase of the plant and factory acceptance test (FAT) by the Operational Equipment Manufacturer or machine builder.

5.3 Scope of integration

The Seveso plant determines the range and applicability of the integration of safety and security management. The following aspects should be considered in doing so:

- The internal and external topics stated in Chapter 5.1;
- The needs stated in Chapter 5.2.

Integration activities focus on the joint handling of safety and security, when it is beneficial or even essential. For example, including both safety and security issues in a combined risk assessment helps to find common, uncontradicted risk management solutions. Joint safety and security training could also help in understanding both viewpoints in relation to each other. This may help to avoid the confusion between trust and suspicion, which are typically linked to safety and security management in different ways. For example, highly educated professionals who are responsible for ensuring safety of very risky activity might sometimes find it difficult to accept tight security control focused on them.

Integration also includes taking into account different requirements of safety and security management. For example, confidentiality or even secrecy is a key approach in handling security sensitive information; whereas, safety nearly always benefits from open information sharing. It should be determined which safety-related information is also security sensitive. In the case of such information, an optimal compromise, which guarantees the security and allows the use of this information for safety purposes, should be developed. This may require, for example, accurate determination and management of the access to the information. However, this must not limit the required use of the information.

It is possible to differentiate various levels of integration. These are **structural integration** (e.g., high-level structure of ISO standards provide a possibility to integrate different safety and security standards in the management systems), **procedural or process-related integration** (e.g., integration of safety and security management procedures, or integration of safety and security in risk assessments) and **cultural**-level integration (requires similar mindset, shared understanding, beliefs and values with regard to safety and security aspects). Cultural-level integrations would be the deepest way to integrate safety and security (Jørgensen et al., 2006). Structural integration is a visible concrete effort. However, it easily remains just putting things together without real connections if integration does not include functional (procedural or process) dimension. Cultural integration extends the integra-

tion in all relevant activities at best. In principle, cultural integration does not necessarily require (formal) structural or procedural/process integration, but they strengthen it. Integration of safety and security cultures are further dealt with in chapter 5.5.

Furthermore, integration can be strategic, by creating common goals in terms of preventing losses, deriving from both safety and security. A systems engineering perspective to integration would emphasise strategic integration and focus on identifying and controlling system vulnerabilities that would contribute to overall system functioning. (Young and Leveson 2014).

The question of integration becomes more complex when moving from a company to multicompany contexts, such as industrial parks.

5.4 Integrated Safety and Security Management System

The Seveso plant may develop, implement, maintain and continuously improve IMSS in line with this guideline. The seven main components of a management system include the following: 1) context of the organisation, 2) leadership, 3) planning, 4) support, 5) operations, 6) performance evaluation and 7) improvement. Integration aspects concerning these main components are presented in this document. If there is any specific reason, the management system may include other main topics or have a different structure.

Integration aims to recognise and, where practicable, take into consideration any synergies between safety and security but also considers potential conflicting requirements, when implementing measures to improve safety and security outcomes.

Integrated Safety and Security Management includes communication between safety and security sectors, building a common understanding and mutual activities handling safety and security topics in an integrated manner. This should be taken into account in all management components.

The integration should be done in a systematic manner. This includes the application of a plan-do-check-act cycle at both the operational and strategic levels. Planning, documenting and ensuring that the system is running is important, but it is just as important to follow up on whether integration works and to carry out corrective actions if it does not. Especially in the beginning of the systematic integration, it is fruitful to have specific integration goals, which will be monitored as other management goals. The integrated safety and security management system needs to be periodically updated based on changes in the state of the art, legislation and regulations and (social) context. The integration aspect is one specific viewpoint in updating. These guidelines aim to help in the systematic approach.

At a strategic level, integration may concern the context analysis, leadership and performance evaluation. The strategic level is facilitated by the proper assignment of responsibilities and authorities within the organisation. At the operational level, this concerns the planning, operations and continuous improvement. The operational level is facilitated by the availability of various resources for support, such as

budget and competences. These levels are connected in the translation of policies developed by leadership into practical actions, taking risks and opportunities into consideration.

An integrated management of safety and security should be understood as a part of the superordinate or integrated management system of a company. However, safety and security are more tightly interconnected with each other than other management aspects, like quality (which is equally connected with everything). Therefore, it is important to solve the integration of these two aspects with each other in addition to the integration of the strategic and operational management of the plant and company. If the organisation has separate certified management systems, integration should be included in them. This means that the effects of any change in one management system to another management system should be examined from the integration viewpoint.

Different approaches towards IMSS can be taken. The EMC² project suggested a concept of interaction between the expert teams from the safety and the security domain as depicted in Figure 3. In this concept, safety and security domains are separate. Combined or integrated approaches are also possible.

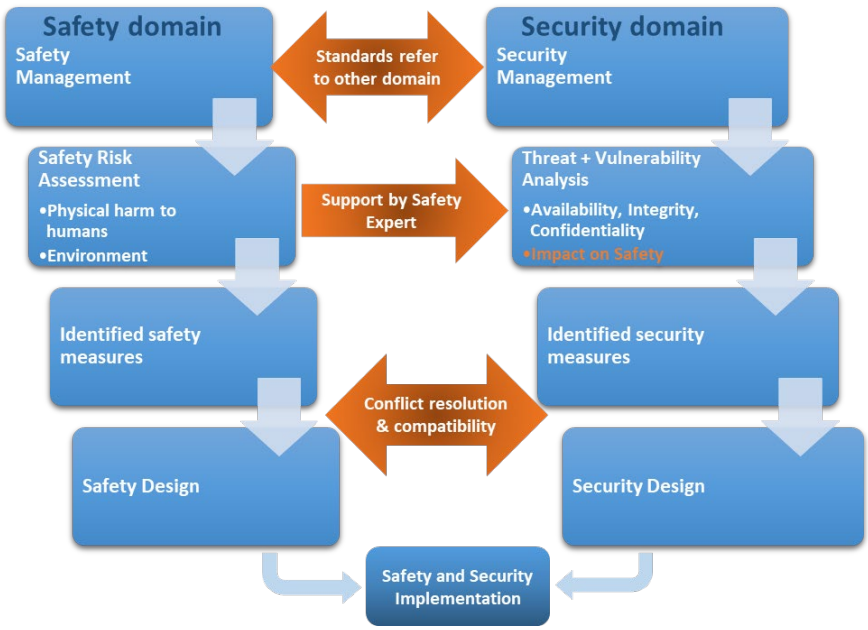

Figure 3. Safety & Security Co-Engineering (EMC2 Project Consortium, 2017)

According to this picture, safety and security teams are expected to do a risk assessment of their own, using existing methodologies within their own domains. Compatibility and conflict identification and resolution activities are carried out further down the risk assessment process with regard to the safety and security

measures defined during individual risk assessments. For both domains this requires taking into account existing legal requirements, requirements from standards that apply to installation and components to ensure safety or security with the correct classification levels are applied for certification purposes (see Appendix A for a non-exhaustive list of relevant standards, best practices and - legislative - references).

The following points represent useful suggestions for integration:

- Create permanent forums where IT experts and process safety, industrial automation and control safety experts can co-create a common understanding of converging risks.
- Ensure that IMSS is a regularly recurring topic of discussion with your chain partners and suppliers. The chain is only as strong as the weakest link. Include cybersecurity levels of processes, products, services and employees in your agreements. Also, make agreements about how to deal with incidents. Regular meetings help keep this topic on the agenda. As a result, awareness and safe behaviour increase.
- Make development decisions based on a preliminary study, a (project) plan and a cost-benefit analysis (or business case). Determine which managers need to be involved in this process, how the management expresses its support and whether any external involvement here is necessary. Make sure you have structurally relevant information so that you can make risk-based assessments. Determine, what do you mainly invest in, and what risks do you accept. Consider the economic interests, the public function, dependences, and the (digital) security and safety.
- Assign the proper authorities and responsibilities to safety and security specialists, including the Chief Information Security Officer (CISO) or a similar position, who has an essential advisory role to the board and is charged with formulating and monitoring the physical and digital information security policy. The CISO should, therefore, operate independently within your organisation and report directly to the Board of Directors.
- Appoint a portfolio holder to the board. The portfolio holder and the CISO define the goals and frameworks, facilitate implementation and monitor the progress and enforcement of the IMSS policy. This ensures that the other directors are not released from their responsibilities.
- Make sure that IT and OT managers act together. They set an example for bringing the domains closer together and a first step in that direction. A first step in forming a team can be initiating joint consultations between the IT and OT team. The initiation of joint consultation between the IT and OT team can be a first step in training the integrated approach to IMSS.
- Create a pool of people who can step in for each other. Make sure that IT and OT knowledge can be applied by several people in this pool.

- Guarantee IMSS as an annual business objective. Management facilitates the sharing of experience and knowledge on this topic with other companies or supply chain partners.
- Use audits to use the possible vulnerabilities as a starting point to bring IMSS to the attention of management.
- Define and monitor your IMSS key performance indicators (KPIs) to sustain adequate IMSS performance.
- Seek out operational information (good and bad news) critical for effective IMSS.
- Recognise the potential for perverse incentives in the IMSS.

5.5 Safety and security cultures

An organisation's culture defines the proper way to behave within the organisation. This culture consists of established shared beliefs and values and is reinforced by leaders or emerges by repeated practices. Culture ultimately shapes employee perceptions, behaviours and understanding. Organisational culture sets the context for everything an enterprise does. Organisational culture describes common understanding and affects the behaviour of the personnel, but does not completely determine it. Safety culture represents safety related aspects of organisational culture, and security culture represents security related aspects of organisational culture. Both of them have multiple definitions of their own.

Safety and security cultures in an organisation may determine the attitude towards the other - for example, that the other is less important. If so, the integration requires additional effort to overcome this problem. Safety and security management in general also have their own cultures or traditions, which are maintained by education and collaboration with experts of the same domain. These cultures have certain differences, which have been introduced above.

