The need of improved methods to handle functional safety and cybersecurity in industrial control and safety systems

Mary Ann Lundteigen[1], Bjørn Axel Gran[2,3]

[1] Department of Engineering Cybernetics, Norwegian University of Science and Technology (NTNU), Trondheim
[2] Department of Mechanical and Industrial Engineering, Norwegian University of Science and Technology (NTNU), Trondheim
[3] Institute for Energy Technology (IFE), Halden, Norway
Corresponding author: 93059365, mary.a.lundteigen@ntnu.no

Abstract

Many industrial sectors like railway, oil and gas, and process industry depend to an increasing extent on active digitalized safety-critical systems, involving sensors, controllers, and actuated devices. The primary focus of such systems is to manage the risks arising within a physical system and environment where hazards can arise, and the consequences of failure can be severe losses to humans, the environment or critical infrastructures. The commonly accepted design principles for digitalized safety-critical systems follow standards like IEC 61508 and its sector specific implementations. The standards take a lifecycle perspective on the definition, implementation, and follow-up for safety requirements formulated on the basis of traditional hazards and risk analyses. Today, the systems have become a part of a cyber-physical environment, which means that hazards and threats relating to information and communication (ICT) security need considerations in the formulation of requirements, design, and operation strategies. Unfortunately, there are no aligned approaches for methods and approaches in IEC 61508 and referenced standards in ICT security, making the analyses separate rather than integrated. This paper presents a literature survey of standards, recommended practises, and publications relating to this topic. The focus is on the process industry sector, including the oil and gas sector. Thereafter the research planned to improve methods and tools for demonstrating functional safety by incorporating strategies to manage ICT security threats is presented. This includes (1) the definition of how safety and security requirements can be formulated, when considering their combined effects on functional safety, and (2) how the follow-up of requirements formulated under (1) are maintained in the operational/use phase.

1. Introduction

On Tuesday March 19th, 2019, Hydro, the global supplier for aluminium, experienced a serious security attack that affected also the ability to operate the plants using the industrial control and safety (ICS) systems [1]. No safety incidents were reported, but many Hydro plants had to operate quite complex processing facilities in the manual mode, and the cost has been estimated to about 300-350 MNOK [2]. It is assumed that many of the safety functions where either degraded or unavailable, and that manual measures would be necessary to stop the plant if unsafe events occur. The attack on Hydro is only one out of several security incidents that have affected ICS systems. Examples include the Maroochy water breach in 2000 [3], Stuxnet worm in 2007 [4], the digital sabotage of the pipeline system in Turkey in 2008 [5], the Maersk ransomware attack in 2017 [6], TRITON attack in 2017 [7]. After each of these events, focus has been placed on improving the ICT security of ICS systems, but still new events following new strategies occur. It is therefore undisputable that effort is needed to develop design strategies, operational strategies, and analysis

methods that can ensure and verify that ICS systems are safe as well as secure. The need to develop digitalization strategies that address ICT security are therefore put on the agenda by industry actors, national authorities and governments, for example through reports like [8] and [5] in Norway.

Before electronic and programmable electronic (E/PE) technologies were introduced to ICS systems, a combination of pneumatic and electrical control were often utilized for control as well as for safety functions. The ICS systems had no or very limited interaction with other systems. The design philosophy governing the process industry sector was that safety systems should be simple and physically separated from all other systems. The philosophy to keep ICS systems separated from other systems, like administrative ICT systems, remained also after E/PE technologies were introduced. However, digital tools and solutions and increased capacities of information and communication (ICT) networks have opened up new ways of operating the facilities, including remote operation, remote maintenance and remote monitoring. The potential challenges from having connections, even if protected, between ICS and administrative and external systems has been addressed by the industry for many years. For example, the Norwegian oil and gas industry made a joint effort through the PDS forum[1] in Norway (also with support from the Research Council of Norway), which resulted in a guideline called the SeSa method for securing remote access to safety instrumented systems (SIS) [9]. A SIS is the term often used in the process industry for the safety part of an ICS system.

Other initiatives have been taken on how to manage safety as well as security in the design and operation of ICS. The introduction of new security standards for ICS systems, like IEC 62443 series [10], have been supported by industry guidelines and recommendations like [11] and [12]. The more complete overview of initiatives are found in a comprehensive review carried out by the MERGE project on Security and Safety Co-engineering [13]. This report was published in 2016, but since then there have been many other publications, such as e.g. [14] [15], [16], and [17]. Despite the work, many regulations (e.g. by the Petroleum Safety Authority Norway [18] and Norwegian Directorate for Civil Protection (DSB) [19]) and standards adapted for ICS systems (e.g. IEC 61508 [20] and IEC 61511 [21] for SIS) focus more on ensuring safety from events that stem from the operation of the facility, not external threats and attacks. Design and operation of ICS systems involve disciplines like automation and technical safety, while disciplines on ICT security are not well integrated. Many of the above referenced guidelines, reports, and papers, on security and combined security and safety engineering and analysis, point to the challenge in mastering the interdependencies between safety and cyber (i.e. ICT) security, as advocated in e.g. [22].

The aim of the present paper is to suggest research directions for methods and tools for demonstrating functional safety by incorporating strategies to manage ICT security threats for ICS systems in the process industry. This includes (1) the definition of how safety and security requirements can be formulated, when considering their combined effects on functional safety, and (2) how the follow-up of requirements formulated under (1) are maintained in the operational/use phase. The paper takes functional safety standards like IEC 61508 and IEC 61511 as the starting point and elaborates on possible strategies for incorporating security analysis in for this purpose, with basis in recommended industry practises and research papers identified for security and safety co-engineering. Examples have been taken from different process industry sectors, including the oil and gas industry which has been quite active in developing sector guidelines.

