Cybersecurity of Offshore Oil and Gas Production Assets Under Trending Asset Digitalization Contexts: A Specific Review of Issues and Challenges in Safety Instrumented Systems

Pengyu Zhu¹ · Jayantha P. Liyanage²

Received: 14 July 2021 / Accepted: 19 November 2021 / Published online: 3 December 2021
© The Author(s), under exclusive licence to Springer Nature Switzerland AG 2021

Abstract

Due to the rapid digitalization of offshore oil fields and production platforms, diverse technological solutions, products, and application software have begun to appear both in upstream and midstream processes raising new organizational and operational challenges. The potential effects of these digital technologies driven developments have also been generating concerns, particularly in safety, security, and regulatory terms. Both hardware and software related changes and challenges in sensitive systems such as safety instrumented systems (SIS) can expose a production asset to new forms of risks. Hence, diverse aspects of cybersecurity have gained serious attention from authorities, operators, and service providers, particularly due to increasing general tendencies of major cyber-attacks on high-risk industrial assets, as well as their significant impact on safety, production, and asset economics terms. A SIS in an offshore oil and gas production asset has a critical role towards its safety integrity level (SIL). In general, a SIS consists of specific safety assurance instruments and pre-defined safety functions that are tightly coupled to detect, prevent, or mitigate hazardous situations ensuring process safety. Under the current industrial contexts of major changes within the offshore oil and gas production sector, partly due to unavoidable commercial changes and partly due to rapid technological developments, a better understanding of the cybersecurity exposure potentials of SIS is quite important to mitigate unwanted events and incidents. Under such circumstances, this paper explores critical issues and challenges related to cybersecurity of SIS as an extended step of a research study done in collaboration with industrial partners. It assesses the current actual status, requirements in governing standards and guidelines, and identifies some dangerous failure modes of SISs that need due security-oriented attention in a continuous asset digitalisation process. Towards the end, the paper defines and elaborates in-depth on specific issues and challenges relating to cybersecurity of SIS. Moreover, it identifies and reflects on generic initial steps that can be taken for assurance of cybersecurity of SIS within offshore oil and

gas production assets to ensure necessary safety and security integrity levels under rapidly changing industrial contexts.

Keywords Cybersecurity · Safety instrumented system · Functional safety · Industrial automation and control system · Digitalization · Engineering asset management

1 Introduction

Industrial digitalization has been changing traditional practices and processes in almost all sectors during the last decades and various digitalization solutions have been moving into engineering assets. The offshore oil and gas (O and G) production sector is no exception, which has been subjected to a rapid digitalization process since the early 2000s. The introduction of intelligent oil fields concepts and the subsequent implementation of integrated operations strategies in upstream and midstream processes have brought new offshore-onshore interface technologies, enhancing remote surveillance and control capabilities while changing traditional practices. As it seems today, highly operational sensitive and regulated systems such as safety-critical systems have also been getting exposed to such digitalization processes and new solutions lately (AkerBP 2019; Equinor 2018; Liyanage 2008; Liyanage and Langeland 2009), enhancing the potential for many latent exposure conditions and active challenges in safety and security terms. Safety instrumented systems (SISs) is an integral part of the functional safety of an offshore asset, which uses multiple safety functions to protect process safety. In general, critical industrial automation and control systems (IACS), such as SISs, are equipped with main features, which are more ‘mechanical’ in nature, that are mostly initiated and controlled locally or through hardwired pushbuttons. Such conventional practices nowadays are continuously challenged exploring more cost-saving solutions and naturally trying to harness the new capabilities of ongoing digital evolution. There are some growing interests within the sector towards new fully automated inspection and testing regimes, as well as remote surveillance of critical functions and dynamic operating conditions based on real-time and online application solutions. Such a change will naturally induce a major paradigm shift towards a new safety and security regime, especially for SIS.

Over a period of decades, a sophisticated safety regime has been developed in offshore oil and gas sector to ensure safety integrity of offshore assets, based on both lessons learnt and proactive thinking. However, cybersecurity remains at the very early stages of growth despite growing concerns and increasing potentials for new cyber threats. In comparison to functional safety, the level of practical awareness and understanding of cybersecurity is said to be at a relatively lower level in the process industries (International Society of Automation 2017). Due to conventional reasons, together with quite strict safety requirements and regimes, the disciplines of functional safety and cybersecurity are often comprehended and addressed as distinctive disciplines within the offshore oil and gas production sector. Those disciplines