There are different understandings of organisational cultures. The anthropological understanding of organisational culture emphasises the emerging nature of culture and the difficulty to steer it, whilst the instrumental understanding of culture stresses that the culture can be steered. Organisations can, for instance, structure their activities, allocate resources and affect processes in ways that are beneficial to safety or security directly, and, in addition, promote a shared understanding and values.

If safety and security cultures are disturbing each other, every effort should be made to overcome this. Such efforts also induce changes in cultures. The following actions, for example, have been suggested (Huang & Pearlson 2019):

1. Identify the values, attitudes and beliefs you want to cultivate to drive cyber-secure behaviours
2. Put someone in charge of building the cyber-security culture

3. Use marketing campaigns to clearly communicate the corporate values and beliefs you want cultivated in your organisation. Make it fun and engaging.
4. Educate the staff (increase awareness and self-efficacy), while not only focusing on compliance.
5. Engage/challenge the whole organisation to find ways to become more cyber secure.
6. Create your roadmap to increase maturity.

Interface between safety and security – especially cybersecurity – in the chemical sector has several historically grown challenges:

- Cultural differences;
- Traditional organisational separation;
- Lack of integration in design process;
- Lack of adequate coordination during facility operation; and
- Inadequate, non-existing regulatory guidance.

In the nuclear industry, the same challenge has been faced earlier. However, IAEA (2010) decided that safety culture and security culture should not be merged into one and should not oppose each other, but reinforce one another. They recognised that specific attributes in some areas related to nuclear safety and nuclear security may lead to conflicts in the implementation of the relevant activities, as is the case with ICS in the chemical industry. This conflict should be managed by proper coordination of the methods and approaches, and operating practices through the research reactor lifetime.

The list below is based on the IAEA (2010) document on how to address the challenges of the interfaces between security and safety culture:

- Expectations
- Use of authority
- Decision making
- Management oversight (periodic audits)
- Involvement of staff
- Effective communication
- Improving performance
- Motivation (and attitudes).

5.5.1 Maturity approach

One approach to examine safety or security culture is to determine the maturity level. The model based on five levels is commonly used for safety culture. The levels

represent subsequently improving safety (management). The idea of different maturity levels is basically the same in different references, even though the levels have different titles:

- Level 1: Emerging, Basic, Unmindful, Pathological
- Level 2: Managing, Reactive, Transitional
- Level 3: Involving, Planned, Calculative, Systemic
- Level 4: Cooperating, Proactive
- Level 5: Continually improving, Resilient, Generative, Leading, Progressive

The level of commitment (of an organisation and individuals) increases from “no-one cares” via “experts or management takes care” to “everyone cares”. Planning, proactivity and continuous improvement increase step by step from the basic reactive level in these models.

The similar models have been introduced for information security, too. After analysing eight different information security maturity models, Karokola et al. (2011a) suggested the following five-step model (other titles from the analysed models are in brackets):

- Level 1: Undefined (Policies, Blind trusting, Blissful ignorance, Responding to basics, Initial, Complacency, Functional)
- Level 2: Defined (Procedures, Repeatable, Awareness, Building protections, Basic, Acknowledgement, Technical)
- Level 3: Managed (Implementation, Defined, Corrective, Security programme, Capable, Integration, Operational)
- Level 4: Controlled (Testing, Managed, Operations excellence, Maintaining security, Efficiency, Common practice)
- Level 5: Optimised (Integrating, Maintenance, Optimising, Continuous improvement, Strategic)

There are certain similarities within these safety and security models, but also a significant difference. The safety culture maturity models do not suggest that organisations should target different levels depending on their safety risk level; they suggest that the higher level is better for every organisation. The security maturity model that Karokola et al. (2011a and 2011b) suggests binds the maturity levels with the security targets and security risk environment of the organisation: the lower the security targets, the lower the maturity level. Different levels introduce increasing requirements for security management measures and increasing embeddedness of security into the organisational culture.

Despite this apparent difference, it is clear that high maturity of safety culture is more important for a high-safety-risk organisation like a Seveso plant. The higher safety risk level should also require higher security maturity, especially focusing on attacks aiming to exploit the high hazardousness of the plant to cause or threaten major damage.

Several approaches can be used to assess the current level of maturity regarding safety and security culture and the various underlying factors. However, normally, safety or security culture assessment does not examine relationships to the other domain. Therefore, an integrated assessment method would be useful.

6. Leadership

Guiding Principle "Top management needs to demonstrate leadership, through polices and by ensuring that the right responsibilities and authorities are communicated and understood. They also have to promote discipline across the organisation"

Leadership is a process of social influence in which a person can enlist the aid and support of others in the accomplishment of a common task (Chemers 1997). The management of an organisation has the natural status and responsibility to lead employees according to the organisation's values and goals. When an organisation's intention is to establish integrated safety and security management, this should show up in leadership performed by the management.

Leadership includes direct statements about an organisation's will (like policy) and goal setting and performance indicators, as well as indirect indications related to management actions, like resource allocation, task and authority assignments, decisions and other exemplary personal behaviour. Management actions naturally also have a direct effect on enabling and directing action towards and according to the desired goal. Leadership also includes the constructive handling of critiques towards a goal or the means planned to gain the goals. Leadership is building organisational culture - building a common understanding about what is important within the organisation.

The leadership role of management also extends to involving stakeholders outside the organisation: customers, suppliers, partners, authorities, the public etc. Power to influence external stakeholders is normally weaker than inside the organisation. However, it is important to take the external stakeholders into account, since they may either disturb or support management in leading the organisation.

To facilitate the integration of safety and security management, top management takes responsibility to lead employees towards such an objective. In doing this, they should also take into account the indirect effects the management actions have on employee viewpoints. Management encourages and supports collaboration between cross-discipline domain experts (technical and social / behavioural; safety and security). They should also demonstrate the importance by committing their own time to promote collaboration and trust-building across the organisation. In order to get subordinates to respect integration efforts, it is important that management understands and can communicate the need and the benefits gained by the integration of safety and security management.

A required change in mind-set, because of a changing risk landscape, should be within the scope of leadership. Risk landscapes are changing due to increasing digitalisation and use of AI tools in the high-risk industries, leading to the interconnectedness of IT and industrial automation and control systems. This interconnectedness makes ICS, which have been historically closed systems, susceptible to cyber-

security interferences. Changing risk landscapes means the convergence of process-safety, physical security and cyber-security risks, which may lead to major accidents. This change calls for a change in people's mindsets, and this is a key subject driving the integration of safety and security management. Leadership should support this change of mindset.

6.1 Leadership and commitment

People choose to act if they are committed; vice versa, if people do not act, they are not committed. Employees cannot read the management's minds, but they can read their behaviour. Management should visibly indicate their own commitment to IMSS by including the topic in management activities and communicating it openly within the organisation. For example, both safety and security, including an integration aspect, could be included in the agenda of board meetings. Formulating, implementing and enforcing the IMSS policy is an evident indication of commitment. Employees may also commit to integration without management's example if they see it as feasible, but an example helps. Demonstration of commitment is not a one-off action but a process requiring continuous attention. Leaders should be seen as models for safe and secure behaviours equally and taking care of the integration aspect.

Contradictions between safety and security management may lead to poor commitment in either of these, in specific situations or in general. Therefore, identifying and solving such conflicts are essential. Conflicts may be related to practices, like in situations where a person cannot follow both the safety and security rules and has to choose one or the other, or compromise. On the other hand, recognition and the aim to solve such conflicts can be a strong motivator for employees to commit to integration.

Conflicts may be related to:

- *Transparency of information*: safety management prefers open information sharing and security management tends to limit information sharing. If the same information is relevant for safety, but also security sensitive, a conflict arises. A conflict may be concrete, e.g., leak of security-sensitive information. It may also be related to trust and mistrust: if people have no access to information, they feel that they are not trusted. The limitations for access to security-sensitive information are certainly needed. Transparency is needed to clarify who has access and who does not, and why. The limitations for access should be carefully considered - placing limitations "just in case", without an actual reason, will deteriorate confidence in the system.

- *Trust and mistrust*: security checks indicate mistrust towards competent professionals who have heavy responsibilities in taking care of the safe operation of safety-critical systems. From the security management point of view, these are the people who especially should be checked since they have the most power to do harm. From a safety point of view, they are the people who need to be the most trusted and should be the most respected. This conflict may be resolved if these professionals could be convinced about their status

as role models for the security topics, too. Different views on trust and transparency may also cause conflicts in cooperation between safety and security professionals. In such cases, management can take the leadership role to promote cooperation by moderating different viewpoints, building mutual understanding and expressing equal respect.

- *Blamelessness*: There is a long tradition in blaming and punishing people about both their unintentional errors as well as intentional offences. Safety management has struggled to build the blameless culture for decades in order to ensure all errors are reported. The same could apply for security management, even though security issues always involve intentionality somehow. Similarly, there can also be the intentional breaking of safety rules. Essentially, the conflict arises between blaming and punishing those who have intentionally made an offence and not blaming those who have unintentionally made an error. This is the same for safety and security, but in security management, the culture of blaming is still more common. There security management could learn from safety management.
- *Awareness and appreciation*: people find safety issues, which may eventually hurt themselves, closer than security issues that mainly would hurt the company. In cases where security threats focus directly on people, the emphasis is turned around, like in the work of security guards. The same stands for process safety and occupational safety, where occupational safety may get more emphasis on the floor level and process safety on management level. The unbalance between safety and security appreciations may lead to a limited awareness of either one: poor management decisions if safety and security investments are competing, and in the case of conflicting safety and security rules. The inherent difference between the appreciation of safety and security management may mean that either of them would require more leadership in order to obtain a balanced state. Balanced appreciation is a necessity for the integrated management of safety and security. The balance should show up in different management aspects, like job ratings, attention and support for different domains. Showing the link between safety and security and building integrated management itself supports this.

