Clarification of the Cybersecurity and Functional Safety Interrelationship in Industrial Control Systems: Barrier Concepts and Essential Functions

Bálint Z. Téglásy

Department of Engineering Cybernetics, NTNU, Norway. E-mail: balint.teglasy@ntnu.no

Bjørn Axel Gran

Department of Risk, Security and Safety, Institute for Energy Technology, Norway.

Sokratis Katsikas

Department of Information Security and Communication Technology, NTNU, Norway.

Vasileios Gkioulos

Department of Information Security and Communication Technology, NTNU, Norway.

Mary Ann Lundteigen

Department of Engineering Cybernetics, NTNU, Norway. E-mail: mary.a.lundteigen@ntnu.no

Cybersecurity requirements for industrial automation and control systems (IACS) are aligned with normative documents like IEC 62443. This standard recognizes that a safety-instrumented system (SIS) must maintain the ability to operate in the presence of cybersecurity events, to avoid harm to people, the environment or physical assets. A SIS has traditionally been designed with only safety in mind, since the technology was proprietary and not connected to general IT systems. Standards on design and operation of a SIS, like IEC 61508, IEC 61511 and IEC 61513 have therefore focused on ensuring the functional safety. Today, a SIS involves also commercial technologies with far-reaching implications for remote monitoring, operation, and updating. Past cybersecurity incidents like Stuxnet and Triton have revealed that there may be motivation as well as resources to exploit new vulnerabilities. It is therefore necessary to treat safety and security in IACS in an integrated manner. Their mutual dependency cannot be ignored since the design allows more logical as opposed to physical access. Co-analysis methods can be found in Lisova et al. (2019) but are not yet applied to guide design or operation decisions in engineering practice. This paper presents how the mentioned safety standards address cybersecurity, and identifies requirements from IEC 62443 which may have an impact on how requirements in the safety standards are formulated. The research gives initial advice on how security and safety requirements are interrelated.

Keywords: safety, security, industrial automation and control system (IACS), safety instrumented system (SIS), critical infrastructures.

1. Introduction

On Tuesday March 19th, 2019, Hydro, the global supplier for aluminium, experienced a serious security attack that also affected the ability to operate the plants using the IACS as seen in Hydro (2019). 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 30-35 million Euros. This was one out of several security attacks that have affected IACS. Examples include Slay and Miller (2007), Langner (2011), the digital sabotage of a pipeline system as reported by NOU (2015), the attack against the Ukrainian power grid as reported by Cherepanov and Lipovsky (2017), and TRITON as reported by Di Pinto et al. (2018). The need to develop digitization strategies that address IACS security are therefore put on the agenda by industry actors, national authorities and governments, for example through reports like the one by the government in Government of Norway (2019).

Safety addresses hazards inherent to the technological process and randomly occurring outside threats. According to the CNSS (2015), security is a condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use

Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference
Edited by Piero Baraldi, Francesco Di Maio and Enrico Zio
Published by Research Publishing, Singapore.
ISBN: 978-981-14-8593-0; doi:10.3850/978-981-14-8593-0

of information systems [a]. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach. Most safety-critical industrial systems are also security-critical. In an industrial setting, safety and security failures can have similarly catastrophic consequences, yet the connections (binary or order relations) between safety and security are not clear. It is our assumption that while safety regulation directly addresses hazards inherent to the technological process and randomly occurring outside threats, security features are intended to protect against harm caused with human intention. In order to find a common level of abstraction for safety and security that is relevant to the way that critical infrastructures are managed on a global scale, our analysis takes a normative approach. This means that standards of the International Electrotechnical Commission (IEC) for functional safety and cybersecurity of these same systems are taken as the starting point, as the resulting IACS will need to comply with both standards. Differing terminology and their underlying concepts are clarified. Unless otherwise stated, all terms are used in the sense of IEC 61508 (2010) or IEC 62443 (2015).