[1] PDS forum: A forum of SIS manufacturers, consultancy companies, engineering companies, oil companies, see www.sintef.no/pds

2. Literature review

2.1 Standards on functional safety

2.1.1 IEC 61508

IEC 61508 [20] is the generic standard for the safety part of ICS systems. It provides general best practise principles for the design of safety-related electrical/electronic/programmable electronic (E/E/PE) systems. The safety ensured by safety-related E/E/PE systems, along with other risk reducing measures, is referred to as functional safety. Safety integrity is used as the measure of risk reduction required by E/E/PE safety functions and is split into four safety integrity levels (SIL). SIL requirements are defined on the basis of risk analyses, while the implementation or realization of E/E/PE systems follow measures for hardware, software, and hardware and software integration as advised by the SIL requirements. All requirements are organized according to what is defined as the safety lifecycle model. One of the objectives of IEC 61508 is to serve as a basis for development of sector-standards. This has led to development of sector standards like IEC 61511 (process industry) IEC 62061 (machinery) [23]. It has also led to the alignment between IEC 61508 and standards that already existed for a domain, such as for railway: EN 50126 [24], EN 50128 [25], and EN 50129 [26], for nuclear: IEC 61513 [27], and for machinery ISO 13489 [28].

The overall aim of IEC 61508 is to ensure safety of “equipment under control’’ (EUC). EUC is used as generic concept for a system that needs protection from hazards arising inside the system, or due to exposures to the environment. EUC can be a process unit (e.g. a vessel), a process section (e.g. separation system, including vessels, pipes, pumps), a fire area (protected by the same fire detection system), and the likes. The EUC concept does not address security threats or realization of security measures, and IEC 61508 even states in part 1 that it “does not specify the requirements for the development, implementation, maintenance, and/or operation of security policies and security services needed to meet a security policy that may be required by the E/E/PE safety-related system”. The few instances that mention security are:

- The scope definition in part 1 requires that “malevolent and unauthorized actions to be considered during hazard and risk analysis. The scope of the analysis includes all relevant lifecycle phases. The note refers to IEC 62443 series and ISO/IEC/TR 19791.
- Clause 7.4.2.3 in part 1 relating to “hazards and risk assessments” states that “If the hazard analysis identifies that malevolent or unauthorized action, constituting a security threat, as being reasonable foreseeable, than a security threats analysis should be carried out”. IEC 62443 is suggested as guidance on security threats analysis.
- Clause 7.5.2.2 (part 1) reads “If security threats have been identified, then a vulnerability analysis should be taken in order to specify security requirements*”.* Again, IEC 62443 series are mentioned as guidance.

Given examples of security incidents in the past where ICS has been affected, it seems evident that the term “if” can be removed from the scope definition. It is difficult to foresee that functional safety is achieved without considering measures against security threats. It is therefore reasonable to assume that the application of IEC 61508 will always require vulnerability analysis for security risks. However, the standard might not give adequate advices to when such analyses are needed, and how they should be done in order to be aligned with functional safety analyses. For example, the advice to carry out a vulnerability analysis in the lifecycle phase “hazards and risk analysis phase”, which takes place before it is determined which functions will be realized by E/E/PE

technologies, seems to be inadequate. Experiences from the industry also show that addressing security at all is hard [29].

IEC 61508 part 2 and part 3 cover the detailed realization of hardware, software, and hardware and software integration. The sector standards (like IEC 61511) can often replace these parts, when systems are built on modularized and already verified hardware and software. For new systems and devices for safety applications, most sector standards refer back to IEC 61508 part 2 and 3. This is why IEC 61508 is referred to as the “manufacturer standard”. What may be a bit of surprise is that security has no focus in part 2 and only one place where security is mentioned in part 3:

- IEC 61508 part 3 (on software) mentions security in appendix D covering normative requirements for software part of the safety manual for compliant items. Here, it is mentioned that the safety manual shall include “Details on any security measures that may have been implemented against listed threats and vulnerabilities”.

Still, we note no mentioning of security in part 2 (on hardware and hardware and software integration).

The maintenance team for IEC 61508 has started the revision process for the standard. Security is one of the topics that is subject to discussions. It is noted that there is a fundamental disagreement in how security is to be handled. As reported by one of the Peter B. Ladkin, one of the committee members on his web page [30]: “There is general agreement that IEC 61508 is not the place to describe details of cybersecurity analyses and how they are to be performed. Currently, the IEC 64223 series (Cybersecurity for IACS) is referenced.” Ladkin is referring to a technical report IEC TR 63069 (being under development) that is planned to cover the combined handling of safety and security for ICS systems. The positions of Ladkin seems to be that security cannot be separated out from IEC 61508, since functional safety and security are too interrelated to be left out of the standard.

2.1.2 IEC 61511

IEC 61511 [31] is the process sector implementation of IEC 61508 for ensuring functional safety. The standard applies safety-instrumented system (SIS) for the safety part of an ICS system, and the scope of the standard cover design and operation of SIS and the integration of SIS with other risk reducing measures. The application of IEC 61511 relies on SIS being constructed of already compliant (to IEC 61508) or prior-use devices and system. The prior use relies on the ability of the end user to demonstrate that the performance of the device is understood well, given an extensive amount of data collected from testing and operation of devices of the type in question. IEC 61511 gives some more attention to security than IEC 61508. EC 61511 was published six years after the second (prevailing) version of IEC 61508 was made available, a period where security has been an important focus of other standardization committees as well. As opposed to IEC 61508, IEC 61511 also mentions requirements for security in the phases of realization and operation of SIS.