Common to safety and security management is a certain cautiousness, need of continuous attention and questioning of current solutions and personal and others' assumptions and practices in the name of safety and security. It should be made clear that these are not expressions of mistrust against employees or management, either personally or professionally. Any honest action should be acknowledged, and the management should set an example. This is a challenging task of management.

Generally speaking, safety and security experts and managers of different domains communicate with each other at different degrees. Health, Safety, Environment and Quality Management (HSEQ) are commonly combined in a joint management system. However, the IT department, which usually is responsible for cyber-

security, is quite often separate even from the industrial control system management. Thus, integrating cybersecurity and process safety management may require additional attention and leadership by the management, in addition to practical arrangements for systematic communication and collaboration, in order to prevent cyber-based process safety issues. Management should credibly state the need and benefits of collaboration. Management may also encourage and make it possible for people to learn and work in other domains.

6.2 Integrated safety and security policy

Principles to guide decisions are included in a policy**.** It is a statement of intent, and is implemented as a procedure or protocol. When the management defines integration policy, they should remember that integration is not a goal as such, but the goal is a more effective safety and security management by means of optimal integration. It should also be ensured that the policy is in line with the organisation's objectives. Management is responsible for defining the policy, but it is advisable to listen to employees when it is defined. The policy should be available as an officially approved document, and the management should communicate the integrated policy to employees and other stakeholders as appropriate, and make it available to the public.

The framework for the integration policy and a systematic step towards integration is the combination of separate safety and security policies. The policy, which includes principles of safety and security management and takes into account the specific needs of each, can be called as an integrated safety and security policy.

As an example, the Responsible Care policy for chemical companies has been specified to include the following topics (American Chemistry Council, 2013):

1.1 Senior management shall develop, document and implement a policy for the organisation that recognises Responsible Care, and shall communicate it to employees and other stakeholders as appropriate, and make it available to the public.

1.2 The policy shall be relevant to the nature, scale and impact of the organisation’s operations, products and processes.

1.3 The policy shall set a framework for establishing and reviewing Responsible Care goals, objectives and targets and shall include a commitment to continual improvement.

1.4 The policy shall include a commitment to comply with legal and Responsible Care-related requirements to which the organisation is subject or subscribes.

1.5 The policy shall promote openness with stakeholders.

1.6 The policy shall reflect a commitment to the Responsible Care Guiding Principles.

1.7 The policy shall be supported by a demonstration of visible leadership, commitment and involvement from senior management and other levels of the organisation with respect to Responsible Care

The Responsible Care programme gathers safety, security and other responsibility topics under a common “umbrella”. However, this policy does not include the integration aspect which would be key content in an integrated policy

The integration aspects in the policy include, at least

- Taking into account both safety and security viewpoints in all management activities, looking for synergies, conflicts and the need to keep them separate (that is, all topics included in these guidelines)
- Treating safety and security equally
- Identifying, analysing and preventing incident scenarios, which combine safety and security threats.

6.3 Organisational roles, responsibilities and authorities

Management ensures that the responsibilities and authority are assigned to the relevant roles and are communicated across the organisation. The integration aspect should be clearly present in determination of roles, responsibilities and authorities in the organisation. The most important are as follows:

- The integration aspect is included in each relevant role
- People know that integration is their responsibility, and they know how to take integration into account in their work, and
- People know and trust that they have the authority to work for integration.

One specific responsibility for all members of an organisation should be to identify and report deviations from integration and conflicts between safety and security, as well as to propose improvements. There should be a system to handle this in the organisation - including the related different roles and responsibilities.

Safety and security specialists - including information security managers and specialists – play a key role in integration: if they do not recognise their role and responsibility on integration, integration cannot be realised.

In addition, there may be the need for the specific role(s) of an “integrator”, who looks after how the integration proceeds. For example, an integration portfolio holder may be appointed to the board. The portfolio holder, together with safety and security specialists, prepare the goals and frameworks, facilitate implementation and monitor the progress and enforcement of the IMSS policy. Although, this will not release the other directors from their responsibilities, and in the end, the board should make the decisions.

There may also be the use for an integration specialist who is not actually (in a role of) a safety or security specialist, but understands both aspects and helps to

find integrated solutions in practice. The ability to cooperate with a safety and security specialist and to mediate different viewpoints is important in this role.

Communication is an important part in getting roles and responsibilities recognised. Communication structures between relevant parties should be clearly defined and actively used. The management should clearly communicate the determined roles, responsibilities and authority - integration as a part of other duties. They should also listen to the possible employee criticism, since this may reveal conflicts between safety and security management.

7. Planning

Guiding Principle "A risk-based approach is required to address threats and opportunities, and to ensure the management system can prevent or reduce undesired affects. Objectives and plans are to be developed and cascaded through the organisation, including responsibilities and time frames."

The risk-based approach should extend through all company planning and management, and safety and security management play key roles in it. The risk-based approach in planning should be based on the realisation that the safety and security incidents and activities are related. The aim of the integration of safety and security management is to improve the overall risk management. That means more effective prevention of undesired events from both safety and security viewpoints. In some cases, people think that the means of prevention make their work more difficult. In such cases, integration is also an opportunity to make the prevention more fluent and even to support the work.

This Planning chapter includes three sections: 7.1 Actions to address risks and opportunities, 7.2 Integration objectives and planning to achieve them and 7.3 Planning of changes. The first section handles integration aspects in different risk-management activities. The second section handles planning for implementation and promotion of integration. The third section handles the integration aspects in management of change.

7.1 Actions to address risks and opportunities

Risk assessment and risk treatment are the natural meeting points of safety and security. This includes:

- Incident scenarios connecting security and safety issues: typically, the intentional causing of an accident, but also weakening of security protection because of an accident.
- Safety and security measures influencing each other. The influence may be both positive and negative. The former means that the measure serves both the safety and security purpose or they strengthen each other. The latter means that the measures disturb each other.

The consequences of a security breach can have direct implications on the effectivity of single or several Information Technology – Operational Technology (IT-OT) barriers at once. A single cyberattack can also cause diverse risk propagation and damaging the IT-OT system further down on different timescales (directly or dormant - the latter requiring more activities to cause any damage). Therefore, the protection objectives and plans should transcend that of individual incidents, IT-OT components and interfaces.

The relationships between incidents also need to be identified and taken into account during the risk assessment. A cyberattack on one of the actors in the supply chain of a chemical cluster can have direct consequences for the other parties in the chain and for the chain as a whole due to the strong interdependence. In a chemical cluster, there may also be chain effects resulting from a chain scenario due to the interconnectedness or interdependence between different companies (Nunen, Reniers and Swuste, 2019). A chain scenario is cluster-specific and can occur when nearby companies use the same facilities. This may concern utilities (such as electricity, steam, water, gases) but also, for example, joint import or export of raw materials and products. In addition, it may also be the case that a company depends on the processes of other nearby companies for its functioning (in other words, they make use of each other's product flows). In the event of a successful cyberattack on one of the actors in the chain, this can have direct consequences for the other parties in the chain and for the chain as a whole.

Risk assessment and its integration depend on the plant and its context (topics in chapter 5.1) and the needs and expectations of the related parties (topics in Chapter 5.2).

The risk assessment consists of the following: 1) Risk Identification, 2) Risk Analysis and 3) Risk Evaluation. The three phases of Risk assessment are followed by risk treatment, which includes 1) Selection of treatment options and 2) Preparing and implementing risk treatment plans. (ISO 31000)

It is beneficial to carry out many risk-assessment actions jointly with both safety and security domains. This enables the utilisation of common interests and solving possible conflicts effectively. Joint actions also promote mutual learning and awareness of risks, which improves resilience as such.

In addition to the standard risk assessment approach, resilience engineering (Hollnagel et al., 2011; Young and Leveson, 2014) may provide framework for integration. The elements of resilience engineering are preparing, anticipating, monitoring, responding and learning.

Digitisation means that more and more machines are connected to each other and to the internet. The IEC 62443 Cyber Security for Industrial Automation and Control Systems series of standards provides guidance on how machine safety can also be ensured by providing detailed technical control system component requirements (Security Levels, SL), concepts and models. The Security Levels are as follows:

- *Security Level 0*: No special requirement or protection required.
- *Security Level 1*: Protection against unintentional or accidental misuse.
- *Security Level 2*: Protection against intentional misuse by simple means with few resources, general skills and low motivation.
- *Security Level 3*: Protection against intentional misuse by sophisticated means with moderate resources, IACS-specific knowledge and moderate motivation.

- *Security Level 4*: Protection against intentional misuse using sophisticated means with extensive resources, IACS-specific knowledge and high motivation.

Risk assessment defines the target level for a system, which should be achieved by an automation solution.

The Confidentiality, Integrity & Availability (CIA or AIC) model of Information Security is designed to guide policies for information security within an organisation. The elements of the triad are considered the three most crucial components of security. In this context, confidentiality is a set of rules that limits access to information, integrity is the assurance that the information is trustworthy and accurate, and availability is a guarantee of reliable access to the information by authorised people. (Samonas & Coss 2014) The same three elements may be applied for safety purposes, too.

Sharing information about incidents within and outside of the organisation is a common action to support safety risk management. However, public information about cyber-security-related incidents is scarce. There are good reasons to not publicise them, mainly as not to expose the weakness of the protection in general and the weak spots in the system especially. The same stands for the detailed results of a risk assessment which includes information about the vulnerabilities of the system that can be exploited by actors with harmful intentions.

There are national Information Sharing and Analysis Centres (ISAQs), which share anonymous information about security incidents as well as best practices within trusted communities. In addition, there is a public initiative to identify industrial security incidents that affect control systems. It is called the Repository of Industrial Security Incidents (RISI database).

7.1.1 Risk Identification

The purpose of risk identification is to recognise and describe issues that might help or prevent an organisation achieving its objectives - in this context, safety- and security-related issues (ISO 31000).