The interconnected nature of new process control technologies leads to efficiency gains but also to new cybersecurity risks. While the new risks are growing in proportion to the safety risks that the industry tackled with the widespread adoption of functional safety, regulated by standards like those by the IEC, the interface between safety and security is becoming more important. This is reflected by the work of many national nuclear safety regulators and authorized organizations such as Strålsäkerhetsmyndigheten (2018) in the nuclear sphere: in their Common Position on Safety Critical Software in Nuclear Reactors, paragraph 1.8.3.3, they ask for - among others - design, assurance, verification and validation to be integrated with regards to cybersecurity across the system lifecycle. The interfaces are currently not well defined: safety and security functions co-exist in modern IACS without consolidated integration as Ladkin (2019) puts it. Specifically, he claims that the threat-risk assessment in IEC TR 63069 "Framework for functional safety and security" is underspecified. Simultaneous assessment or co-analysis of safety and security is researched but not yet widely applied in industrial applications. Lisova et al. (2019) provides a recent literature review of co-analyses. Although security and safety engineering are distinct areas with developments that are largely independent of each other until the recent past, the perspectives opened up by Cyber-Physical Systems (CPS) to support a transition to an Industrial Internet of Things (IIoT) make it critical to handle potential inconsistencies between two abstractions of safety and security. Practical and compliance issues emerge from the increased use of IT systems in Operational Technology environments.

The management of functional safety in a modern information and communication technology (ICT) enterprise environment is intertwined with cybersecurity policies and mechanisms. This was elaborated on by Lundteigen and Gran (2019). While IEC 61508 only refers to IEC 62443 when it comes to security, the latter does make prescriptions in dealing with SIS in terms of essential functions. Thus a modern IACS including a SIS will likely need to comply with both. To examine the safety and security interrelationship, the remaining content of the paper is structured as follows: (i) clarifies how safety and security barriers are defined in chapter 2.1 and 2.2, respectively, (ii) elucidates potential contradictions regarding the independence of implied barriers in the security and safety systems by translating the IEC 62443 security domain requirements to the safety domain requirements in chapter 2.3, (iii) discusses why the essential functions of both security and safety systems need to be defined on a facility-specific level in chapter 3, and (iv) discusses the implications for individual IACS architectures and their compliance-based regulation in chapter 4.

2. Barriers

Functional safety and cybersecurity have in common that they both rely on a Defense-in-Depth approach when it comes to high risk technologies. Defense-in-Depth implies the existence of more than one barrier. The interpretation of Defense-in-Depth in safety relies on independent barriers and this independence is often queried by compliance. The independence assumption of IT cybersecurity barriers, also known as layers, was challenged by the work of Schudel and Wood (2001) and Kewley and Lowry (2001): in cybersecurity, additional barriers seeming independent at first can become vulnerabilities endangering the whole network by a matter of configuration (see also Wolff (2016). In the case of security applications, competing integration and independence requirements for the barriers need to be investigated in terms of networked IACS architectures.

2.1. *Barrier concept in functional safety*

In IEC 61508-5, paragraph A.5.4 on "Common Cause and Dependency Failures" provides re-

[a] CNSS (2015) is also referenced by the IEC 62443-1-1 for the definition of security as being the *capability of a computer-based system to provide adequate confidence that unauthorized persons and systems can neither modify the software and its data nor gain access to the system functions, and yet to ensure that this is not denied to authorized persons and systems*, but this definition can not be found in the source.

quirements for dividing safety system(s) into barriers. This is in the informative part of the standard, as the normative parts are 1-3. Figures A.1 through A.4 in part 5 are all drawn with the assumption that all safety systems relevant for the same hazard are fully independent. Out of many imaginable cases, five examples are given as exemptions from independence: in these cases, common cause failures (CCF) are expected to be treated. The residual hazard rates are influenced negatively in the absence of independence. This means the hazard can not be further reduced with the risk reduction measures available within the chosen architecture and is likely to be significant in designs aimed at high safety integrity levels (SILs).