have their characteristics and concerns of specific nature. It is not uncommon to observe many instances where distinctive domain experts (e.g., safety specialists vs. IT specialists) are involved in a conventional silo manner, where marginal efforts have been taken to address the realities without taking into consideration the mutually influential, co-related, or integrated nature of safety and security challenges in modern industrial contexts. In general, the actual integration level across security-related core disciplines is argued to be quite limited across many industrial sectors (International Society of Automation 2017). This also implies that many sensitive issues related to digitalization risks and cybersecurity of safety critical systems can still be left unaddressed without clear knowledge or standard industrial solutions in many offshore oil and gas production contexts. Moreover, due to organizational restructuring as well as rapid technology implementation efforts that inundated the offshore sector since mid-2000s, many new operational conditions have begun to demand organizational and expert attention, for instance, on responsibility distribution patterns for performing critical tasks, testing regimes of critical systems and its connection to the overall functional safety, resilience of a safe state under unwanted or unexpected conditions, access to data of critical failure modes and thorough analysis to identify future threats, etc. This further implies that many unresolved operational and organizational challenges, due to almost two decades of continuous change processes, are still present only contributing to current uncertainties and risk profiles. Under such modern industrial contexts and growing uncertainties, this paper explores and reviews some critical issues and challenges related to SISs of offshore production assets based on available industry standards, guidelines, and current practices. It aims at highlighting general operational and functional constraints and challenges when SISs gradually get exposed to industrial digitalization. The paper also sheds some light on initial steps that can be taken to help improve current practices on cybersecurity of SIS within offshore O and G production systems under modern changing contexts. It is an extended part of a detailed research study performed on SISs in close collaboration with some industrial partners and does not represent any specific cybersecurity case review, nor is an effort to find specific solutions to a specific industrial case.

2 Methodology

The study covered in this paper in principle adopts an inductive research approach. It is a continuation of an applied research study related to data-driven decision support for SISs conducted in close cooperation with the offshore industry. The original study covered industrial contexts that gave good insights from operational, technological, and service-related aspects on SISs. The industrial data that provided the basis could be coupled with practical industrial exposure, experience, publicly available sources, scholarly literature, as well as audit reports. The underlying research strategy was exploratory that helped much to identify various issues and challenges that the offshore O and G industry is currently facing related to safety and security in various lifecycle phases of SISs and IACS in general. Due to the sensitivity and limitations of open data that can be collected, this study does not cover any specific

safety and security-related incidents that have occurred in offshore assets in the most recent years. A qualitative approach was used with a specific focus on how novel conditions and issues arising from digitalization can potentially affect the functioning of safety instrumented systems and hence both process safety and cybersecurity.

3 Safety Instrumented Systems

A SIS is allocated as an additional protection layer when other safety functions fail to mitigate the identified risk to an acceptable level. In the O and G industry, such systems include emergency shutdown (ESD) systems, process shutdown (PSD) systems, fire and gas systems, and HVAC (Heating, ventilation, and air conditioning). SIS is a set of instrumented safety functions that is composed of initiator, logic solver and final elements.

Figure 1 shows a boundary of a typical pressure protection SIS (dotted line), which is constituted by the pressure transmitter (PT) as the initiator, PSD as the logic solver, and ESD valve as the final element. The function starts from a pressure transmitter that detects a higher pressure than its pre-defined setpoint. The transmitter sends the signal to its associated logic controller, which will initiate the closing of a PSD valve through a dedicated solenoid valve. The process enters a safe state, and the hazard is thus no longer present. In some cases, a SIS can also be initiated by human operators instead of pressure transmitters. In more traditional terms, data flow patterns in and out of SISs are clearly defined, following a hierarchical pattern inside the onsite supervisory control and data acquisition (SCADA) architecture.

In the known Purdue Model, SISs are grouped as Level 0 and Level 1 equipment. A SIS can be either preventive or mitigative. As part of the conventional process hazard analysis, the need for SISs is identified with quantitative analysis, for example, layer of protection analysis (Norwegian Oil and Gas Association 2020). For an identified risk scenario, more than one SISs can be identified if the level of risk reduction requirement is high. The unreliability of a SIS is measured in terms of

Fig. 1 Boundary of SIS, an example of pressure protection shutdown function

safety integrity level (SIL). The higher level a SIS's SIL is, the more risk mitigations it can provide.

In the process industry, SISs shall be maintained and verified in a lifecycle manner based on requirements defined in IEC 61511 (2016). For example, within pre-defined maintenance requirements, one typical activity is proof testing, which verifies that the functionality and performance of the SIS loop are according to its design specifications. In addition to this, the assumptions relating to SIS continuing from the design phase, such as demand rate and failure rate, shall be verified continuously to demonstrate that sufficient protection level is maintained throughout the lifecycle of the system. In general, SISs are part of the overall industrial automation and control systems with quite active organizations involved.

Over the last decades, the introduction of consumer electronics into the industrial control networks has been increasing as a result of digitalization and smart field trends (Wollschlaeger et al. 2017). The need for live data and control is only getting stronger in this new era in almost all industrial sectors. The offshore O and G industry is no exception, and it has been seeing the increasing need for more dynamic connectivity, especially in the background of integrated operations, distributed computing, and remote control.

4 Cybersecurity of Safety Instrumented Systems

Over the years, the domain of cybersecurity has grown into many industrial contexts and sectors generating an abundance of terms and concepts (Zhu and Liyanage 2020). In a generic sense, information security is expected to cover the security of both data and information. However, due to growing industrial activity level on the subject, other terminologies can also be seen in use in various contexts, for instance: physical security, cybersecurity, network security, cloud security, information and communication technology (ICT) security, operation technology (OT) security, and IACS security. Each concept has its scope and focus and covers issues that overlap more or less with information security.