Integration in risk identification means the recognition and description of incident scenarios where safety and security issues influence each other. This may happen when a) an accident scenario is caused or affected by intentional actions aiming to cause harm b) security is endangered by an (unintentional) accident.

Accident scenarios consisting of the failures leading to unwanted consequences are identified in a safety analysis. The different (unintentional) causes of failure are also identified. Integrated risk identification would complement these scenarios from the starting point that every failure could also be caused intentionally. The objective of complementing the accident scenarios is to describe how it would be possible to cause failures intentionally. For example, the six different cyber-attack mechanisms known to be used in the chemical and petroleum sector include:

- Buffer overflow attacks: an attack aimed at overwriting parts of memory data;

- Denial of Service attack: an attack aimed at making a machine or a network resource unavailable;
- Code overwriting attack: an attack aimed at reprogramming parts of the software code (e.g., attack to program logic controllers - PLCs);
- Ransomware attack: an attack aimed at publishing the data contained in the target machine or perpetually block access to it unless a ransom is paid;
- Wiper attack: an attack aimed at wiping the hard drive of the target machine;
- Spyware attack: an attack aimed at gathering information about a person or organisation.

Visualisation of the overall network architecture, including devices in use and ICS components, based on complete and correct (up-to-date) documentation, helps in the examination.

Outdated operating systems may also cause a specific risk with limited or very few cybersecurity measures, and older ICS components that are increasingly connected to the internet for remote management and monitoring purposes, but are not designed for it. For example, be aware of vulnerability in the process operating systems due to built-in capabilities in (e.g., remote assistance and maintenance) software- or hardware-enabling digital espionage or sabotage.

The security analysis produces scenarios related to security threats. These may be complemented by identifying how different accidents (scenarios) may affect security, for example, different means of protection. In addition to accidental technical failures, it should be noted that a major accident could easily cause a disordered situation in which security management is also threatened.

In addition, connections of different risk scenarios should be identified, including:

- Overlapping nodes
- Dependencies (within the company and as a result of interdependencies with other companies in the chemical cluster you are in)
- Technical dependencies of safety and security barriers.

The consequences of cyberattacks may be as follow (BSI, 2016):

- Loss of availability of the ICS / loss of production
- Data leakage / loss of know-how (intellectual property)
- Physical damage to facilities
- Triggering of safety procedures or interfering with safety systems
- Deterioration of product quality
- Reputational damage

This list is similar to the potential consequences of accidental failures. All of these may also have consequences on safety. Losses, damages, and product quality issues may have evident direct potential safety consequences. In addition, interfering

with safety systems may, for example, cause false alarms, which induce false, possibly harmful, reactions. Data leakage may enable, and reputation damage may attract sabotage or terrorism.

In order to carry out risk identification, for example, a physical security expert and a cybersecurity expert could be included in the hazard and operability study (Hazop) team and to provide those security-related risk assessments that could be integrated into the same Hazop. Similarly, other methods, such as Process Hazard Analysis (PHA), Failure Modes, Effects and Criticality Analysis (FMECA), Fault Tree Analysis (FTA), Bow tie, What If- analysis, etc. can be used in integrated assessments of safety and security risks.

In principle, normal safety risk assessment processes, such as hazard and operability studies (HAZOP) and process hazard risk analysis (PHR), are not sufficient to address cybersecurity threats to automation and control systems since they do not, in general, consider multiple contingencies (i.e., several dangerous events occurring at once) or take into account malicious intents that are typical of a cyberattack.

There are several examples combining safety and security risk assessments (Chockalingam et al., 2017; Kavallieratos et al., 2020; Langner, 2013). HAZOP could be adequately applied for IMSS purposes since it is already carried out by a suitably experienced multi-disciplinary team during a series of meetings. The HAZOP technique is qualitative and aims to stimulate the imagination of participants to identify potential hazards and operability problems. Security scenarios can be brought in by security experts to complement the HAZOP analyses. Examples about security applications of PHA (Marszal & McGlone, 2019) and HAZOP (Wei et al., 2016) are available.

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

Different descriptions and documentation are normally used for risk identification. For example, Piping and Instrumentation Diagram (PID) is used in HAZOP and layout drawings are used in other studies. Similarly, system network architecture drawings may be used for cyber-security risk identification (see, for example, HSE OG 0086). For the identification of physical risks integrating security and safety, for example, the layout information is important. For the identification of risks integrating cyber-security and safety, information about connections between information systems, control systems and process equipment and their operation is important.

It is important that the documents used for risk identification are up to date, and even more important is to know if they are not. Therefore, it is necessary that the risk identification team includes those who know the current state of the plant. It

should not be expected that people always follow the rules, neither security, nor safety rules.

HSE has published guidelines in an Operational Guidance (OG 0086) for Inspection Cyber Security for Industrial Automation and Control Systems on major accidents in the workplaces. Self-assessment checklists to address the major cyber-attack avenues for protecting ICS are also available. These aid in identifying the most-common potential threat scenarios and known countermeasures.

7.1.2 Risk Analysis

Risk analysis involves a detailed consideration of uncertainties, risk sources, consequences, likelihood, events, scenarios, controls and their effectiveness (ISO 31000). Risk analysis defines the risk level of different scenarios considering different factors affecting the risk level and the certainty of the risk-level estimation. The level or numeric value of risk is commonly determined as a function of likelihood and extent of consequences - typically a product, if calculated. The risk level is usually presented in the risk matrix with the likelihood and consequence dimensions. Uncertainty related to the risk-level assessment increases the risk level.

The assessment of the severity of potential consequences is similar for both safety and security incident scenarios: in the end, it will end up with the evaluation of human, material or immaterial losses, including environmental harm. In this phase, the potential extent of the harm is evaluated (lost lives, amount of lost materials and production, etc.) and the value of the harm will be assessed in the risk-evaluation phase.

The assessment of likelihood concerning safety- and security-related causes are different. The likelihood of an accidental failure is assessed by the reliability of components or operation with a specific solution in the specific use and specific operating environment. In many cases, this can be fairly reliably done. The likelihood of intentionally caused failures could be assessed on the basis of vulnerability and protection against external or internal intentional attempts at damage.

A reasonable assessment of likelihood requires information about occurred failures. In the case of rare events, such information does not exist. Therefore, the likelihood of many security-related issues cannot be reliably assessed. It is reasonable only in regions and cases where certain intentional security violations are recurring. The limitation of rare events applies also to certain safety-related cases, for example, when newly developed technology is used.

Assessments of likelihood and severity may be done with (more or less) absolute scale, indicating the true likelihood and extent of consequences. Alternatively, the risk may also be assessed with a relational scale, comparing the likelihood and severity of different scenarios with each other.

7.1.3 Risk Evaluation

Risk evaluation involves comparing the results of the risk analysis with the established risk criteria to determine where additional action is required (ISO 31000). Risk evaluation determines acceptability of the risk related to each risk scenario, taking into account existing and planned means to mitigate the risk. It includes a decision on what risk level is acceptable in general and in each individual case. The purpose of risk evaluation is to identify the risks that still require additional mitigation actions.

Risk assessments done in the risk analysis phase always include more or less uncertainty. Assessments that have been done on the same basis can be compared with each other in the risk evaluation phase, but assessments that have a different basis cannot be compared as such. A different basis can mean significantly different uncertainty of assessments (i.e., different information basis) or a different basis of likelihood assessment (e.g., reliability vs. vulnerability, as presented above). Therefore, in most cases, security and safety risk assessments should not be compared with each other in the risk evaluation phase. Instead, it should focus on searching for the weakest points of either to be improved. The greater uncertainty in the risk assessment also means greater risk, which should be taken into account in the risk evaluation. For example, if two scenarios have the same risk level assessments, but the assessment of the other is (significantly) more uncertain, the risk is also actually higher.

A specific method to support the safety risk evaluation is a Layer of Protection Analysis (LOPA), which evaluates the risk of each identified scenario. The purpose of a LOPA is to determine whether there are sufficient layers of protection, or independent layers of protection (IPLs), to protect against an accident scenario. The number of IPLs required depends on the complexity and potential severity of the consequence(s) of an accident scenario. The LOPA gives a clear picture of the weaknesses and strengths of the Safety Instrumented Systems. Since the layers of protection approach is also used for security risk management, it could be fruitful to integrate these safety and security activities.

Criticality of the component or operation is a criterion, which is common to the safety and security in integrated scenarios. Criticality defines how big of a role the component or operation would have in the development of unwanted consequences. Most critical components cause catastrophic consequences immediately and inevitably if they fail. In integrated risk scenarios, critical parts are critical from both safety and security viewpoints, and thus also require equal attention from both viewpoints.

Certain safety related features that rely on instrumentation are called safety instrumented systems (SIS), and the following design standards give a systematic approach that is internationally recognised as a best practice:

- IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems. This standard is focused towards manufacturers and suppliers of devices.

- IEC 61511: Functional safety – Safety instrumented systems for the process industry sector. This standard is focused towards system designers, integrators and end users.

Both standards give guidance on how to achieve suitable reliability for these safety instrumented systems (risk graph method, layer of protection, etc.). The required reliability is called the safety integrity level (SIL) (which is numbered 1 to 4) and such systems are usually considered to be safety critical.

A high SIL rating means a more demanding safety function, requiring more sophistication in the equipment (for example, SIL 4 is usually used in the nuclear industry) and would require duplication/redundancy/diversity in the instrumentation so that no single component could cause the overall system to fail. In the control system security management (IEC 62443), required security levels are determined similarly (see **Error! Reference source not found.**). Connection of these two activities could be beneficial.