In the guidelines on hardware failure (part 6 of IEC 61508), electrical/electronic/programmable electronic (E/E/PE) safety-related systems in continuous (synonymous with high demand) mode are differentiated from the ones in low demand mode by the quantifications and qualifications for barriers. The considerations about probabilistic calculations are diverging when a continuous mode has to be assumed. The failure of continuous mode systems fall into the unreliable case if they form a single barrier working in continuous mode, but in the unavailable case if multiple safety barriers are present. The difference between unreliable and unavailable systems is primarily the ability to repair before a residual hazard event. The ability to repair in the context of recovery hinges upon detectability of the individual barrier failure and could be generalized to software or even security: consequently, the diagnostic coverage of a safety-related system (driving the self-announcing failure ratio in IACS reliability studies) would be applied to cybersecurity. Probabilistic models could quantify recovery options typical for resiliency-oriented networked systems, but this is not standardized in the security domain.

2.2. *Barrier concept in cybersecurity*

The cybersecurity interpretation of barriers and similar terms like zone boundaries, on the other hand, does not focus on the independence of these barriers, presumably because it is not realistic to assume such independence in modern communication networks. Nevertheless, for hazardous or otherwise critical processes cybersecurity claims a defense in depth concept which necessitates separate barriers. If applied at the same point in a network or at a zone boundary, no amount of cybersecurity countermeasures or hardening can provide defense in depth for the whole facility, because other points of entries exist by definition of a networked system.

2.2.1. *Boundaries*

The IEC 62443 uses boundaries as a synonymous definition to barriers (def. 3.2.19) and categorizes them as software, hardware or physical. The latter (physical security boundaries) do not have a common set with functional safety as they are interpreted to limit the movement of people[b]. Software and hardware boundaries, on the other hand, should be investigated to clarify the interface with the E/E/PE safety systems. In the following, examples of such boundaries are given.

2.2.2. *Barrier devices, Network segmentation*

In Establishing an IACS Security Program (IEC 62443-2-1), the element Network Segmentation is defined in paragraph 4.3.3.4, and among others requires that *IACS should be designed in a manner that filters/prevents nonessential communication packets from reaching the IACS devices* and, formulated harder in Table 10, *Barrier devices shall block all non-essential communications in and out of the security zone containing critical control equipment.* The definition and especially the implementation of essential communications is crucial when considering a safety instrumented system (SIS). The implementation would need to focus on a clear differentiation of what is essential, otherwise the barrier devices might block safety critical signals. Barrier devices are typically firewalls (configured to block, as seen above), routers and layer 3 switches. A network segment is not explicitly defined in IEC 62443, but can be interpreted as a segment between two barriers. The vertical zoning displayed in Fig. 1 can be understood as a simplified Purdue Reference Enterprise Architecture (see Williams (1994), where levels 0 to 2 are in the Control Zone, level 3 functionalities are shared between the Control Zone and the Demilitarized Zone (DMZ), and level 4 is in the Enterprise Zone.

To model and analyze safety hazards in conjunction with security risks, the location of the SIS in this architecture needs to be elucidated. The SIS can be:

(i) Non-programmable, e.g. relay-based, consequently precluding remote logical access and cyber events through networked technologies. In this case, cyber threats could only penetrate the safety barrier through human actors, e.g. with a fake maintenance instruction.
(ii) Digital (hosted on a programmable platform) that can

[b]This might change with the application of autonomous vehicles, e.g. drones for exploiting a hybrid physical/cyber security vulnerability through transporting rogue access points.

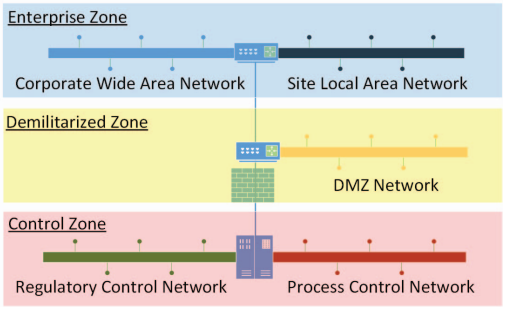

Fig. 1. Barrier devices segment networks, but a network segment is not always a security zone to itself. See reference architecture alignment with a segmented architecture in IEC 62443-2-1 for a more detailed figure.