Security is first mentioned in clause 8.2.4 of part 1 (as part of the requirements for hazards and risk analysis). The clause reads: A security risk assessment shall be carried out to identify the security vulnerabilities of the SIS”. Unlike IEC 61508, IEC 61511 details what the security risk assessment should consider. Each point is presented and briefly commented by the authors’ own reflections:

- “A description of devices covered by this risk assessment”.

According to IEC 61511, the scope of the hazards and risk analysis is the process that is subject to physical hazards (“equipment under control”), including the control system part of the ICS system.

From a security point of view, it seems not appropriate to limit the scope of a security threat analysis to a part (and not the whole) ICS system. The practical limitation is that the SIS at this stage of the lifecycle is not yet been defined. This means that devices (that at a later stage) are added to perform the necessary safety instrumented functions (SIFs), i.e. sensors, logic solver (Central processing unit and I/O cards), actuated devices, and human interfaces, are not considered in the specified security threat analysis. A security threat analysis needs to consider the impact of communication and network devices. In traditional safety analysis, the communication and network devices may be disregarded, in cases where the SIF devices are assumed to fail to a safe state upon loss of power or loss of signal/communication. The possibility to have wrong commands or modified/corrupted commands from the logic solver due to security attacks, are usually not considered, beyond assuming that communication for safety commands follow principles like “black channel”. The scope of devices to include in security analyses may therefore be different than for the analyses of functional safety.

- “A description of identified threats that could exploit vulnerabilities and results in security events (including intentional attacks on the hardware, application program and related software, as well as unintended events resulting from human errors”.

The traditional hazards and risk analyses of the EUC are based on layout descriptions of the plan, process and instrument diagrams (P&IDs), operational procedures, and like. Disciplines involved are usually operators, maintenance persons, risk analysts, and disciplines like technical safety, process, mechanical, electrical, and automation. Over time the methods used (including terminologies) are well known by these parties. This is not the case when analyses are extended to also include security threats. The analyses may need to add new disciplines with ICT and security knowledge, and in order to communicate, it seems necessary that the security terminologies are aligned or explained against terminologies used in traditional hazards and risk analyses. It also seems necessary that all involved disciplines have some basic competence in ICT security.

- “A description of the potential consequences resulting from the security threats and the likelihood of these events occurring”

The risk matrix, often with risk acceptance criteria embedded, is often used to prioritize and evaluate the need for risk reduction in traditional risk analyses. Frequencies and consequences needed to evaluate the risk, are often provided by expert judgment, by simulation tools, and company or other available statistics. For example, OREDA [32], the offshore reliability database and reports on trends in risk level in the petroleum activity (RNNP), published once per year. The same maturity level of security risk analysis might not be expected. What to define as a security event may not be well understood, and tools used for safety are not suitable to model the consequence spectrum. While protection layers for managing safety risks are well defined, this is not the case protection measures provided to ensure secure systems. There are also limited data to support security risk analyses. In fact, this is a point that is stressed by organizations like Dragos, an organization that tracks public vulnerability advisories that have had an impact on ICS systems [33].

- “Consideration of various phases such as design, implementation, commissioning, and maintenance”

It seems reasonable to require that security risk is related to different phases. The measures may be quite different. For example, in design and implementation one may expect that technical security measures as well as security programs are important. In the commissioning and maintenance phases, when many tasks (e.g. testing, mounting, and installation) are carried out

with no or limited ICT security background, one may foresee that more practical rules and advice on how to avoid introducing new vulnerabilities are needed.

- "A description of, or references to information on, the measures taken to reduce or remove the threats."

It is referred to the elaborations made for the previous bullet. It seems to be a need to clarify who are the targets for measures. Which measure relies on the ICT security experts and which ones must be specified and implemented in a way that is comprehensible for ICS operators and engineers.

- "The determining of requirements for additional risk reduction."

Additional risk reduction following a traditional risk analysis (for safety) points to the use of non E/E/PE technologies. It is not clear if additional risk reduction for security has a similar meaning.

For the specification and realization phases of SIS, IEC 61511 specifies in clause 11.2.12 that "The design of the SIS shall be such that it provides the necessary resilience against identified security threats". Reference is made very specifically to security standards that concern security programs: IEC 62443-2-1 [34], ISA TR84.00.09 [35] and ISO/IEC 27001 [36]. IEC 61511 also places requirements to systems interfacing the SIS for maintenance and engineering in clause 11.7.3 in part 1. For example, access protection must be provided for a number of SIS functionalities, such as SIS mode of operation, program, data, disabling alarms, bypass, fault handling, testing, and maintenance. It is also specified in clause 11.7.3.4 that enabling and disabling the read-write access shall be carried out only by configuration management process using the maintenance/ engineering interface with appropriate documentation and security measures such as authentication and user secure channels. This measure was not adequately implemented in the system exposed to the TRITON hacking even, as we understand the analysis made by [7]. Two last clauses addressing security are 11.8.4 (relating to testing) and 12.4.2 (relating to application program implementation). The first requirement requires that forced inputs and outputs must be announced, both as part of engineering and as part of maintenance testing. Clause 11.8.6 requires that documentation for application program specifies how communication is made secure, if secure communication is specified as a requirement in the safety requirements specification (SRS).