4.1 Status Quo and Changing Context

The widely acknowledged ISO 27000 series defines information security as the “*preservation of confidentiality, integrity and availability of information*” (ISO/IEC 27000 2018, p. 4). This definition reveals the classic security objectives which are often described as the ‘CIA triad’, i.e., confidentiality, integrity and availability. In addition, ISO/IEC 27000 (2018) also suggests some other security objectives namely: authenticity, accountability, non-repudiation, and reliability.

In the domain of industrial automation and control systems, cybersecurity is defined as “*actions required to preclude unauthorized use of, denial of service to, modifications to, disclosure of, loss of revenue from, or destruction of critical systems or informational assets*” (IEC 62443-1-1 2009, p. 15). Addressing issues of cybersecurity, Von Solms and Van Niekerk (2013) point out that cybersecurity

covers a wider scope compared to information security in terms of failure impacts, e.g., assets and personnel safety. Critical safety measures related to industrial control systems, such as SISs, are often implemented as automatic systems, with remote control and operation functions. In addition, a comprehensive understanding of data and information flow is also becoming more and more critical to cybersecurity and safety. Moreover, with the growth of industrial ICT networks and digital data-sharing practices, there should also be sufficient independence and resilience from potential network related shortfalls, for instance as recently underlined by Balador et al. (2018) and Norwegian Oil and Gas Association (2016).

In terms of security objectives, they are defined in industrial control systems, in a quite similar manner to the classic information security, but with different priorities. For instance, availability is often prioritized in the industrial control systems domain, whereas confidentiality is seemingly more preferred in the information security domain. Adding more momentum to this current situation, there are also ongoing discussions in standardization organizations on identifying more representative and additional security objectives for industrial control systems, within specific domains such as industrial asset management and incident management.

Cybersecurity of industrial control systems is multidisciplinary and involves multiple stakeholders, including operator companies, vendors, service providers, authorities, adversaries, and sometimes the public. The complexity of managing cybersecurity requires a lifecycle approach and an effort across the whole supply chain. In the accelerating asset digitalization context, new threats and vulnerabilities are emerging daily (Haber and Zarsky 2016; Humayun et al. 2020; Iaiani et al. 2021). Cyber-attack incidents of industrial processes are exposed and reported more and more often in mass media. The cybersecurity community is working ever closer together to fight against the rising trend, especially in the era of the ongoing global pandemic of COVID-19 (Carrapico and Farrand 2020; MITRE ATT&CK 2021; National Institute of Standards and Technology 2018). Most companies operating safety critical control systems in the offshore O and G industry perform security risk assessments, either on a high level or detailed level. Commercial cybersecurity solutions often find their paths into the management of cybersecurity risk, such as threat intelligence and intrusion detection systems (Samtani et al. 2020).

4.2 General Regulations, Standards, and Guidelines Applicable for SIS

In principle, the IEC 62443 series of standards provides the main reference and defines the overall framework to secure IACS. The standard series is still under development, at the time this paper is written, and currently includes 10 normative standards and 4 technical reports. The mandatory standards shall be followed to demonstrate compliance and the technical reports have proposed guidelines and practices. The standards are arranged in four groups so that different players in the supply chain can identify the relevant standards to use (IEC 62443-2-1 2010; IEC 62443-3-3 2013; IEC 62443-4-2 2019).

In addition to the IEC 62443 standard series, several industry guidelines and frameworks have also been developed, focussing on implementation of cybersecurity

in IACS. The Norwegian Oil and Gas Association (2016) released guideline 104, giving practical recommendations on the implementing information security baseline requirements. DNV-GL (2017) published a guideline for implementing IEC 62443 in the O and G industry sector, as part of the outcomes of a joint industry project constituting regulatory authorities, operator companies, and technical service providers. Moreover, The International Society of Automation (ISA) also published a technical report to explain the implementation of cybersecurity in the functional safety lifecycle (International Society of Automation 2017). Furthermore, The National Institute of Standards and Technology/NIST (2018) proposes a cybersecurity framework (CSF) constituting of five steps: identify, protect, detect, respond and recover from a security incident. The CSF approach provides an effective framework for the simple integration of various standards, guidelines, and practices within the domains of industrial asset management and cyber risk management.

As part of regulatory activities, Petroleum Safety Authority (PSA) Norway performs various audits that cover the use of industrial information and communication (ICT) systems (Petroleum Safety Authority Norway, Norwegian Environment Agency, Norwegian Directorate of Health, Norwegian Food Safety Authority, and Norwegian Radiation and Nuclear Safety Authority 2019b). It has suggested that operators should use Norwegian oil and gas association (NOG) guideline 104 (2016) to protect against hazards related to industrial ICTs (Petroleum Safety Authority Norway, Norwegian Environment Agency, Norwegian Directorate of Health, Norwegian Food Safety Authority, and Norwegian Radiation and Nuclear Safety Authority 2019a). Concerning the O and G production, PSA requires that operators shall report hazards and accidents, which impair safety-related systems (Petroleum Safety Authority Norway 2017a).