7.1.4 Risk Treatment

The purpose of risk treatment is to select and implement options for addressing risk. Risk treatment involves an iterative process of a) formulating and selecting risk treatment options, b) planning and implementing risk treatment, c) assessing the effectiveness of that treatment, d) deciding whether the remaining risk is acceptable, e) if not acceptable, taking further treatment. In general, the options are: avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk; taking or increasing the risk; removing the risk source; changing the likelihood; changing the consequences; sharing the risk; or retaining the risk by informed decision. (ISO 31000)

Integration in risk treatment means: 1) selection or development of options that would treat both safety and security risks and 2) selection or development of options that are not in conflict with each other. Therefore, it would be best if the risk treatment selections and planning could be carried out jointly with both safety and security domains – including cybersecurity. At least, all domains should be aware and able to comment on the plans of other domains. Cooperation should be fluent, since quick and targeted interventions are required as much as possible for cybersecurity due to the dynamic character of security threats.

In safety risk treatment, the options that completely eliminate the risk are the first priority. This means, for example, replacing hazardous chemicals or processes with safe ones. This also eliminates security threats related to these hazards. Risk treatment options, which decrease the (inherent) hazardousness of chemicals and processes, also have a similar integrated effect.

Procedural controls – that is, rules, warnings and guidance – are generally the least preferable risk-treatment options, since they are less reliable: people make errors or break rules more often than appropriate technology fails. The same stands for both safety and security rules. However, people have an excellent ability to identify and control both failures as well as malpractices if they are motivated to do so.

It may be difficult to motivate all people to look after each other at the workplace, but in the name of safety, it might be easier than in the name of security.

A multi-layered defence, in-depth strategy with redundancies in protective barriers at all levels is typically used for IT systems. Defence in Depth is an approach to cybersecurity, in which a series of defensive mechanisms are layered in order to protect valuable data and information. If one mechanism fails, another mechanism steps up immediately to counter an attack. This multi-layered approach with intentional redundancies increases the security of a system as a whole and addresses many different attack vectors. This can be applied to all levels of IT systems. It could be examined how such security defences could also serve safety and, on the other hand, if they are in conflict with safety.

At the level of implementing countermeasures, there is a lot of coherence with the safety measures taken. Both security and safety have a preventive effect. For example, various access control measures are primarily designed to prevent unintentional human actions, such as keeping unqualified personnel away from enclosed spaces. Another example is a compartmentalisation plan designed to keep a fire local.

There may also be seemingly conflicting objectives between the different plans. From a security perspective, it is often the intention to make it more difficult for unauthorized persons to escape; while, from a company emergency assistance perspective, open escape routes are of great importance. In the elaboration of the measures, both objectives should be taken into account and must be met. The security process also includes intervention activities to stop unauthorised actions and unauthorised persons. Most of these activities can be included in the preventive column of the safety chain, because this prevents the offender from achieving the undesired effect (i.e., loss of containment).

7.2 Objectives of Integrated management and planning to achieve them

Integration of safety and security management is not a target as such. The actual target is improved safety and security management. Targets for improvements because of integration activities should be set as well as targets for fulfilment of the related activities. There should not be integration targets which cannot be justified with improvements in safety or security.

Ensuring the achievement of integration targets is a leadership task. It should be determined if some additional activities; knowledge, learning or resources would be needed to ensure planned integration. The following general guidance should be followed.

The organisation will determine the IMSS targets for the relevant levels and roles. IMSS targets must adhere to the following:

- Be consistent with IMSS policy;
- Be measurable (if workable);

- Take the applicable requirements into account;
- Be monitored;
- Be carried out;
- Updated when necessary.

The organisation will document information relating to IMSS targets.

When planning how to achieve IMSS targets, the organisation will determine the following:

- What must be done;
- What resources are needed;
- Who is responsible for carrying out the activities;
- When the activities must be completed;
- How the results should be assessed.

7.3 Planning of changes

Changes taking place at a plant increase the uncertainty for a certain amount of time. This uncertainty increases the vulnerability to both safety and security issues. An increase of vulnerability is the same for both physical and organisational changes, even though the potential issues are different.

When integrating safety and security management, it should be especially considered how integrated safety and security management should be arranged in different possible states of change. This would form a basis for a specific integrated risk management, which should be included in the planning and management of all changes. It should be noted that the integration is a significant change as such, too.

Since many changes happen gradually at the plant, it is necessary to update risk assessments periodically – with the integrated process. Changes in operating environment may appear, maintenance may use changed replacement components or software updates, and operation practices will change gradually if not controlled.

8. Support

Guiding Principle *"Resources need to be provided to support the management system, including providing competent people, appropriately maintained infrastructure and environment. Document control and records management have been replaced with documented information, where the organisation determines what documentation is necessary and the most appropriate medium for that documentation."*

Specific integration activities require additional resources and competence. However, established integrated management should require fewer resources or would gain better results with the same resources and improved competence, compared to separate safety and security management.

Integration efforts require an investment in time and budget, above existing resources for their independent management. In addition, existing policies, and communication thereof, need to be clarified concerning relevant cross references and overlaps. Employees need to know how they can contribute and understand the importance of their contribution. Therefore, they need to understand relevant policy documents and feel no restrictions to act accordingly. However, since even the separate management systems and instructions require updating, all resources needed for integration cannot be counted as additional.

8.1 Resources

Additional time allocated for the personnel, money for different expenses and even hiring new personnel is required during the integration process. Additional resources are needed for preparing and learning new integrated practices and tools. Integration process also requires additional leadership.

8.2 Competence

Management and safety and security experts need to have the ability to resolve conflicts between safety and security aspects. They should be ready to learn about the other topic when necessary and to find solutions, which are satisfactory from both viewpoints. Crossing disciplinary boundaries might require support from senior managers, which would require that managers sufficiently understand both topics and promote multidisciplinary collaboration.

Safety and security management and experts should learn to communicate about their subject in a way that non-experts find it easy to understand. Mutual understanding between safety and security domains is essential, and all management should be able to understand the safety and security basis of their decisions.

All management should learn to answer the questions concerning the integration according to their role in the organisation.

All personnel should learn the new integrated practices and understand why they have been implemented (e.g., common goal, similar means, solving conflicts). They should also learn the remaining separate safety and security practices and understand why they remain separate (e.g., different nature of threats and different requirement for transparency of information). The basis for this is that personnel understand different aspects of safety and security, for example occupational and process safety and physical and cybersecurity.

There might be the use for specific integration expert support, who, for example, search for the best integration practices or external expertise when required.

It should be ensured that in any integrated activities (e.g., risk assessment), there should be competent representation of all safety and security domains, including cybersecurity.

Senior managers, and those who take care of procurements regarding IT systems, would need to have a broad understanding regarding the convergence of risks. As there are increasing interests in obtaining real-time data from the industrial processes, also for the use of the organisation's business, it would also be important to increase the knowledge regarding the risks and vulnerabilities.

8.3 Awareness

Employees who perform activities under the authority or instructions of the company need to be aware of the following:

- Company's integrated safety and security policy, which includes also guiding principles for integration
- The contribution they are expected to make towards the effectiveness of IMSS, including the benefits arising from improving the performance of IMSS.
- The consequences of non-compliance with the IMSS requirements.

The specific subjects that everyone should especially be aware of related to integration are as follows:

- The odds of a cyberattack causing or threatening with a major incident related to hazardous chemicals are increasing and should be taken seriously.
- Both safety and security aspects should be taken into account in all activities in an integrated manner in order to utilise possible synergies and to solve possible conflicts.
- Continuous collaboration between safety, security and cybersecurity domains is required to establish integrated management, but also to build mutual trust and understanding.

- Vulnerability to both safety and security incidents especially increases at states of change and emergency situations requiring additional situational awareness concerning safety and security. A threat is that when you need to focus on safety you forget security, and vice versa.

8.4 Communication

Communication is an essential part of both the integration process and integrated activities. In order to make it happen, official channels and occasions need to be established. Especially strategic and operational management and risk management activities require taking both safety and security formally on agenda, and open and understandable communication.

Security aspects may require a limit on communication about certain content and within certain groups. Such limitations should be carefully and understandably justified and all personnel should be made aware of these reasons. In general, the openness of communication is for good. Management may promote this by setting a good example and by requesting it regularly.

It should be noticed that communication is a two-way process, which includes both sharing and receiving information. In addition, understanding those who are being communicated with, improves the chance of successful communication. This is particularly important in integration and integrated activities.

The company must determine the need for internal and external communication which is relevant to IMSS, including the following:

- The information to be communicated (e.g., relevant IMSS documentation, policy)
- When the information should be communicated;
- To whom the information should be communicated;
- Weaknesses and strengths of different communication methods;
- Enhancing communication to enable interdisciplinary cooperation and teamwork.

8.5 Documented information

The management of safety and security requires sufficient documentation and multiple documents. When a document of either domain is changed, it should be checked to see whether the changes affect documents of the other domain.

9. Operation

Guiding Principle "Processes for operations, along with appropriate acceptance criteria is required along with contingency plans for non-conformances, incidents and emergency preparedness. Change management and control of external providers (such as contractors, outsourced processes, procurement etc.) is needed."

Operation primarily means putting the plans into practice. Management and leadership are required for this. In general, this means organising, leading, and controlling. There should be plans for different foreseeable situations: normal operation, changes and incidents. Both the internal operations and external providers of the plant are included. In addition to general plans, sufficient planning of each operation is needed before starting it. Even the standard processes should be checked. Controlling includes identification and resolving possible conflicts between safety and security in operations.

Situational awareness is important during operation, especially for safety and security. It should be rapidly recognised, when exceptional action is required. For example, specific check lists and simple rules may be used in different operations to identify hazards and ensure safety and security (in addition to relevant technical measures).

It is impossible to prepare detailed plans for each exceptional situation. In such situations, a good understanding of both safety and security aspects, and their connections, is essential. Since neither safety nor security are often an intrinsic target of operation (instead, the product and effectiveness are), strong compatible safety and security cultures are needed to guide operations, in addition to instructions and rules during both normal and exceptional operations. Collaboration between safety and security domains should not be neglected; this is especially important to remember in exceptional situations.