(a) be connected to the Regulatory Control Network[c]; in this case an additional security zone just for the SIS is recommended
(b) have their own (potentially redundant) network(s)
(c) be highly integrated with the Basic Process Control System (BPCS), such that they run on the same hardware

(iii) Diverse, that can be any combination of the above, adding not just safety but also security barriers to the overall architecture.

According to the IACS technical requirement SP.05.04 in IEC 62443-2-4 relative to the integration of SIS into the IACS, the safety functions of a SIS must be protected from other systems, e.g. BPCS communications. This requirement is unique in that a security standard takes the initiative to specify the network design from a safety perspective as well. The security barrier concept of zones is meant to substantiate service provider claims to fulfil this requirement.

2.2.3. *Security products spanning different networks and zones*

Vulnerabilities in additional security barriers, e.g. those found by Ormandy (2015) in security products, might actually decrease the overall security posture. Security products and the companies supplying them are attractive targets due to the likelihood of obtaining access to all information or root-level privileges through just one successfully exploited application as described by Fishman and Marquis-Boire (2017), thereby traversing multiple security barriers. Broadening the coverage of an individual barrier and therefore maximizing the recovery options could be called defense in breadth as used by Kewley and Lowry (2001) to complement defense in depth. This can be interpreted as a call for quality in security systems, because functions implied to be centralized across the IACS architecture related to Security Incident and Event Management (SIEM, mentioned among others in IEC 62443 SR6.1 Audit log accessibility, SR6.2 Continuous monitoring) are potential weaknesses affecting multiple barriers. The exploitation of e.g. syslog packet forwarding across multiple IACS networks would lead to a CCF in safety analysis parlance.

Concepts of statefulness can become problematic at higher SILs with concurrent high Security Program Ratings. Stateless software constitutes a linear control system and has a positive safety connotation (in C.2.12), being highly recommended for SIL 4. But, staying within the bounds of our previous example, communication to ensure that syslogs are analyzed and correlated centrally would require a stateful protocol (typically TCP instead of UDP) and a corresponding stateful firewall. The overall architecture then runs stateless applications for control but stateful applications or services for security communications.

2.3. *Discussion of a possible unified barrier concept*

The motivation for conceptualizing a barrier concept that unifies security and safety barriers arises from our objective (i) above. For accident and security threat progression to be modelled in complex environments like those encountered in the energy industry, we need to consider the security threats facing safety systems and safety hazards disabling security systems. We propose modelling in terms of adjacent barriers to improve the engineering workflow of future high-integrity plants. The safety barrier classes and performance criteria as clarified by Sklet (2006) are also applicable to cybersecurity barriers. Among the different classifications available, we recommend those by Hollnagel (2016) due to the attention devoted therein to the barrier interrelationships. The quality criteria for adequacy, availability, reliability, robustness and specificity allow for a unified treatment if specific requirements for their application in security systems can be formulated.

Barrier monitoring is a central issue in both security and safety. Whereas higher diagnostic coverage is always a positive aspect in IACS functional safety, security often focuses on the integrity (or breadth) of an individual barrier and uses the diagnostics in different context. Diagnostic interfaces and services are mentioned as potential vulnerabilities that need to be secured,

[c]The Regulatory Control Network here as well as in IEC 62443 is to be interpreted as the first network above the field devices and buses, including networked devices such as PLCs and the SIS. It typically uses a different protocol from the Process Control Network and therefore has to be connected to the latter via a gateway.

an example being Joint Test Action Group (JTAG) diagnostics for integrated circuits. The JTAG interface is used by most chip manufacturers and can give rise to security breaches as demonstrated by Skorobogatov and Woods (2012).

Anomaly detection can possibly cover both failure diagnostic and intrusion detection, but the derivation of realistic statistics to quantify e.g. true positive vs. false positive ratios is less consolidated in the security sphere. The limited confidence in effectiveness as reported by the Australian DoD Signals Australian DoD Signals Directorate (2017) is purported to be due to the abundance of detection evasion methods.