5 Issues and Challenges Related to Cybersecurity of SIS

Since the last few years both the importance and attention towards cybersecurity have begun to increase in greater scale among major stakeholders inclusive of, commercial, political, authoritative, as well as public sectors. The general tendency is to focus, address, and resolve diverse insecure conditions and pitfalls in technical IT terms closing weak spots and designing preventative and mitigative technical barriers. However, more recent publicly known incidents related to cybersecurity have begun to underline the sensitive role of non-technical elements within industrial systems and organizations that can create various latent as well as active unsafe conditions against the protection of safety critical systems (Norsk Hydro 2019; Di Pinto et al. 2018).

The general practice related to SIS in the offshore sector is based on decentralized roles and responsibilities across four principal disciplines, namely mechanical, process, automation, and safety. The current development within cybersecurity simply adds the fifth discipline, i.e., IT, to the existing structure. A clear effect of the digitalization trend is that operational technologies (OT) gradually begin to play a major role in the existing IT infrastructures towards SIS. Many digital products and remote services with advanced functional attributes raise interests of major offshore

operators particularly when oil and gas production platforms move towards hybrid or unmanned operating modes. This simply indicates early signs of a forthcoming change in the industrial safety paradigm of SIS in the new era, where both safety and security attributes display much stronger interdependencies. Under such change-oriented contexts, some principal issues and challenges related to the cybersecurity of SIS are defined and discussed (also see Fig. 2) in this section.

5.1 Governing Standards and Regulatory Frameworks

Given the nature and the complexity of cybersecurity related matters, both standard development organizations and regulatory authorities appear to be lagging, in comparison to aggressive developments of conditions that can be exposed as potential threats. Both the lack of strong expertise and comprehensive understanding of novel conditions seem to have contributed to the current state of limited know-how and know-what to a large extent. At the same time, due to the growing commercial and political sensitivity of the subject matter, many voluntary and commissioned expert groups are involved in diverse capacities to develop suitable guidelines, standards and frameworks to resolve general threats and insecure conditions. As it seems this has led to a diversity of solutions, but from different technical perspectives, trending towards a unique situation that many users can identify as overwhelming. In relation to SIS, three specific conditions immediately emerge as challenges under the present conditions:

- a. The slow pace of growth of regulatory specifications in national and local contexts. In the European Union (EU) context, the NIS Directive (2016) plays a vital role as the first EU-wide legislation on cybersecurity. In the Norwegian offshore industry, the safety authority is leading a series of studies understanding the complexities and robustness of industrial communication systems (Lars et al. 2018; Petroleum Safety Authority Norway 2020b). However, the authority has

Fig. 2 The diversity of cybersecurity attributes of SIS in offshore oil and gas sector

not yet defined mandatory regulations other than proposed guidelines in the areas of concern (DNV-GL 2019).

- b. There is a large diversity of currently available standards, frameworks, and guidelines from standard development organizations and expert groups both internally and locally (DNV-GL 2017; IEC 62443-2-1 2010; IEC TR 63069 2019; International Society of Automation 2017; ISO/IEC 27000 2018; MITRE ATT&CK 2021; National Institute of Standards and Technology 2018; Norwegian Oil and Gas Association 2016). They are not specifically well-coordinated or integrated into the existing process safety management, which directly challenges users in terms of; clear reference, commitment of resources, and implementation efforts.
- c. Standards and guidelines do not reflect on the interdependencies among different disciplines working on the safety instrumented systems. Despite that cybersecurity is a multi-dimensional subject, there is still a major lack of an integrated approach for process safety and cybersecurity risk assessment. IEC TR 63069 (2019), for instance, proposes an initial framework for functional safety and cybersecurity, but a pragmatic guideline is still missing.

5.2 Risk Intelligence

Cybersecurity is a relatively new domain for many professionals and industrialists, and the subject matter has many familiar and unfamiliar facets. Due to its multifaceted attributes, it appears that the classical risk analysis and management practices can only generate limited insights into the real dynamics and complexities of securities in the digital domain. Current knowledge related to sophisticated attacks and state of growing concerns of affected organizations, strongly underlines the urgent need for timely consideration of a smart and innovative, as well as more comprehensive, risk management regime specifically targeted towards safety systems. In effect, potentially complex exposure profiles of SIS demand a higher degree of risk intelligence, than the current risk analysis and management practices allow, to implement new countermeasures and to reduce exposure levels (IEC TR 63069 2019; Zhu and Liyanage 2020). In essence:

- a. The nature of diverse attacks, their sophisticated nature, and the latent conditions exploited as attack interfaces, have made it quite challenging to map the dynamic risk and its stochastic nature (Albright et al. 2010; Humayun et al. 2020). Compared to traditional process safety risks, cybersecurity related risks are not deterministic and constantly change due to the ever-changing external threat picture, making it even challenging for discipline engineers to monitor the risk level and barrier functions about cybersecurity.
- b. Security-related data naturally claims for an extremely high degree of sensitivity. This has resulted in major practical limitations in sharing data related to historical events and incidents related to cybersecurity in most cases. Moreover, there is a lack of real data of threats and attacks relevant for specific safety systems equipment. The evaluation of security levels is performed with qualitative requirements