2.2 Standards on ICS security

2.2.1 IEC 62443 series

The most commonly referenced standards for ICS security is IEC 62443 series [10]. The different parts of the standard focus on different aspects of security for the ICS system: General, policies & procedures, system, and component. The standards introduce security life cycle model, security assurance levels (SALs), topology architectures with the definition of zones and conduits, and a security program. The IEC 62443 parts have their equivalent version published by ISA, the international Society of Automation.

2.2.2 ISA TR84.00.09

ISA TR 84.00.09 [35] published in 2017 is a guideline on incorporating cybersecurity in functional safety lifecycle. This standard focuses on work processes and countermeasures to reduce the risk of cybersecurity threats and identifies cyber-attacks as potential causes of common mode failures. It suggests, for example, that ICT risks are added to the preliminary hazard analysis. A search indicates

that the standard receives a bit less attention than would be expected from being referenced by IEC 61511 as well as the title where cybersecurity is related to functional safety lifecycle.

2.2.3 Analysis of functional safety and security concepts

In the review of functional safety and security standards, we notice different terminologies and concepts, with some potential interrelationships. The table below summarizes our findings.

Functional safety	ICT security	Discussion
Equipment under control (EUC)	ICS	EUC is the system, e.g. a process facility, which needs some protection due to hazards that arise within the EUC itself or from external safety events. From the security perspective, it may be reasonable to consider the ICS as the analogue terms, where security hazards may arise internally in the ICS (by local intrusion) or externally.
Safety instrumented systems (SIS), Safety Instrumented Function (SIF)	Zones and conduits (networks and signals)	The SIS is a system that carries out one of more SIFs. At a facility, there may be more than one SIS, to separate systems with different purposes. Examples include: Process shutdown system, emergency shutdown system, fire and gas detection system, and fire extinguishing systems. The need for SIS (and SIFs) stems partly from risk analysis and partly from industry practises. Zones and conduits are defined areas where ICS devices share some common attributes, such as security risk level. The higher the risk level, the stricter measures to ensure that the zones and conduits are protected. Several SIS may be placed within the same zone and use the same conduits, but they may also be separated due to practical or physical layout considerations.
Safety integrity level (SIL), with four SIL levels	Security assurance levels (SAL), with four levels (per IEC 62443) or evaluation assurance level (EAL), with 7 levels (per ISO 15408)	A SIL requirement is placing corresponding integrity requirements on: Hardware (hardware safety integrity), software (software safety integrity), and work processes (systematic safety integrity). Hardware safety integrity is partly achieved by following requirements about minimum hardware fault tolerance and estimating the failure target measures according to the ranges specified for the SIL requirement. Software safety integrity and systematic safety integrity are fulfilled meeting requirements about tools, design principles, and work process, believing that the effort made is able to reduce the contribution from software and systematic safety integrity requirements to a level that is negligible compared to the SIL requirement. Demonstrating fulfilment of SAL focuses also on work processes and design principles and may therefore take a similar approach as for systematic safety integrity and software safety integrity.
Functional safety assessment (FSA)	IT cyber security assessment (per IEC 62443). Independent assessment focusing on detecting errors and faults that may lead to a loss of security (confidentiality, integrity,..).	An independent assessment focusing on verification and validation of the specification of safety requirements, realization of SIS, integration of SIS with other risk reducing measures, and of maintaining adequate performance in the operational phase. Functional safety assessment is focusing on ensuring that the necessary risk reduction is achieved, by the SIS and the SIS in combination with other risk reducing measures. A security assessment seems to focus more on economic consequences. It may be argued that when ICT security is considered for ICS systems, it is just as important to also consider the safety impacts. Priorities and requirements to measures may be different, depending on the consequences considered.

Functional safety plan	Security program	Traditional safety and security plans are treated as two independent plans. To fulfil the objectives for both safety and security the plans should be coordinated and integrated [29].

2.3 Reports on Industry recommended practise

In this section, we highlight industry recommended practises identified for the oil and gas industry. Some of these reports have relevance beyond this industry sector and are also referenced by other authors from other application areas.

2.3.1 SeSa method on secure remote access to SIS

The SeSa method on securing remote access to SIS was developed by SINTEF in 2007, as part of a research project funded by the PDS forum participants and the Research Council of Norway. The need was identified in relation to the at that time new operation concept “integrated operations”, where digital tools and internet communication platforms were introduced to improve internal collaboration (for oil companies) and external collaboration, with e.g. suppliers, like SIS manufacturers. The internet platforms were allowing SIS manufactures to carry out remote upgrades and maintenance of SIS application program and operating systems, but concerns were raised to how such access could be introduced under the full control of oil companies.

The suggested approach to secure remote access, referred to as the SeSa method, was based on a review of recommended practises in security at that time, in combination with discussions with PDS forum participants. The report concluded on the following needs for further research and work:

- More testing of SeSa method on real cases, in order to verify it against different scenarios and system setups
- Extending the approach to broader ICS context, which is believed to mean that a method like SeSA should cover also systems that have an interface to ICS (e.g. systems for condition monitoring), and which potentially, could be impacted of unsecure remote access.
- Development of what is called approved solutions, i.e. solutions for remote access that has been proven to resistant to the identified threats. Such solutions could be templates and examples for future realization of remote access.
- Integrating SeSa method beyond ensuring functional safety, meaning that the method is embedded into working procedures and technical measures across industry sectors.