One of the difficulties in proving the efficacy of a barrier concept for both functional safety and cybersecurity applications is that most barriers are active. For engineered barriers in general, reliance on electric power as opposed to natural phenomena like convection and heat transfer distinguishes between active and passive barriers. Active barriers are more difficult to document due to possible spurious actuations in safety, and possible additional vulnerabilities or blocked safety-oriented actions in security. The adoption of the active/passive distinction for barriers according to IEC 61508-7 2.6 "Fault tolerance (in Software design and development)" could be a key factor in aligning barrier concepts. Passive defensive design features would *guarantee the imperviousness to particular types of errors or particular conditions (avalanches of inputs) without the software taking any specific action.* Cybersecurity hardening and whitelisting are introducing such features as well. Proving that a spurious actuation results in a safe failure and therefore presents itself as an availability issue at the plant level is an important safety analysis task. Security analyses have yet to include the effects of spurious security mechanism activation.

3. Essential Functions

To frame the significance of essential functions for the security and safety interrelationship, we turn to the term of specificity as used by Hollnagel (2016):

(a) The effects of activating the barrier must not lead to other accidents.
(b) The barrier shall not destroy that which it protects.

These criteria are especially important in a barrier system consisting of active, electronic security and safety barriers, because the security barriers should not hinder the execution of safety functions and vice versa.

We therefore investigate the definition of essential functions in the different sources from a security and safety perspective. An essential function is one that should be implemented in order to provide an acceptable level of safety. Such prescriptive statements of standards should be investigated in particular because in case they contradict, e.g. security and safety standards call for different behaviours, the implementation consistency and the meaningfulness of compliance can suffer.

3.1. *Essential Functions from a functional safety perspective: IEC 61508*

Essential functions are not defined in any of the seven parts of IEC 61508 but should be understood as relating to all of safety and therefore all of IEC 61508. But IEC 62443 realizes that there are necessary functions within the IACS that have to provide sufficient process reliability for continuous operations. This is why IEC 62443-3-3 defines essential functions as those *required to maintain, health, safety, the environment and availability for the equipment under control*. IEC 62443 defines every safety-related aspect as essential, therefore all topics covered by functional safety should be essential. This includes Safety Instrumented Functions (SIF), control functions and the ability for the operator to view and manipulate the equipment under control. The latter sub-set forms the interface to human factors and situational awareness from a safety perspective.

Therefore all topics covered by IEC 61508 should be considered essential.

3.1.1. *Essential safety conditions*

Despite no direct semantic mapping from the IEC cybersecurity definition beyond the use of the word *essential*, the following provide an example for the non-application-specific requirements. These generic requirements can be independent of security considerations or can strengthen those. It is interpreted as a requirement towards the security barriers that they do not hinder these conditions.

Entry 3a in Table E.2 in part 6 of IEC 61508 specifies that IACS should have dedicated PLC program ladder logic to test what it calls essential safety conditions. Each of these conditions, although not explicitly defined, cover engineering techniques that are beneficial beyond safety to ensure security as well:

(i) Checking of data range:
Data range checking can preempt intentional memory corruption, and is therefore advised by e.g. Plakosh and Seacord (2005) as a way to eliminate security vulnerabilities.
(ii) Watch-Dog timer:
Watch-Dog timers can also be used as a security mechanism to protect against some types of Denial-of-Service attacks, as proposed by Stajano and Anderson (2000).

(iii) I/O, communication:
The interpretation of I/O and communication in the functional safety context is driven by 7.4.3 "Requirements for software architecture design" of IEC 61508-3 point e): design features are to be selected for maintaining the safety integrity of all data. Integrity is typically the highest priority security objective in IACS in hazardous industries. Message authenticity (i.e. the message originated from a trusted entity) implies message integrity. Message authenticity is usually achieved through use of a MAC (message authentication code), while confidentiality is achieved through the use of encryption. Bellare and Namprempre (2000) consider ways of combining the use of a message authentication code and encryption, known as Authenticated Encryption. As noted in their paper, encrypting the message first, and then computing the MAC is recommended.