- (IEC 62443-3 2013). Practically, this makes it hard to justify if sufficient measures have been implemented and if an adequate level of protection has been achieved.
- c. Data flow in industrial automation and control systems are becoming more dynamic with the development of electronic and telecommunication technologies, such as edge computing (Stankovski et al. 2020; UcedaVelez and Morana 2015). Data flows are no longer following hierarchical or linear patterns as described in the classic Purdue model. The complexity of data flows thus makes it challenging to identify the vulnerabilities and to perform risk assessments. There are tools available in the market that can help map data flows, but the criticality of data flows can only be truly understood by a multidisciplinary team.
 - d. The majority of countermeasures taken up until now have much focus on preventive measures, with relatively little focus on mitigative measures, such as emergency response and recovery (IEC 62443-3-3 2013; National Institute of Standards and Technology 2018). Publicly known incidents and events have indicated that cyber-attacks have varying attributes, purposes, and mechanisms. For instance, some high-profile attacks have shown that malware/ransomware can hide their traces for quite a long time before the attacks occurred (Albright et al. 2010; Norsk Hydro 2019). Such unfamiliar dynamics make the detection of breaching/attacks, a very challenging task.
 - e. The limitations of general security regime implementations, the level of inconsistencies of local measures, as well as lack of expertise and organizational attention, have contributed to increased vulnerability levels (Haber and Zarsky 2016; Simon and Omar 2020). For instance, the extended supply chain of organizations (e.g., technology and service providers, and engineering contractors) who have shared data platforms and applications can increase exposure patterns through existing and new data communication nodes.
 - f. The core disciplines related to SIS and cybersecurity in most cases still operate with traditional silo practices. The traditional approach naturally introduces considerable limitations to the understanding and knowledge of the holistic risk profile under dynamic conditions. More specially, cybersecurity related risks are heavily affected by external threat factors, making it more demanding and challenging for discipline engineers to monitor, evaluate and respond to the evolving risk landscape with regard to SIS and IACS in general (Humayun et al. 2020; UcedaVelez and Morana 2015).
 - g. Some commercial cybersecurity solutions claim to be capable of risk management, despite that, a product, such as threat intelligence, intrusion detection or patch prioritization, is only part of the overall risk management. Companies should not rely on a few high-profile countermeasures to identify and manage various cybersecurity risks, despite that such solutions can sometimes provide timely inputs on external threats (Narayanan et al. 2018). More importantly, the interrelationships between process safety and cybersecurity are complex and can change over time due to, for example, process safety systems in degraded or deactivated mode as a result of ongoing maintenance activity. Multidisciplinary approaches are more important in comparison to the use of stand-alone commercial solutions.

5.3 Barrier Design, Continuous Revision, and Management

In general, barriers play a very important role in the safety integrity of industrial systems. Safety instrumented systems are equipped with technical, operational, and organizational barriers. Current digitalization trends, which also has begun to influence SIS, raises a principal need for a complete review and re-design of traditional barriers and the development of up-to-date techniques for improving barrier performance monitoring and management practices.

5.3.1 Technical Issues

The technical issues related to cybersecurity of SIS arise due to the active use of various digital programmable devices/systems, shared data, remote sensing, etc., which are necessary conditions for remote surveillance and support towards both upstream and midstream processes. A recent audit done by the Petroleum Safety Authority Norway (2020a), revealed that no significant deviation was apparent from the supervisory areas related to cybersecurity of IACS, which reaffirms that the O and G industry, in general, has a clear focus on securing IACS systems, and in particular SIS. Some of the main issues of interest here include:

- a. Unprotected user accounts and/or poor password control. In general, user access control, as a passive protection measure, has a critical function towards security. A recent report on cybersecurity by SINTEF (Lars et al. 2019) points out that preventing unauthorized access is a major challenge due to the presence of many shared user accounts in older IT/Data systems.
- b. The gradually increasing need for remote access (write-access) and remote support (see for instance Lars et al. 2019; Liyanage 2008; Liyanage and Langeland 2009; Zhu 2020), generates a clear trend towards more digital work processes with several access points from a common digital and data platform. As underlined by Albright et al. (2010) and Norsk Hydro (2019), regarding some of the recent incidents, external unauthorized access can occur with severe safety and financial consequences.
- c. Obsolete operating systems are still in use due to many practical reasons in many offshore assets. Though there are clear arguments that historical lifecycle data stored in those systems do have a considerable value for analytical purposes, those obsolete systems can suffer from a lack of vendor supports or delayed firmware upgrades. This can potentially lead to degradations of both safety and security levels.
- d. In the functional safety domain, the safety integrity level (SIL) measures the unreliability of a SIS as a risk-reducing safety function. In cybersecurity risk assessment, security level (SL) measures the confidence level that an industrial control system can survive from external threats and vulnerabilities (DNV-GL 2017; IEC 62443-3-3 2013). SL does not directly reflect how reliable a counter-

- measure is. The evaluation of the sufficiency of protection is rather qualitative and requirements from IEC 62443-3-3 (2013) are too ambiguous for simple execution.
- e. Due to the sensitivity of the technical data related to threats, vulnerabilities, and cyber-attacks on safety functions, there are practical difficulties for sharing cases and experiences. Because of that, it is practically challenging to accumulate, extract and organize relevant evidence from historical data in a systematic manner to analyse if sufficient technical countermeasures have been implemented, tested, and verified from a lifecycle perspective. This can lead to a lack of understanding of how well security barriers are functioning or if there are any weak attributes.