2.3.2 NOG 104

The Norwegian Oil and Gas (NOG) published the second revision of the guideline 104 on information security baseline requirements for process control, safety and support ICT systems [12] in 2016. The purpose of the guideline is “to enhance overall information security in the offshore industry and thereby improve the safety and regularity of the operations on the Norwegian continental shelf (NCS)”. The standard uses the bow-tie model, well-known from risk analysis, to illustrate the security functions, and their relevance for either preventing ICT security events or mitigating their consequences. The standard introduces also 19 information security baseline requirements (ISBRs), where each of these are accompanied by:

- Specification of measure (called “control”)
- Objective (why is the requirement needed)
- Recommendations about implementation, using the cyber security framework from National Institute of Standards and Technology (NiST)

The implementation of measures according to ISBRs is considered as “good practice”.

2.3.3 DNV-GL RP G108

DNV-GL RP-G108 [11] on cyber security in the oil and gas industry based on IEC 62443 [10] was published in 2017, as the result of Joint industry project (JIP) with participation from several industrial partners and the Petroleum Safety Authority (PSA). The focus was not on the alignment of IEC 62443 with standards on functional safety however, the recommended practice is an important basis for such effort.

The standard defines its target audience as people involved in ensuring security, but not necessarily with security background, such as oil companies, system integrator, product supplier, service provider, compliance authority. The focus areas are: clarification of responsibilities with respect to implementing IEC 62443 requirements, and document is structured so that it covers the traditional project phases of an ICS design, realization and installation plus key activities after the system has been put into operation such as operation, maintenance, monitoring, management of change, and incident response and recovery. The recommended practice has a reference to IEC 61508 in the bibliography, but no discussion of its relevance and influence is included.

2.4 Regulatory perspective

2.4.1 Petroleum Safety Authority report on digitalization

The PSA has published a report by IRIS (in Norwegian), the International Research Institute in Stavanger, on the digitalization in the petroleum industry: Trends, knowledge, and proposal for new measures [37]. The report builds on literature review and interviews and workshops with experts and informants in various companies related to the oil and gas industry. Even if this report is focused on digitalization in general, and not on ICT security in specific, some findings relating to ICT security are reported:

- ICT security is one of the most important contributors to risk of accidents from increased digitalization. A concern is that the degree of digitalization can make systems more difficult to protect when the ability to detect, prevent, and respond to events rely on not only oil companies, but also suppliers and sub-suppliers.
- There is a need to balance the need for information flow between different actors and the ability to ensure ICT security.
- More complex ICT systems require more competence in ICT for all personnel involved with ICS systems.

General recommendations, that seems to apply well also for ICT security specifically, are (as interpreted by the authors):

- Digitalization represents an upheaval for the petroleum industry. The dimensions of risk contributors and consequences needs to be better understood.
- New risks that arises from new ways of collaborating and information sharing need to be identified. Information sharing is not a national matter, but can also go across national borders, with different sets of regulations and rule sets.
- There is a need to react to the lack of adequate competence in digitalization and effects of digitalization.

- There is a need for PSA to consider how the risks associated with digitalization can be reflected in targets, for monitoring (e.g. by RNNP). New indicators relating to ICT security needs to be added, and how to collect necessary input to these.

2.4.2 NOU report

The Norwegian public progress (NOU) report on digital vulnerability [5] discusses status on digital solutions and vulnerabilities in various arenas of society. In addition, a more detailed presentation of security risks associated with industrial sectors is included. For our review, we focused on identifying risks pointed out in the report related to ICS systems for energy supply, oil and gas, and water distributions. In this paper, focus is on findings related to the oil and gas sector

The oil and gas sector consists of offshore oil and gas facilities, exploration facilities, transport with pipeline networks and vessels, and receiving facilities onshore. Each of these facilities have their own ICS system, with necessary interfaces to other ICS systems where control and safety are interrelated. Some of the identified vulnerabilities include:

- Field development phase: The suppliers and sub-suppliers have an important role since they are heavily involved in engineering and in the delivery of systems and equipment. However, the security culture is not always sufficient, and vulnerabilities introduced in the development phase can make their way into the production phase.
- Production: Remote operation and remote support (internally and with external suppliers) are connecting ICS systems to networks based on internet technologies. If an attacker breaks through the firewalls, it is possible to impact the ICS system in many different ways. The human factor is also critical, as control centres, maintenance support centres, and systems for monitoring involve tasks where human errors can introduce security vulnerabilities.
- Transport: The ICS systems control the flow in pipelines and, in some cases, also provide instrumented overpressure protection. A security attack on these systems may result in potential hydrocarbon spills.

Examples of measures needed are:

- A transfer of traditions and practises in HSE into the digital area. The HSE area has had for decades a focus on measures to prevent major safety accidents, and most engineering disciplines like mechanical, process, technical safety, automation, and electrical systems are integrated into this work. The ICT security has in the past focused more on the office systems and may not have the detailed knowledge of how security can result in major safety accidents.
- The Petroleum Safety Authority should introduce requirements to the establishment of barriers to prevent and respond to digital vulnerabilities.
- The industry should establish arenas that can collaborate on responding to security events. Only a few actors in oil and gas are connected to NSM Nor-CERT[2]

2.5 Research on safety and security co-engineering

2.5.1 MERGE project

Safety and security co-engineering concern the process from safety and security requirements elicitation, through implementation of safety and security solutions, and the verification and validation of those properties [13]. This topic was the focus in an EU project called MERGE, carried out by a

[2] NSM NorCert is the operational part of the national security authority, see https://www.nsm.stat.no/norcert

large partner consortium from France, Finland, and Belgium. This project published a report with a very comprehensive state of the art on safety and security co-engineering, covering the period 2014-2016. The motivation to start this project was, according to [13], split into five main points:

1. Security *must* be considered: The questions is no more *if* your system is going to be subject to cyber-attacks, but *when and how.*
2. ICS systems are security targets: ICS systems, including SIS, are no more an exception to being subject to security attacks.
3. Components-on-the-shelf (COTS) have become ubiquitous in software and hardware engineering.
4. System maintenance in secure conditions and system maintenance in operational conditions have very different update rates and life cycles.
5. There are no complete and convincing solutions in the market to address safety and security engineering, including the trade-off decision support.