3.2. *Essential Functions from a cybersecurity perspective: IEC 62443*

IEC 62443 defines every safety-related aspect as essential. The security barriers or boundaries therefore have to be implemented in a way that guarantees the availability of essential functions and services. The standard uses the analog terms essential functions and services, where no differentiation is apparent.

3.2.1. *Ramifications for IDS/IPS Configuration*

IEC 62443 recognizes the supremacy of essential functions to security measures for IACS. It follows that Intrusion Detection Systems (IDS) or Intrusions Prevention Systems (IPS, usually differentiated from IDS by configuration), should be configured to "block" or to "prevent" only in exceptional cases. Furthermore, Knapp and Langill (2014) caution that IDS should normally be bound to the IACS network as a tap or span port, so as not to introduce latency with an inline solution.

3.2.2. *Ramifications for Access Control*

In requirement SP.09.02 of IEC 62443-2-4, security-oriented measures are limited voluntarily to allow the asset owners to set never expiring:

(i) auto-login
(ii) operator accounts
(iii) services

This commonly happens by configuring a root account for the authorized users. For keeping up essential services, the cyber risks emerging from this are accepted and further mitigated according to the outcome of risk assessments as instructed by SP.03.01. The reliance on a multitude of never expiring essential services can therefore increase the attack surface. As the risk assessments have to be done by a third party, countermeasures might be specified.

The failure of a certificate authority in a public-key infrastructure, according to requirement SR 1.8 of IEC 62443-3-3, shall not interrupt a high-availability control system. This requirement relatives the usefulness of encryption in SIS beyond the latency considerations. Cryptographic techniques in IACS, like asymmetric and symmetric cyphers (implemented as digital signatures and MAC, respectively) might be more important for integrity than for confidentiality reasons.

IACS operating in degraded modes anticipated in the design are supposed to provide essential functions in case of compromise or intentional system isolation due to suspected compromise. The degraded IACS that still ensures essential functions constitutes a parallel to fail-safe functions in safety. When viewed in a security barrier framework, this also means that SIFs need to be maintained if security zone boundary protection initializes island mode or fail close[d]. SIF implementation remains a challenge when considering possible SIS architectures relying on cloud or fog computing, and might further complicate the achievement of safety goals when using artificial intelligence in a security-informed IACS environment (C.3.9 in IEC 61508-7).

3.2.3. *Contingency planning*

In the *A.3.4.5.2 Planning phase* contingency planning is discussed with a focus on incident response. One of the prescriptions is that procedures are needed for *separating the IACS from all nonessential conduits that may provide attack vectors, protecting essential conduits from further attacks* so that recovery activities can start. Nonessential conduits are typically those above the DMZ.

3.2.4. *ISO/IEC 62443-2-3 Patch Management*

In *B.5.4 Impact, criticality and risk assessment* a list of questions details what the asset owner should consider. The device to be patched is to be investigated: is it essential to normal operations? This question and others should be answered in a risk assessment specific to the individual security patch involving system administrators, cybersecurity staff, IT, control system suppliers, contractors, engineering and operations. Summoning such broad support can be time-consuming, but

[d] Island mode is the capability defined in IEC 62443-3-3 as the prevention of any communication through the control system boundary. Detection of a security violation in any zone may necessitate the use of it. Fail close will aim for the same results, but due to natural or operational failure of the security devices.

brings together the organizational functions that are jointly responsible for safety and security. This opens avenues of cooperation for considering the safety effects as well.

4. Discussion

Both IEC 61508 and IEC 62443 avoid an interpretation of essential functions or services and do not relate these to the physical process apart from the safe state. IEC 62443 defines essential services only implicitly and in an organizational context, meaning that committees or expert panels should judge the essential nature. Requirements placed by IEC 62443 on essential functions put additional responsibility for avoiding problems regarding availability and integrity of SIFs on staff with core competence in security. Asset owners pursuing compliance might therefore have to invest time and resources in the safety development process and in their security program to document their essential functions. The resulting technical specifications could then be co-engineered. We can conclude that essential functions have a broad definition that potentially includes most functions of a typical IACS used in a critical infrastructure. It follows that support for essential functions as safety-oriented security constraints will have large consequences during the whole IACS life cycle.