5.3.2 Operational Issues

Safety instrumented systems in principle consist of different workflows that cover the functional lifetime of SISs. The management of functional safety of SIS follows given industry standards and guidelines, for instance, IEC 61511 (2016) and NOG-070 (2020). However, the current industry practice treats cybersecurity as a separate domain from functional safety issues. In operational terms, some main concerns include:

- a. The inadequacy of clear and standard industry guidelines for systemic implementation of cybersecurity has been raising concerns. The broadly quoted IEC 62443 standard series is more prescriptive and lacks specific details as to how things should be addressed and resolved operationally to achieve different specified security levels (SL) (IEC 62443-3-3 2013; DNV-GL 2017). Different companies may have defined and executed their internal guidelines to protect against cyber threats, but recent audits underlined that current security challenges can mostly be attributed to the lack of necessary standard guideline(s) and poor execution of companies own procedures (see, for instance, Petroleum Safety Authority Norway 2020a).
- b. Industrial observations related to security and functional safety assessments (FSA), indicates that most companies have not adequately specified suitable and necessary cybersecurity hazard analysis in their internal or external guidelines. In general, the lack of a framework for safety and cybersecurity is more apparent. Moreover, software safety specification requirements appear to have not been developed adequately to reflect on the level of maturity accomplished related to the safety and cybersecurity of SISs. As highlighted in PSA's audit reports, there is a lack of procedures and emergency preparedness to respond to a cyber-attack to mitigate its consequences (Petroleum Safety Authority Norway 2020a). A major issue of potential concern can be, for instance, the competing nature of the economy, production, safety and security objectives, as well as its implication on decision and task priorities.
- c. The digitalization and automation processes within the O and G sector allow enabling of more functions from onshore (AkerBP 2019; Lars et al. 2019; Zhu 2020). The new offshore-onshore collaborative structure introduces many sensitive changes to existing work processes that have direct effects on roles and responsibilities, workflows, competence, etc. (Liyanage and Bjerkebaek 2007).

There seems to be a lack of systematic practices for continuous assessment and re-qualification of countermeasures in the operational phase.

- d. From a lifecycle perspective, an offshore asset, systems, and equipment undergo a range of engineering upgrades and modifications. From a cybersecurity perspective, the exposure profile and threat picture are constantly changing during those modifications that raise concerns about the sufficiency of protection in different lifecycle stages. This implies that the adequacy and performance level of countermeasures need to be re-evaluated over different lifecycle phases. Companies have not yet clearly adopted lifecycle perspectives towards continuous cyber-related risk management with necessary periodic testing or verification plans on the latest measures taken.

5.3.3 Organisational and Human Issues

Various incidents that occurred during recent years, clearly underline the lack of clear organizational focus as well as under-allocation of necessary internal resources to improve the efficiency and effectiveness of non-technical countermeasures in achieving cybersecurity. There are many aspects related to organisational issues, human aspects and decision culture, which play pivotal roles in the planning, implementation, and assurance of cybersecurity. Among those influence factors, some of the principal ones include;

- a. Missing clear and consistent Cybersecurity Management Systems (CSMS) across all levels of organizations. Many organizations are at the very initial stages of developing clear communication processes and taking preventive measures. It is largely unclear as to what extent all levels and units of an organization fully understand the nature of threats, what specific preventive and mitigative measures are in place, and what risk management guidelines and strategies have been developed and implemented. While some preliminary measures may have been taken to protect against general threats, the lack of comprehensive organization-wide approaches raises major concerns.
- b. Unspecified ownership of OT/IACS Risk, changes within RACI (responsible, accountable, consulted and informed), and dynamic decision culture. Due to industrial and operational demands, a company may change the scope of remote operations, willingly or unwillingly (Lars et al. 2019). Lars et al. (2019) point out that onshore operators of IACS systems are blunt end users and may not have all necessary local knowledge of systems or have a close enough 'connection' to installations. Offshore-onshore decision processes are not always optimal, and may remain isolated from the practical workflows, designated human roles, and domain-based responsibilities. Moreover, the decision-making processes are being re-defined, which can have an implicit or explicit effect on cybersecurity. In addition to these, there is a very limited overlap between core technical and operational disciplines on safety and security. It all points to the inadequacy of current responsibility assignment matrices.
- c. Excessive trust is given to IT capabilities and external resources. Technological evolution brings diverse smart and innovative technologies and external services

for both offshore and onshore use. This increases the level of dependency on external vendors and suppliers, who can have inconsistent and ambiguous cybersecurity strategies. For instance, operator companies usually rely on selected vendors to develop and update SIS-related software due to their domain expertise. Moreover, the onshore personnel can be responsible for several installations that have different technological solutions from different vendors with varied security attributes. These conditions can subsequently increase the likelihood of human errors, potentially leading to a degradation of security levels.