In the following, practical aspects, regarding securing production processes against a cyberattack, are presented:

- Many of the ICS systems are now connected to the internet, despite the fact that they are not initially designed for this purpose, with few obstacles preventing unauthorised access. Network segmentation can prevent this link. That means the process operating system is on a separate network without an internet connection, and without such a connection being present (e.g., to occasionally connect the process operating system to the internet to download or send something). A more legitimate reason for this may be to remedy faults remotely, enable remote management or simply monitor the process. If you choose that, the virtual private network (VPN) connection must be used, and it must be extremely secure.

- It is important to keep the ICS systems that contain (potential) vulnerabilities up to date. It may happen that companies perform updates of the required

patches, but only when the production is stopped due to a maintenance shutdown. This means that the system is vulnerable during the period from the release of a critical update to the installation of it in the stop of the production process. Planned production shutdowns may occur only a few times a year. Some minor stops may occur more frequently. This means that during these three months between stops, a system may not be eligible for an update. It is important to realise that, during this period, the systems are vulnerable. In exceptional cases, an update will only be carried out if there is no other option, only if it is necessary for the production process. This leaves a system vulnerable indefinitely. It goes without saying that such a situation is extremely undesirable and should be avoided.

- Operators may have access to the ICS from home via a VPN connection and perform the same actions as from the plant control room. Through this connection, they are able to control processes at the factory from home, such as opening or closing valves, or making changes to the process system. A VPN connection is often believed to be secure, but when the VPN connection is set up from an infected computer, the infection could spread and propagate through the IT network. If a company has a constant connection between process automation and office automation, and a hacker succeeds in entering office automation, it may be possible to take over the process control system as well. Not all systems make it possible to immediately perform different kinds of actions in the system from a computer. Many systems require physical actions, such as opening a valve physically. Cooperation between an operator behind a computer and an operator in the field is often necessary. When it is possible to perform actions only from the computer, a mechanical protection can be built into the system, such as a physical limitation or an alarm system that indicates, for example, that there is too much pressure in the system building up. It is often the case that the process control system can only be accessed when the relevant ports become manually opened up. This is only done on instructions from the shift supervisor or installation manager on duty. This is a time when the system is vulnerable and could theoretically be the target of an intrusion. The intruder then runs into other security measures in the system and, therefore, cannot simply take control of the system. These physical and mechanical limitations build a certain degree of security in the system. As a result, it is not simply possible to let a tank storage overflow, for example explode or execute other wild scenarios on a chemical installation. However, systems can indeed be seriously damaged by such sabotage attacks.

10. Performance evaluation

Guiding Principle "Evaluation, data analysis, and monitoring and measurement, including the Evaluation of Compliance (Legal and other), is required. Internal Audits and Management Reviews are to be conducted."

Performance monitoring and evaluation is important for both the motivation and to find needs for improvement. Typically, performance is evaluated with predefined indicators or measures against targets. Evaluation includes continuous monitoring and measurement, periodic management reviews, and internal and external audits. Deviation reporting and improvement proposals are part of continuous monitoring

When incident and deviation reporting and improvement proposals are established in the origination, it is essential to handle the reports and proposals efficiently and transparently, learn from them, and implement improvements. This requires an adequate management system, tools and resources.

Once it has been decided to establish integrated safety and security management, both the performance of the integration process and the integrated operations should be included in both the continuous monitoring and periodical evaluations.

The integration process includes different tasks and their fulfilments is a natural evaluation object (integrated risk assessments, revised instructions, integrated trainings, communications, etc.). Resolved conflicts and other improvements are other tasks.

The expected impacts of integration include improved safety, security and savings because of exploitation of synergies and solving deficiencies. The number and severity of occurred safety and security incidents is a typical measure for safety and security, but the use of such measure is problematic in many ways. A better proactive measure is, for example, the realisation of different means to ensure safety and security (e.g., safe and secure behaviours and the upkeep of technical measures). Safety and security cultures, including their interlinking, may be assessed periodically. Used resources is still another measure, but it should be always compared to effort and results.

11. Improvement

Guiding Principle "Organisations are required to address non-conformities and incidents, and take action to control, correct, deal with consequences, and eliminate the cause. The organisation has to improve the suitability, adequacy and effectiveness of the management system."

The aim of integration is to improve safety and security management as such. Improvements are necessary to fix the deficiencies in the system, improve the performance and to adapt changes in operating environments. Assessment of the need for improvements is based on performance evaluation (see Chapter 9 above). Improvement is the final phase of the 'Plan-Do-Check-Act' management cycle, complementing management as a continuous improvement cycle. When improvement in safety and security management is considered and planned, its connections should be taken into account as presented in this document. Improvements for resolving the conflicts between safety and security and taking advantage of synergies are the primary focus when considering integration.

Acknowledgements

This document has been produced in the research project: Integrated Management of Safety and Security Synergies in the Seveso Plants. The project has been accepted for funding by SAF€RA, which is a partnership between 16 research funding organizations from 12 European countries who collaborate on research programming and launch joint calls in the field of industrial safety. The project was funded by Finnish Safety and Chemicals Agency (Tukes), Finnish Work Environment Fund, and the National Institute for Insurance against Accidents at Work (INAIL) from Italy together with research partners. Tukes participated actively also in execution of the project. The project was coordinated by VTT Technical Research Centre of Finland, who carried out it together with research partners: University of Bologna, University of Roma Campus Biomedico (Italy), and the Netherlands Organization for Applied Scientific Research TNO.

References

Aven, T. and Ylönen, M. 2019. The strong power of standards in the safety and risk fields: A threat to proper developments of these fields? Reliability Engineering and System Safety, vol. 189, 279-286. https://doi.org/10.1016/j.ress.2019.04.035

American Chemistry Council (2013) Responsible Care Management System® Technical Specification. Document Number: RC101.04

BSI (2016) Industrial Control System Security - Top 10 Threats and Countermeasures. BSI Publications on Cyber-Security, BSI-CS 005E | Version 1.20 https://www.gi-de.com/corporate/user_upload/MS/Industries/Manufacturing_and_IIOT/SIV_Solutions/BSI-CS_005E.pdf

Chemers, M. (1997). An integrative theory of leadership. Lawrence Erlbaum Associates, Publishers. ISBN 978-0-8058-2679-1.

Chockalingam, S., Hadžiosmanovi´c, D. H., Pieters, W., Teixeira, A., & Van Gelder, P. (2017). Integrated Safety and Security Risk Assessment Methods: A Survey of Key Characteristics and Applications. arXiv:1707.02140

De Groot, J. (2020) What is Cyber Security? Definition, Best Practices & More. https://digitalguardian.com/blog/what-cyber-security

de Ruijter, A., & Guldenmund, F. (2016). The bowtie method: A review. Safety science, 88, 211-218.

Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast)

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

EMC² Project Consortium (2017). Embedded multi-core systems for mixed criticality applications in dynamic and changeable real-time environments ARTEMIS Call 2013, project 621429 EMC², D13.26 Final Standardization Report and Outlook. https://www.artemis-emc2.eu/fileadmin/user_upload/Publications/Deliverables/EMC2_D13.7_Final_Report_PartA_Publishable_Summary_v1.1.pdf

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

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

HSE OG86. Cyber Security for Industrial Automation and Control Systems (IACS). HSE Operational Guidance https://www.hse.gov.uk/foi/internalops/og/og-0086.pdf

Huang, K. and Pearlson, K. (2019) For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture. Working Paper CISL# 2019-02. Cybersecurity Interdisciplinary Systems Laboratory (CISL) Sloan School of Management, Room E62-422.

IAEA (2010). INSAG-24 The Interface Between Safety and Security at Nuclear Power Plants. A report by the international nuclear safety group.

Iaiani. M. & Tugnoli, A. (2020). Main references of the Cyber Attack events to Chemical & Petroleum sector recorded in the UniBo Database. Updated 05/08/2020

ISO 31000:2018, Risk management — Guidelines

Jørgensen, T. H., Remmen, A., & Mellado, M. D. (2006). Integrated management systems - Three different levels of integration. Journal of Cleaner Production, 14(8), 713–722. https://doi.org/10.1016/j.jclepro.2005.04.005

Karokola, G., Kowalski, S. and Yngström, L. (2011a) Towards An Information Security Maturity Model for Secure e-Government Services: A Stakeholders View.HAISA, 58-73. https://www.diva-portal.org/smash/get/diva2:469623/FULLTEXT02.pdf

Karokola, G., Kowalski, S. and Yngström, L. (2011b) "Secure e-government services: Towards a framework for integrating it security services into e-government maturity models," 2011 Information Security for South Africa, Johannesburg, 2011, pp. 1-9, https://doi.org/10.1109/ISSA.2011.6027525.

Kavallieratos, G.; Katsikas, S.; Gkioulos, V. (2020) Cybersecurity and Safety Co-Engineering of Cyberphysical Systems—A Comprehensive Survey. Future Internet 12, no. 4: 65. https://doi.org/10.3390/fi12040065.

Khakzad, N., Martinez, I.S., Kwon, H., Stewart, C., Perera, R., & Reniers, G. (2018). Security risk assessment and management in chemical plants: Challenges and new trends. Process Safety Progress, Vol.37, No.2

Langner, R. (2013). The RIPE Framework. A Process-Driven Approach towards Effective and Sustainable Industrial Control System Security. Langner Communications Whitepaper. https://www.langner.com/wp-content/uploads/2017/04/The-RIPE-Framework.pdf

Marszal, E. M. and McGlone, J. (2019) Security PHA Review for Consequence-Based Cybersecurity. International Society of Automation, 168 pages ISBN: 978-1-64331-000-8

Merriam-Webster, (2021) Information technology. https://www.merriam-webster.com/dictionary/information%20technology

NIST SP 800-37 Rev. 2. (2018) Risk Management Framework for Information Systems and Organizations. A System Life Cycle Approach for Security a nd Privacy NIST Special Publication 800-37 Revision 2. 2018 https://doi.org/10.6028/NIST.SP.800-37r2

NIST SP 800-66 Rev. 1 (2008) An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. Information security. NIST Special Publication 800-66 Revision 1

Nunen, K., Reniers, G. and Swuste, P. (2019). Verkennende studie naar (petro)chemische clusters en veiligheid: Veiligheidsparameters binnen (petro)chemische clusters en losstaande (petro)chemische bedrijven. Report for the Ministry of Infrastructure & Watermanagement.