Given the examples of security attacks in the past where ICS have been affected, it seems difficult to foresee that functional safety is achieved without considering measures against security attacks. It is therefore reasonable to assume that the application of IEC 61508 will always require vulnerability analysis to be carried out in order to specify security requirements. However, the advice to carry out a vulnerability analysis in the lifecycle "hazards and risk analysis phase", which takes place before it is determined which functions to realize by E/E/PE technologies, seems to be inadequate. The experiences of Gran et al. (2017) from the industry also show that addressing security is hard.

The remote operation of high-value and high-risk assets is gaining traction, with the prime motor being economy, but also personnel safety. This provides important study cases for security and safety. The remote setting compels the integrated treatment of security and safety insofar as any human interventions, be they safety-oriented or cybersecurity attacks, are likely to happen remotely. Co-engineering these two disciplines in IACS therefore seems unavoidable.

Although the sources used here are IEC norms, our takeaway messages are relevant for authorities and enterprises seeking to address growing ICT security concerns within an existing safety regulatory framework. If security is regulated by applying existing safety regulation, as is the case for Norwegian Petroleum Safety Authority, the implications for cybersecurity compliance need to be verified. Compliance to safety regulation through cybersecurity programs will remain a challenge in establishing common vocabulary and assumptions, e.g. between regulators and asset owners.

The MERgE project by ITEA2 (2016) had this focus and produced a freely available IACS security and safety software modelling tool. The systems-theoretic safety analysis method (STPA), originally developed by Ishimatsu et al. (2010) for the aerospace domain, was expanded with STPA-SafeSec by Friedberg et al. (2017) to provide coverage of security issues. We can assume that trade-offs between functional safety and cybersecurity sometimes become necessary in many IACS, e.g. due to shared resources in concurrent processes, but the absence of normative or even informative sources describing the integration gives rise to questions on the engineering level that are not straightforward to resolve. Lisova et al. (2019) provides a systematic literature review of the subject.

5. Conclusion

With this paper we have contributed to the understanding of control system safety and security co-engineering principles as they emerge from the analysis of state-of-the-art normative literature. We provided (i) the barrier definitions as they emerge from IEC 61508 and 62443, (ii) an explanation of the different barrier independence assumptions in safety and security, (iii) the interpretation of essential functions, and (iv) a foundation for further research into a unified safety and security barrier framework.

The analysis is high-level so as to provide practicable solutions to a wide range of industries in the process of networking their systems. Our study has shown that IEC 61508 and 62443 are applicable simultaneously to provide protection from intentional and unintentional harm to critical infrastructures. Further research will be driven by the implementation details in specific sectors. We are not aware of related work for systematically qualifying technical security barriers and intend to continue research on a universally usable barrier framework for IACS security and safety.

Acknowledgement

This paper has been written under the collaboration between the Norwegian University of Science and Technology and the Institute for Energy Technology. The research is a part of BRU21 – NTNU Research and Innovation Program on Digital and Automation Solutions for the Oil and Gas Industry (www.ntnu.edu/bru21).

References

Australian DoD Signals Directorate (2017).

Strategies to mitigate cyber security incidents. *Australian Department of Defense, Canberra*.

Bellare, M. and C. Namprempre (2000). Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. In *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 531–545. Springer.

Cherepanov, A. and R. Lipovsky (2017). Industroyer: Biggest threat to industrial control systems since stuxnet. *WeLiveSecurity, ESET 12*.

CNSS, U. (2015). *Committee on National Security Systems*. Instruction No. 4009 - Glossary.

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

Fishman, A. and M. Marquis-Boire (2017). Popular security software came under relentless nsa and gchq attacks. *The Intercept*.