- d. Gaps related to human competence and organizational control. Offshore assets and systems are subjected to the industrial fusion of OT and IT. This brings numerous challenges to an operator in terms of safety and security, due to shortfalls in thorough organizational control mechanisms and internal skillsets/know-how defined w.r.t. operational roles and responsibilities. Human interactions related to SIS and IACS in general can occur locally or remotely, through hardwired human-machine functions or other ad-hoc interfaces. Such interactions can directly affect safety and security within and without pre-defined logic during task executions as well as through other types of interventions. In achieving cybersecurity, individual skill level and knowledge are among the first layers of protection (Kobes 2017). The lack of domain-specific know-how, gaps in specific skill-sets necessary for specific roles, ill-defined inter-personal and inter-organizational communication processes, etc. introduce many latent conditions that can weaken critical safety functions and challenge acceptable integrity levels (Zhu 2020).

5.4 Change Control, Surveillance, and Systems' Resilience

Offshore assets and safety systems undergo various upgrades, modifications, and other types of technical and operational improvements. Moreover, software applications gradually begin to gain control over functional and operational characteristics. There is a continuous technological, procedural, or regulatory basis for such changes throughout all lifecycle phases. While some technical and operational changes can be executed under thorough quality control, fast-tracked implementation processes are not very uncommon due to time and resource constraints, as well as business demands. Under such rapidly changing industrial contexts, change management and quality control processes gain increasing importance from safety and security perspectives in all types of changes. For SIS, the updating/patching of IACS does not happen as often as for IT and Networks related issues. But there has to be a safe and secure process to guide decisions and tasks, for instance, based on a thorough assessment and control of when and how patching can be performed, to protect against uncertainties that can challenge safety integrity and security levels.

From the threat modelling perspective, new threats and vulnerabilities related to IACS may emerge daily. The reasons can be external or internal. External reasons include the evolving malicious technologies and services, such as ransomware as a service (RAAS). Internal reasons include the change of work procedures, network architecture, and data flows patterns. The security protection system may remain in a relatively static manner, regardless of the changing operating context.

In general, both upgrades, as well as introduction of new solutions, can have direct or indirect effects on existing defence systems and work procedures. In many instances, new protection measures would be needed to enhance safety and security levels, depending on the nature and scale of change. From such perspectives, the adequacy of current control mechanisms and strategies, as well as the effectiveness of measures implemented to ensure protection and resilience, appear to be at suboptimal levels.

5.5 Industry Specific Cybersecurity Culture

As Fig. 2 depicts, a new cybersecurity culture is an important industrial need that needs to be developed based on central attributes from different domains, beyond IT domain. The need for such a well-cultivated cybersecurity culture is immediate in all high-risk industrial sectors, such as the offshore O and G industry. Some define cybersecurity culture as a risk-reducing measure regarding possible human errors that may impair security integrity and availability (Gcaza and von Solms 2017; Uchendu et al. 2021). At the same time, Gcaza and von Solms (2017) underlined the lack of a widely acknowledged definition for cybersecurity culture and the terminology may entail different details depending on the application context. For the offshore O and G industry sector, some of the main issues include:

- a. Human factor is often considered as a weak point in the cybersecurity domain and hence the traditional approach of establishing cybersecurity culture often has a focus on raising human and organizational alertness, such as listing historical attacks that caused substantial losses in terms of economy, reputation, and so on (Gcaza and von Solms 2017). Forrester (2021) points out that though people may gain such alertness, it may happen without a comprehensive understanding of the context, which may lead to fears and false risk aversion culture. More importantly, there is a gradually growing need for a new and more in-depth understanding of what role human plays in the management of cybersecurity risks (Zimmermann and Renaud 2019), particularly in highly dynamic and demanding operational contexts.
- b. In the offshore O and G industry, an emerging need for regime change is gradually becoming apparent by more open cooperation between operating companies, asset owners, third parties, and authorities. This in turn calls for better intercommunication protocols related to cybersecurity issues and security alerts, as well as joint efforts for the development and implementation of new governing standards, regulatory frameworks, and industry best practices.
- c. More focus on common attack-safe strategies within shared data networks, particularly where active IT and OT integration takes place to enhance operational performance. This also underlines the need for dedicated industrial forums for experience-sharing and dialogue based on incidents, facts, and data. To realize the fullest benefits of such joint industrial forums, some initial industry-wide efforts are also needed to develop quality assured databases to stimulate organizational dialogue and learning. Recent studies show that historical data of IT and OT

incidents, whether leading to operation interruption or not, are lacking in terms of quantity and quality (DNV-GL 2019; Petroleum Safety Authority Norway 2020b).