Perlroth, N. & Krauss, C. (2018) A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try. New York Times. March 15, 2018. https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html

Pereira D., Hirata C., Pagliares R., Nadjm-Tehrani S. (2017) Towards Combined Safety and Security Constraints Analysis. In: Tonetta S., Schoitsch E., Bitsch F. (eds) Computer Safety, Reliability, and Security. SAFECOMP 2017. Lecture Notes in Computer Science, vol 10489. Springer, Cham. https://doi.org/10.1007/978-3-319-66284-8_7

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

Reniers, G. L., Cremer, K., & Buytaert, J. (2011). Continuously and simultaneously optimizing an organization's safety and security culture and climate: the Improvement Diamond for Excellence Achievement and Leadership in Safety & Security (IDEAL S&S) model. Journal of cleaner production, 19(11), 1239-1249.

Sabaliauskaite, G.; Liew, L.S.; Cui, J. (2018) Integrating autonomous vehicle safety and security analysis using stpamethod and the six-step model.Int. J. Adv. Secur. 2018,11, 160–169.

Schmittner C., Ma Z., Puschner P. (2016) Limitation and Improvement of STPA-Sec for Safety and Security Co-analysis. In: Skavhaug A., Guiochet J., Schoitsch E., Bitsch F. (eds) Computer Safety, Reliability, and Security. SAFECOMP 2016. Lecture Notes in Computer Science, vol 9923. Springer, Cham. https://doi.org/10.1007/978-3-319-45480-1_16

Sklet, S. (2006). Safety barriers: Definition, classification, and performance. Journal of loss prevention in the process industries, 19(5), 494-506.

Samonas, S. and Coss, D. (2014), The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security. Journal of Information System Security, Volume 10, Number 3 (2014) Pages 21–45. ISSN 1551-0123

SRA (2018) Glossary Society for Risk Analysis, www.sra.org/resources. Accessed February 5, 2019.

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.

Van Fleet, D. D., & Peterson, T. O. (1994). Contemporary management. Boston: Houghton Mifflin.

Villa, V., Reniers, G.L.L., Paltrinieri, N. and Cozzani, V. (2017) Development of an Economic Model for Counter Terrorism Measures in the Process-Industry. Journal of Loss Prevention in the Process Industry Industries 49:437-460.

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

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, pp. 31-35.

Appendix A: Bibliography

Below is a non-exhaustive list of relevant standards, best practices and (legislative) references that are related to the subject addressed in this document:

Legislation

Seveso-III-Directive (see EU 2012/18/EU)

NIS Directive (see EU 2016/1148)

Machine Directive EU 2006/42/EC incl. Guide to application of the Machinery Directive 2006/42/EC - Edition 2.2

Norms and standards

ISO/IEC

ISO 17776:2016 Petroleum and natural gas industries — Offshore production installations — Major accident hazard management during the design of new installations

ISO/IEC 27001: 2013 Information technology – Security techniques – Information security management systems - Requirements

ISO/IEC 27002:2013 — Information technology — Security techniques — Code of practice for information security controls

ISO/IEC 27005:2018 Information technology - Security techniques - Information security risk management

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

ISO 28000:2007 Specification for security management systems for the supply chain

ISO 31000:2009 Risk Management — Principles and guidelines

IEC 61508-1/7: Functional safety of electrical/electronic/programmable electronic safety related systems

IEC 61511: Functional safety – Safety instrumented systems for the process industry sector

IEC 61513: 2011 Nuclear power plants. Instrumentation and control important to safety. General requirements for systems

IEC 62443-4-1:2018 Security for Industrial Automation and Control Systems

IEC 62859:2016 Nuclear power plants - Instrumentation and control systems - Requirements for coordinating safety and cybersecurity

BS EN / IEC 62443: Security for Industrial Automation and Control Systems

ISA

ISA-TR84.00.09-2017, Cybersecurity Related to the Functional Safety Lifecycle

ISA99/IEC62443 Industrial Automation and Control Systems Security
(ISA99 WG7 TG1 Recommendations to align safety and security for industrial automation control systems, 30 January 2015)

Other

OSHA 29 CFR 1910.119 Process safety management of highly hazardous chemicals

Unmanned air gas plants: design and operation. Document: 132/15. European Industrial Gases Association (EIGA)

Best practices

American Chemistry Council (ACC) 2016 Guidance for Addressing Cyber Security in the Chemical Industry https://chemitc.americanchemistry.com/RCSC-NIST-Framework-Guidance-Jan-2016.pdf

ARIA July 2016 Cybersecurity in industry https://www.aria.developpement-durable.gouv.fr/wp-content/uploads/2017/08/2017_08_18_Note_cyberterrorisme_JFM_vfinale_EN.pdf

ARPANSA (2017). Regulatory guide: Holistic safety. Regulatory services, REG-COM-SUP-240U v1.1 https://www.arpansa.gov.au/sites/default/files/reg-com-sup-240u.pdf

BSI (2019). Industrial Control System Security - Top 10 Threats and Countermeasures. BSI-CS 005E | Version 1.30 of 06/06/2019 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_005E.pdf?__blob=publicationFile&v=7%20

Cefic Security Code https://cefic.org/app/uploads/2019/01/ResponsibleCare_SecurityCode.pdf

Center for Chemical Process Safety (CCPS) - Guidelines for Integrating Management Systems and Metrics to Improve Process Safety Performance. ISBN: 978-1-118-79510-1 February 2016 https://aiche.onlinelibrary.wiley.com/doi/abs/10.1002/prs.11720

Centre for Cyber Security Belgium - Cyber Security Incident Management Guide. https://www.cybersecuritycoalition.be/content/uploads/cybersecurity-incident-management-guide-EN.pdf

CSR (2019). Handreiking cybersecurity voor de bestuurder (Cybersecurity guide for the executive board). https://www.cybersecurityraad.nl/binaries/Handreiking_Bestuurders_NED_DEF_2019_tcm107-316868.pdf

Engineering Equipment and Materials Users Association (EEMUA) 2015 Cyber security assessment process for industrial control systems - Industry Information Sheet 2 https://www.eemua.org/EEMUAPortalSite/media/EEMUA-Flyers/EEMUA-Industry-Information-Sheet-2.pdf

ENISA (2018). Cybersecurity culture guidelines: behavioral aspects of cybersecurity. https://doi.org/10.2824/324042

ENISA - Cyber Insurance: Recent Advances, Good Practices and Challenges. November 2016. https://www.enisa.europa.eu/publications/cyber-insurance-recent-advances-good-practices-and-challenges

GCCS 2015 Cyber Security of Industrial Control Systems. Eric Luiijf and Bert Jan te Paske. March 2015 https://www.thehaguesecuritydelta.com/media/com_hsd/report/39/document/Cyber-Security-of-Industrial-Control-Systems-GCCS2015.pdf

Holstein, D.K., Hammond, V.B., Weiss, J., Mishra, A., Ginter, A., Abercrombie, R.K., Newton, C., Deibert, D., Johnson, D., Crawford, E.D., Cosman, E.R.,

Persson, E., Greitzer, F.L., Thomas, H., Hamad, I.A., Bouhdada, J., Langill, J.T., Day, J., Medoff, M., MacLeod, P., Landes, R., Singh, S., Miller, W., Loebl, A.J., & Cusimano, J.S. (2015). Recommendations to align safety and security for industrial automation control systems ISA 99 WG 7 TG 1.

HSE OG0086 Cyber Security for Industrial Automation and Control Systems (IACS) https://www.hse.gov.uk/foi/internalops/og/og-0086.pdf

IEC TR 63069:2019 Industrial-process measurement, control and automation - Framework for functional safety and security

MITRE Cyber Resiliency Engineering Framework. Deborah J. Bodeau & Richard Graubart, September 2011. MITRE TECHNICAL REPORT MTR110237.

Nationaal Cyber Security Centrum (NCSC). Zicht op risico's van legacysystemen - Een self-assessmentmethode om de risico's van (vitale) legacysystemen in kaart te brengen. Versie 1 november 2015.

Nationaal Cyber Security Centrum (NCSC). Checklist beveiliging van ICS/SCADA-systemen - Tref organisatorische én technische maatregelen. Factsheet FS-2012-02, versie 1.2 | 22 december 2015.

Nationaal Cyber Security Centrum (NCSC). Uw ICS/SCADA- en gebouwbeheer-systemen online - Zorg voor een actueel overzicht en tref maatregelen. Factsheet FS-2012-01, versie 2.2 | 6 juni 2016.