The first observation made by the MERGE partners in their state-of-the-art review, was the fact that the topic of safety and security co-engineering had already been devoted extensive attention in academic research. The literature review resulted in a comprehensive overview of the standards in the safety and security domain, research papers on co-engineering frameworks, aiming to align security and safety lifecycle models, and methods aiming to assess in combination the effects of security and safety properties. According to [13], 160 publications were identified. They also identified that the industrial community was revising existing and elaborating new standards to address the security of ICS systems, and a remark was made that there is very limited guidance from international regulations on security risk management.

The MERGE project has classified methods for safety and security co-engineering along two dimensions. One is the classification of methods into generic, model-based (graphical), and model-based (non-graphical). The other classification considers whether the methods:

- Took the approach of unification or integration: Unification means that security and safety phases are fully merged, while integration means that the interrelationship between a security approach and a safety approach are identified and harmonized.
- Covered lifecycle phases on development or operation: Development phases cover requirements and/or design/realization, while operation focuses on monitoring, maintenance, operation, and modifications after the system has been installed.
- Were qualitative or quantitative: Qualitative approaches are based on reasoning, while quantitative approaches use models supported by parameters that have been assigned quantitative values.

In the review of referenced publications in the MERGE state of the art review, we summarize the following findings:

- There is a potential conflict in the level of desired coupling: Safety-critical systems aim for few, linear and known interactions, and from loose coupling, while security requires an environment with few and controlled interactions and leads to tightly coupled systems.
- Harmonizing security and safety may result in many practical challenges: Safety and security analyses rely often on different system models, different documentation structures, and different focus of results produced. If requirements for safety and security are developed in isolation, they may be conflicting with each other. A unified approach could provide *one* set of requirements, while the harmonized approach gives two sets of requirements where consistency must be checked, and conflicts resolved. A concern raised against the use of unified approaches is that the specifics (tools, skills) of each domain (security and safety) may

not be fully captured, and this might lead to security and safety risks being overlooked or not observed.

- Knowledge and methods should be shared between safety and security disciplines: Security analysis techniques may have perspectives, methods, and tools that can improve safety analysis techniques, and vice versa. There are also some methods that can be extended to cover security as well as safety.
- In the future, we may expect most ICT systems to be security-critical as well as safety-critical, and not just one of these categories.
- There is a need to share information about security and safety among those being involved in protecting and supporting ICS systems.
- Reliance on quantitative analyses is more common insafety analyses than security analyses. While probabilities are widely adopted in safety domain, it is not always accepted in security field.

The MERGE report [13] provides a list of relevant international workshops that address safety and security and summarizes some examples of discussions that are ongoing on the topic. Examples include:

- There are exploitable similarities: Safety as well as security design approaches focus on multiple layers of defence and the separation/independence of each of these layers.
- There are some critical differences: Avoidance of systematic faults and random faults may not be effective to avoid malicious faults. Fault probabilities in safety often stem from mature models on failure statistics, while fault probabilities due to security threats must include factors that are difficult to predict and understand, like attacker motivation, rescources, and skills. Safety certification rely on few or no changes, while security patching relies on frequent updates.
- It seems that the community of safety and security co-engineering can be split into two categories: The *integration optimists*, who put forward the similarities of e.g., assurance activities, and the *integration pessimists* that put forward the differences in assumptions, practise, terminologies, and certification processes.

2.5.2 Selected research papers

We have identified some additional papers in the period following the state-of-the-art survey in the MERGE project. For example:

- STPA-SafeSec [14]: This paper focuses on presenting unified approach for identifying security and safety hazards using the systems-theoretic process analysis (STPA) approach [38]. The STPA has focused primarily on safety risks, without considering security. As such, this approach may be seen as an attempt to unify STPA and STPA-Sec. The authors of point to the ability of the combined approach to identify conflicts between safety and security in requirements derived from the analysis.
- A survey of approaches combining safety and security [22]: This paper is also identified in the MERGE project. The paper identifies some useful observations regarding safety and security dependencies:
    - Conditional dependency: Lack of security may directly impact the ability to carry out a safety function (ref. recent attacks into control systems).
    - Mutual reinforcement: Some measures are efficient both for safety and security (e.g. protecting communication protocols).
    - Antagonism: Conflicting interests. Door to be left open to let people out on fire, while for security (access control) it would be better to keep door closed.

    - Degree of relevance: Adding secure redundant devices may be good for safety, while not important for security.
- Integrated functional safety and cyber security analysis [15]: The authors reviews and discusses methods for integrating security and safety analyses, while not necessarily making them unified. The authors suggests a relationship between security assurance levels (SAL) and evaluation assurance level (EAL) and SIL. The also discusses how to extend the traditional definition of a safety instrumented function (SIF) with elements of relevance from a security point of view. The paper concludes that they want to extend the research by including the human as a hazard factor.
- UFoI-E method for combined safety and security analysis [16] [17]: This paper introduces a diagrammatic model to support the identification of uncontrolled flows of information and energy, referred to as UFoI-E method. The model identifies the how security threats may propagate through the system and eventually cause a harm to the physical system controlled by an ICS system.