Friedberg, I., K. McLaughlin, P. Smith, D. Laverty, and S. Sezer (2017). STPA-SafeSec: Safety and security analysis for cyber-physical systems. Journal Article 2.

Government of Norway (2019). *National Cyber Security Strategy for Norway*. https://www.regjeringen.no/en/dokumenter/national-cyber-security-strategy-for-norway/id2627177/.

Gran, B. A., A. Egeli, and A. Bjerke (2017). Addressing security in safety projects – experiences from the industry. In *Fast abstracts at International Conference on Computer Safety, Reliability, and Security (SAFECOMP)*.

Hollnagel, E. (2016). *Barriers and accident prevention*. Routledge.

Hydro (2019, 03). Update on cyber attack March 22.

IEC 61508 (2010). Functional safety of electrical/electronic/programmable electronic safety-related systems (7 parts).

IEC 62443 (2010, 2015). Industrial communication networks - network and system security series. Book, Geneva.

Ishimatsu, T., N. G. Leveson, J. Thomas, M. Katahira, Y. Miyamoto, and H. Nakao (2010). Modeling and hazard analysis using STPA.

ITEA2 (2016). *MERgE project report Recommendations for Security and Safety Co-Engineering (Deliverable D.3.4.4 - Part A)*. Information Technology for European Advancement.

Kewley, D. L. and J. Lowry (2001). Observations on the effects of defense in depth on adversary behavior in cyber warfare. In *Proceedings of the IEEE SMC Information Assurance Workshop*, pp. 1–8. Citeseer.

Knapp, E. D. and J. T. Langill (2014). *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*. Syngress.

Ladkin, P. (2019). *Cybersecurity in IEC 61508*. Web-page: http://www.systemsafetylist.org/4502.htm last accessed 13.01.2020.

Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy 9*(3), 49–51.

Lisova, E., I. Šljivo, and A. Čaušević (2019, Sep.). Safety and security co-analyses: A systematic literature review. *IEEE Systems Journal 13*(3), 2189–2200.

Lundteigen, M. A. and B. A. Gran (2019, May). Conference paper draft for the enlarged halden project group.

NOU (2015). *Digital sårbarhet - sikkert samfunn (NOU rapport 2015:13)*. Oslo: Departementenes sikkerhets- og serviceorganisasjon.

Ormandy, T. (2015). Fireeye exploitation: Project zero's vulnerability of the beast. Post at google project zero blog.

Plakosh, D. and R. C. Seacord (2005). Range checking. Report, Department of Homeland Security US-CERT.

Schudel, G. and B. Wood (2001). Adversary work factor as a metric for information assurance. In *Proceedings of the 2000 Workshop on New Security Paradigms*, NSPW '00, New York, NY, USA, pp. 23–30. Association for Computing Machinery.

Sklet, S. (2006). Safety barriers: Definition, classification, and performance. *Journal of Loss Prevention in the Process Industries 19*(5), 494 – 506.

Skorobogatov, S. and C. Woods (2012). Breakthrough silicon scanning discovers backdoor in military chip. In E. Prouff and P. Schaumont (Eds.), *Cryptographic Hardware and Embedded Systems – CHES 2012*, Berlin, Heidelberg, pp. 23–40. Springer Berlin Heidelberg.

Slay, J. and M. Miller (2007). *Lessons Learned from the Maroochy Water Breach*, pp. 73–82. Boston: Springer.

Stajano, F. and R. Anderson (2000). The grenade timer: Fortifying the watchdog timer against malicious mobile code. In *in Proceedings of 7th International Workshop on Mobile Multimedia Communications (MoMuC 2000), Waseda*.

Strålsäkerhetsmyndigheten (2018). Licensing of safety critical software for nuclear reactors. common position of international nuclear regulators and authorised technical support organisations. Report number: 2018:19.

Williams, T. J. (1994). The Purdue enterprise reference architecture. *Computers in Industry 24*(2), 141 – 158.

Wolff, J. (2016). Perverse effects in defense of computer systems: When more is less. *Journal of Management Information Systems 33*(2), 597–620.