NIST SP 800-30 Guide for Conducting Risk Assessments – Information security https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

NIST march 2018. Systems Security Engineering Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems. Draft NIST Special Publication 800-160 VOLUME 2. https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/archive/2019-09-04

NSAC - Universal Security Management Systems (USMS) Standard 2017 - Standard for Managing Security with Requirements and Guidance for Use. https://www.lulu.com/shop/marcel-spit/universal-security-management-systems-standard-2016/paperback/product-23049821.html

Organization for Security and Co-operation in Europe (OSCE) 5 March 2013 Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection from Terrorist. https://www.osce.org/atu/103500

Repository of Industrial Security Incidents (RISI). https://www.risidata.com/About

Safe and Open Higher Education (last accessed: 21-07-2020). *Manual: Integrated safety and security management system high education (MISH)*. https://integraalveilig-ho.nl/wp-content/uploads/Manual-MISH-Safe-and-Open.pdf

U.S. Department of Energy (DoE) Attacks Focusing on Threats Emanating from Cyberspace - 21 Steps to Improve Cyber Security for SCADA Systems https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf

Van den Berg, J., van Zoggel, J., Snels, M., van Leeuwen, M., Boekee, S., Koppen, L., van den Berg, B., de Bos, A. & van der Lubbe, J.C.A. (2015). On (the emergence of) cyber security science and its challeges for cyber security education. Proceedings of the NATO IST-122 Cyber Security Science and Engineering Symposium, Tallinn, Estonia, October 13-14 2014.

John Bumgarner en Scott Borg. De U.S. Cyber Consequences Unit (US-CCU) Checklist voor cybersecurity. Vertaald door het Nationaal Adviescentrum Vitale Infrastructuur. © 2006-2007 U.S. Cyber Consequences Unit.

Appendix B: Main references to cyberattack events chemical sector

BUFFER OVERFLOW ATTACK

https://www.risidata.com/Database/Search_Results/search&keywords=Welchia+Worm+Infects+Automation+Network/

https://www.risidata.com/Database/Search_Results/search&keywords=Blaster+Worm+Infects+Chemical+Plant/

https://www.risidata.com/Database/Search_Results/search&keywords=Infected+New+HMI+Infects+Chemical+Plant+DCS/

https://www.risidata.com/Database/Search_Results/search&keywords=Sasser+Worm+Causes+Loss+of+View+in+Chemicals+Plant/

https://www.risidata.com/Database/Search_Results/search&keywords=Nachi+Worm+on+Advanced+Process+Control+Servers/

https://www.risidata.com/Database/Search_Results/search&keywords=Blaster+Infects+Onshore+Oil+Production+Control+System/

https://www.risidata.com/Database/Search_Results/search&keywords=Sasser+Worm+Infection+in+Process+Control+System./

RANSOMWARE ATTACK

https://www.chemistryworld.com/news/hexion-momentive-and-norsk-hydro-all-hit-by-ransomware-cyberattacks/3010328.article

WIPER ATTACK

https://www.cybersecurity360.it/nuove-minacce/saipem-attacco-di-cyber-sabotaggio-contro-leinfrastrutture-critiche-che-ce-da-sapere/

DENIAL OF SERVICE ATTACK – DoS

https://www.risidata.com/Database/Search_Results/search&keywords=Control+System+Infected+with+SQLslammer+Worm/

https://www.risidata.com/Database/Search_Results/search&keywords=SQL+Slammer+Impacts+Drill+Site/

https://www.risidata.com/Database/Search_Results/search&keywords=Slammer+Impacts+Offshore+Platforms/

https://www.risidata.com/Database/Search_Results/search&keywords=Slammer+Infected+Laptop+Shuts+Down+DCS/

SPYWARE ATTACK

https://techerati.com/news-hub/bayer-cyber-attack-malware-china/

CODE OVERWRITING ATTACK

https://futurism.com/saudi-arabia-cyberattack

https://www.risidata.com/Database/Search_Results/search&keywords=Malware+Targets+Uranium+Enrichment+Facility/ & https://en.wikipedia.org/wiki/Stuxnet

Series title and number

VTT Technology 385

Title	**Guidelines** Integrated Management of Safety and Security Synergies in Seveso plants (SAF€RA 4STER)
Author(s)	J Heikkilä, M Nissilä, M Ylönen, A Tugnoli, M Iaiani, V Cozzani, G Oliva, R Setola, G Assenza, D van der Beek, W Steijn, H Young, M Roelofs
Abstract	The digitalisation trend in the process-industries bring with new safety and security challenges. Modern plants are constantly investing in automation, allowing plant to operate autonomously, to different degrees. For a long time, chemical plants were not connected to networks, and thus they were not designed with cybersecurity in mind. However, now the connections to information networks outside the plant are more and more common. As a result, cyberattacks launched against the safety-critical chemical industries can cause severe safety threats, in the worst case, trigger an explosion. The probability that computer networks and information systems belonging to such sectors is attacked - and successfully so - is now higher than ever. This document provides guidance on what to consider when designing and implementing integrated safety and security management in Seveso plants. The guidance cover different aspects of management including a) recognition of the context of organisation, b) leadership, c) planning, d) support, e) operation, f) performance evaluation and g) improvement. Integrated management refers to connecting, coordinating and combining safety and security management activities in order to exploit synergies and to resolve conflicts between them. Understanding and recognising 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. The integration of activities requires motivation. The need is based on increasing cybersecurity threats concerning the plants involving major chemical hazards. The benefits of integration include convenience, improved safety and security performance, resource optimisation, and increased resilience. 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. Safety and security are intertwined domains, 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 due to the intertwined and complex nature of present safety and security issues. A new integrative mind-set is required in the future.
ISBN, ISSN, URN	ISBN 978-951-38-8745-2 ISSN-L 2242-1211 ISSN 2242-122X (Online) DOI: 10.32040/2242-122X.2021.T385
Date	April 2021
Language	English, Finnish abstract
Pages	54 p. + app. 13 p.
Name of the project	
Commissioned by	
Keywords	
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 385

Nimeke	**Guidelines** Integrated Management of Safety and Security Synergies in Seveso plants (SAF€RA 4STER)
Tekijä(t)	J Heikkilä, M Nissilä, M Ylönen, A Tugnoli, M Iaiani, V Cozzani, G Oliva, R Setola, G Assenza, D van der Beek, W Steijn, H Young, M Roelofs
Tiivistelmä	Digitalisaation lisääntyminen prosessiteollisuudessa tuo mukanaan uusia turvallisuusuhkia. Nykyaikaiset laitokset investoivat jatkuvasti automaatioon, jolloin laitos voi toimia itsenäisesti ilman operaattoreiden läsnäoloa. Aiemmin kemiantehtaita ei oltu kytketty verkkoihin, joten niiden suunnittelussa ei myöskään ole otettu huomioon kyberturvallisuutta. Nyt yhteydet laitoksen ulkopuolisiin tietoverkkoihin ovat kuitenkin yhä yleisempiä. Tämän seurauksena kyberhyökkäykset turvallisuuden kannalta kriittiseen kemianteollisuuden laitokseen voivat aiheuttaa vakavia turvallisuusuhkia, ja pahimmassa tapauksessa johtaa esimerkiksi räjähdykseen. Todennäköisyys, että vaarallisia kemikaaleja käsitteleviä laitoksia vastaan hyökätään onnistuneesti, on nyt suurempi kuin koskaan. Tämä opasjulkaisu antaa ohjeita siitä, mitä on hyvä ottaa huomioon suunniteltaessa ja toteutettaessa integroitua turvallisuuden hallintaa Seveso-laitoksilla. Opas kattaa seuraavat johtamisen eri: a) organisaation toimintaympäristö, b) johtajuus, c) suunnittelu, d) tukitoiminnot e) toiminta f) suorituskyvyn arviointi ja g) parantaminen. Integroidulla hallinnalla tarkoitetaan turva- (security) ja turvallisuus- (safety-)näkökulmien kytkemistä, koordinointia ja yhdistämistä synergioiden hyödyntämiseksi ja keskinäisten ristiriitojen ratkaisemiseksi. Niiden samankaltaisuuksien ja erojen tunnistaminen ja ymmärtäminen ovat välttämättömiä integraation toteuttamiseksi. Integraatio voidaan toteuttaa rakenteellisesti, toiminnallisesti ja kulttuurisesti. Ne kaikki edistävät uuden integroidun kulttuurin luomista ja hallintaa. Integroinnin toteutuminen edellyttää motivaatiota. Tarve perustuu vaarallisia kemikaaleja käsittelevien laitosten kasvaviin kyberturvallisuusuhkiin. Integraation tuomia etuja ovat parantuva turvallisuus, resurssien käytön optimointi, henkilöstön tyytyväisyys ja lisääntynyt selviytymiskyky erilaisissa häiriötilanteissa (resilienssi). Mahdollisia toimintoja, joissa turva- ja turvallisuusnäkökulmia on syytä yhdistää, ovat esimerkiksi riskien arviointi, tapahtumaraportointi, hätätilanteiden hallinta, muutosten hallinta ja yleisölle tiedottaminen. Turvauhkien ja turvallisuuden hallinta ovat toisiinsa kietoutuneita asioita, joihin liittyy sekä yhteisiä että erilaisia näkökohtia. Tarvitaan sekä erityistä turvauhkiin ja turvallisuuteen liittyvää tietoa että näiden integroitua hallintaa. Pelkkä turva- ja turvallisuusalojen yhteen liittäminen ja kommunikointi ei kuitenkaan riitä johtuen nykyisten turva- ja turvallisuuskysymysten toisiinsa kietoutuneesta ja monimutkaisesta systeemisestä luonteesta. Tulevaisuudessa tarvitaan uutta integraatioon perustuvaa ajattelutapaa.
ISBN, ISSN, URN	ISBN 978-951-38-8745-2 ISSN-L 2242-1211 ISSN 2242-122X (Verkkojulkaisu) DOI: 10.32040/2242-122X.2021.T385
Julkaisuaika	Huhtikuu 2021
Kieli	Englanti, suomenkielinen tiivistelmä
Sivumäärä	54 s. + liitt. 13 s.
Projektin nimi	
Rahoittajat	
Avainsanat	
Julkaisija	Teknologian tutkimuskeskus VTT Oy PL 1000, 02044 VTT, puh. 020 722 111, https://www.vtt.fi/

Guidelines

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

ISBN 978-951-38-8745-2
ISSN-L 2242-1211
ISSN 2242-122X (Online)
DOI: 10.32040/2242-122X.2021.T385

VTT beyond the obvious