3. Discussion and recommendations for further research

The review of literature in this paper has identified the extensive effort ongoing in the field of safety and security co-engineering and analysis directed to ICS systems, including academic research, standards, and recommended practises. Questions and topics that seem to be unresolved from our point of view are:

- Should the design and operation of the control part (not safety-critical) of ICS system be treated differently for the SIS part from the security point of view?
- Should the SIS take on new roles to detect and respond to security threats occurring inside the control system part of ICS?
- Should separate and dedicated measures be introduced for handling the situation after an intrusion in the ICS system has been detected, with some restricted functionalities that can ensure the safe state of the facility? The analogy can be drawn to the use of critical alarm panel (CAP) in the oil and gas industry. The CAP panel represents a non-computerized human interface that will provide (based on hardwired signals) the status of key information (e.g. fire and gas detector status) and buttons to initiate manually (by hardwired fail-safe signals) to breakers, switches, and contactors that can isolate power. Some selected functions will have uninterruptable power supply (UPS) to initiate safety functions that rely on power supply, e.g. start of emergency generator.
- How will new ways of operating the facilities, e.g. unmanned and autonomous, influence requirements to security measures, in order to close down the facility and prevent uncontrolled restart in case of security attacks?
- The community of safety and security seems to disagree on what is the best: integration or unification. Will different strategies be needed in different phases of the safety life cycle?
- How can we manage the human and organizational factors when managing ICT security for ICS systems? An ICS system cannot be safe unless it is also secure, and all disciplines involved in ICS specification, design, installation, testing, operation, maintenance and modifications have the potential to introduce security vulnerabilities. The disciplines cover most engineering disciplines, in addition to operation and maintenance personnel, and the minimum level of ICT security knowledge needs to be defined for each of these.
- How can we integrate security barriers into a similar framework as for safety barriers? For example, the Norwegian Petroleum Safety Authority (PSA) states in the facility regulations §5 that “Personnel shall be aware of what barriers have been established and which function they

are intended to fulfil, as well as what performance requirements have been defined in respect of the concrete technical, operational or organisational barrier elements necessary for the individual barrier to be effective." It seems reasonable to suggest that these requirements should also apply to security barriers. Some security barriers may influence the performance of specific safety barriers, while others may be potential single points of failure for multiple barriers. These aspects should be considered in the visualization and monitoring of safety barrier status.

In relation to the work with this paper and needs identified in discussion with industry, a joint research effort between NTNU and IFE have been initiated through a Ph.D. position at NTNU with co-supervision at IFE, linking the research to the newly established cyber and digitalization centre at IFE [39]. The Ph.D. candidate will focus on:

- The identification of how safety and security requirements can be formulated, when considering their combined effects on functional safety, e.g. identify how the current SIS shutdown and restart philosophy can be impacted by security threats. The starting point can be to analyse philosophies that are well documented as e.g. in NORSOK S-001 [40].
- How to follow-up of that the requirements formulated are also maintained in the operational/use phase. Safety and security requirements may need to be reformulated at regular intervals. Otherwise the work hours of highly qualified engineers will be ground up between a large set of national and international standards, some of which are rather lengthy, and others are expensive to obtain. On an organizational level, this encourages either a culture of cutting corners or inflates costs. While the former is an obvious threat to safety, the latter is indirectly also affecting human health. Inflated costs also drive companies to places where regulation in not enforced or to pursue technologies that have a constant level of health risks over rare but spectacular failures.
- Development of suitable methods to support the formulation of requirements and the demonstration of adequate performance of implemented solutions. This includes identifying what types of analyses can be added, or how can existing analyses in IEC 61508 and in some selected related standards, like IEC 61511, can be modified, and how the lifecycle model should be updated accordingly.
- How to reformulate requirements to include both safety and security shall be inspiring and executable to the involved project engineers. There will be a need for necessary buy-in from their side, as any formulation of requirements depend of the real-life feedback. A low threshold should be implemented for providing this feedback. The method might be to crowd-source the project specific requirements from the subject matter experts and validate them statistically, introducing democratic verification in addition to an agile framework.

Ensuring safe and security ICS systems in the process industry relies on collaboration and transfer of experience between different industrial application areas. As such, this paper can also be regarded as a platform for sharing experience between the oil and gas sector and the nuclear sector.

Acknowledgement

This paper submitted to the OECD Halden Programme Meeting in OECD Reactor Project, May 19-24, 2019 (Sandefjord, Norway), *http://ehpg.hrp.no/* is produced through a cooperative agreement between IFE and NTNU.

Bibliography

[1] Hydro, 22 03 2019. [Internett]. Available: https://www.hydro.com/en-NO/media/news/2019/update-on-cyber-attack-march-22/. [Visited 22 03 2019].

[2] Hydro, 26 03 2019. [Internett]. Available: https://www.hydro.com/en-NO/media/news/2019/update-on-cyber-attack-march-26/. [Visited 26 03 2019].

[3] J. Slay and M. Miller, «Lessons Learned from the Maroochy Water Breach,» *IFIP International Federation for Information Processing (Volulme 253)*, Boston, Springer, 2007, pp. 73-82.

[4] R. Langner, «Stuxnet: Dissecting a Cyberwarfare Weapon» *IEEE Security and Privacy,* vol. 9, nr. May/June, pp. 49-51, 2011.

[5] NOU, Digital sårbarhet - sikkert samfunn (NOU rapport 2015:13), Oslo: Departementenes sikkerhets- og serviceorganisasjon, 2015.

[6] A. Belokas, «Safety4sSea.com» [Internett]. Available: https://safety4sea.com/cm-maersk-line-surviving-from-a-cyber-attack/. [Visited 24 3 2019].

[7] A. Di Pinto, D. Y. and C. A., TRITON: The First ICS Cyber Attack on Safety Instrumented Systems: Understanding the Malware, Its Communcation and its OT Payload, Nozomi Networks, 2018.

[8] Goverment of Norway, Meld. St.38 (2016-2017): Cyber Security - A joint responsibility, Oslo: https://www.regjeringen.no/en/id4/, 2017.

[9] T. Grøtan, M. G. Jaatun, K. Øien and T. Onshus, The SeSa Method for Assessing Secure Remote Acccess to Safety Instrumented Systems (SINTEF A1626), Trondheim: SINTEF, 2007.

[10] IEC 62443, Industrial communication networks - Network and system security series, Geneva: International Electrotechnical Commitee, 2010, 2015.

[11] DNV-GL RP-G108, Cyber security in the oil and gas industry based on IEC 62443, Oslo: DNV-GL, 2017.

[12] NOG-104, Norwegian Oil and Gas recommended guidelines on information security baseline requirements for process control, safety and support ICT systems, Stavanger: Norwegian Oil and Gass, 2016.

[13] ITEA2, MERGE project report Recommendations for Security and Safety Co-Engineering (Deliverable D.3.4.4 - Part A), Information technology for European Advancement, 2016.

[14] I. Friedberg, K. McLaughlin,, P. Smith, D. Laverty and S. Sezer, «STPA-SafeSec: Safety and security analysis for cyber-physical systems» *Journal of Information Security and Applications,* vol. 34, nr. 2, pp. 183-196, 2017.

[15] M. Sliwinski, E. Piesik and J. Piesik, «Integrated functional safety and cyber security analysis,» *IFAC Conference PapersOnline*, USA, International Federation of Automatic Control, 2018, pp. 1263-1270.

[16] N. Guzman, D. Kufoalor, K. I. and M. Lundteigen, «Combined safety and security risk analysis using the UFoI-E method: A case study of an autonomous surface vessel» *Submitted to ESREL 2019 conference*, 2019.

[17] N. Guzman, M. Wied, I. Kozine and M. Lundteigen, «Conceptualizing the key features of cyber-physical systems in a multi-layered representation for safety and security analysis» *Submitted to Journal of Systems Engineering,* 2019.

[18] PSA, «Petroleum Safety Authority Norway,» [Internett]. Available: http://www.ptil.no/regulations/category873.html. [Visited 24 3 2019].

[19] DSB, Norwegian Directorate for Civil Protection (DSB) , [Internett]. Available: http://www.ptil.no/regulations/category873.html. [Visited 24 3 2019].

[20] IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems (7 parts), Geneva: International Electrotechnical Commitete, 2010.

[21] IEC 61511, Functional safety - Safety instrumented systems for the process industry sector (3 parts), Geneva: International Electrontechnical Commitee, 2016.

[22] S. Kriaa, L. Pietre-Camacedes, M. Bouissou and Y. Hagland, «A survey of approaches combining safety and security for industrial control systems» *Reliability Engineering and System Safety,* pp. 156-178, 2015.

[23] IEC 62061, Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems, Geneva: International Electrotechnical Committee, 2015.

[24] EN-50126, EN 50126, Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS), European Committee for Electrotechnical Standardization (CENELEC), 2017.

[25] EN-50128, Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems, European Committee for Electrotechnical Standardization (CENELEC), 2011.

[26] EN-50129, Railway applications – Communications, signalling and processing systems – Safety related electronic systems for signalling, European Committee for Electrotechnical Standardization (CENELEC), 2003.

[27] IEC 61513, Nuclear power plants - Instrumentation and control important to safety - General requirements for systems, International Electrotechnical Commission, 2011.

[28] ISO 13489, Safety of machinery -- Safety-related parts of control systems -- Part 1: General principles for design, International Organization for Standardization, 2015.

[29] B. A. Gran, A. Egeli and A. Bjerke, «Addressing security in safety projects – experiences from the industry» *Fast abstracts at International Conference on Computer Safety,Reliability, and Security (SAFECOMP)*, Trondheim, 2016.

[30] P. Ladkin, Cybersecurity in IEC 61508, [Internett]. Available: http://www.systemsafetylist.org/4502.htm, 2019. [Visited 24 3 2019]

[31] IEC 61511, Functional safety: Safety instrumented systems for the processindustry sector (3 parts), Geneva: International Electrotechnical Commiteee, 2016.

[32] OREDA, [Internett]. Available: https://www.oreda.com/. [Visited 28 03 2019].

[33] Dragos, Year in review (2018) Industrial controls system vulnerabilities, Dragos, 2018.

[34] IEC 62443-2-1, Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program, Geneva: International Electrotechnical Commission, 2010.

[35] ISA TR84.00.09, Cybersecurity Related to the Functional Safety Lifecycle, International Association of Automation, 2017.

[36] ISO/IEC 27001, Information technology - Security techniques - Information security management systems - Requirements, International Organization for Standardization, 2013.

[37] IRIS, Digitalisering i petroleumsnæringen: Utviklingstrender, kunnskap og forslag til tiltak, Stavanger: International Research Institute of Stavanger, 2018.

[38] N. G. Leveson and J. Thomas, STPA Handbook, Boston: Massachusetts Institute of Technology (MIT), 2018.

[39] NRK Østfold, [Internett]. Available: https://www.nrk.no/ostfold/atomen-i-halden-bygges-om-1.14493860. [Visited 28 3 2019].

[40] NORSOK S-001, Technical Safety, Stavanger: NORSOK, 2018.