6 Some Initial Steps Identified for Improving Cybersecurity of SIS

The offshore oil and gas sector have been exposed to major technological and operational changes since the early 2000s, mainly due to production and economic reasons. Such developments have also begun to influence safety instrumented systems, in terms of for instance new technological concepts with advanced functionality and performance features, online condition monitoring, and also towards the utilization of wireless communications, 5G and remote control (AkerBP 2019; Balador et al. 2018; Halgamuge et al. 2010). As aforementioned, such ongoing technological, functional, and operational changes, as well as organizational restructuring processes, introduce new potentials to generate active or latent exposure conditions that raise concerns related to the cybersecurity of SIS. A clear need under such circumstances is to take industry-wide initiatives to define steps and mechanisms to ensure safety integrity and cybersecurity related to SIS operations. Some preliminary considerations in this regard are discussed in the sections below, to generate more attention and actions towards the development and implementation of more dedicated defensive initiatives.

6.1 In-depth Understanding and Knowledge Related to Technical and Functional Performance of SIS

The offshore oil and gas industry has been actively supporting the development of new and innovative technological solutions for a couple of decades that can bring production, economic, as well as safety and environmental benefits. This has resulted in the implementation of diverse solutions from upstream to downstream processes, which possess unique data-driven and inter-dependent characteristics. Under such new conditions, it is essential to understand how overall safety can be affected by the growing scale of connectivity through new industrial data platforms and business-to-business partnerships, and what consequences a cybersecurity incident in any node of such inter-connected industrial systems may bring to asset integrity, personal safety, and environment. This calls for a better and thorough knowledge of how the technical and functional performance of critical systems are affected implicitly and explicitly with new smart and remote solutions. In that regard, new digital skills, competencies, and know-how of operating crew and lead professionals are critical to ensure that up-to-date initiatives are taken to strengthen principal defensive and protective features of SISs. This in turn will help improve core reliability, availability, maintainability, and supportability characteristics of such systems under new developments, and at the same time to ensure that safety and security levels are not compromised.

Increasing focus on safety integrity and the need for new preventative measures to safeguard against new safety risks have resulted in some new interests lately on both fault and failure diagnosis processes related to safety critical systems and equipment of offshore assets. As a part of such new developments, critical failure modes of SISs have been focussed and studied more in-depth by many (ANSI/ISA 2017; ISO 14224 2016; Zhu 2020) to gain more knowledge and understanding on underlying technical and functional performance characteristics. In traditional process hazard analysis, various safety functions are implemented, to prevent and mitigate the consequences of dangerous failures. Even though SISs are generally bounded by strict regulatory regimes, the lack of a thorough cross-disciplinary interface at the moment between safety and security domains brings unique practical challenges to the surface. The IEC 61511 (2016) approach classifies critical failures into safe and dangerous failures depending on the effects. Based on some years of industrial study related to industrial automation and control systems, this section sheds some light on how safety functions can become vulnerable to cyber-attacks and how cyber threats can affect or even disable a SIS's functionality and performance.

An overpressure protection system used in the O and G production process is illustrated in Fig. 1. Due to inherent technical and functional interdependencies, some SISs may have connections with other SISs as well as with designed-in human-machine interface (HMI) elements that for instance share a common communication facility, either through dedicated internal or external systems using regular organizational IT networks (Zhu 2020; Zhu and Liyanage 2020). Such conditions, subsequently not only add complex safety and security attributes but also make the overall situation relatively more vulnerable to external digital threats.

In more traditional terms, process hazard analyses such as hazard and operability (HAZOP) are performed to evaluate critical risks and available safeguards. In most cases, process risk assessments do not cover cyber scope, in terms of threats, vulnerabilities and consequences. However, these process control systems are not isolated from the industrial control networks. On the contrary, the data flows from low-level processes to wide area networks or enterprise networks are becoming more dynamic and no longer follow the hierarchical flow as defined in Purdue Model (UcedaVelez and Morana 2015).

The physical processes and safety guards in relation to process risks can be vulnerable to cyber threats, such as unauthorized access and control of safety systems. To better understand active or latent conditions and performance patterns, an effort was made to perform a pre-emptive failure analysis to reveal the interdependencies between process and cyber aspects of a system, as shown in Table 1.

In Table 1, examples of dangerous failure modes of ESDs were identified. These specific modes were derived based on an initial consideration of different process hazards and cybersecurity situations. For an ESD system, 'fail to close' is one of the most dangerous failure modes to avoid. The root causes for such unwanted conditions can vary from hardware reliability issues to an unauthorized change of system's attributes due to the weaknesses or failure of countermeasures. There is a possibility that the inhibition of ESDs can be initiated internally based on wrong information received from remote access, or simply due to human errors (Di Pinto et al. 2018). Such unauthorized control of systems, or even creating conditions that

Table 1 Cybersecurity situations and pre-emptive failure analysis of an ESD system (Adapted from Zhu and Liyanage 2020)

Scenario	Threat/event	Weakness/vulnerability	Impact/failure modes	Failure classification	Other safety functions	Security countermeasures
High pressure in vessel	Valve solenoid stuck	Hardware reliability	Fail to close	Dangerous	Basic process control system (BPCS) Pressure safety valve (PSV)	No
	Tampering with instrument setting	Insecure protocol	Fail to close	Dangerous	BPCS PSV	Physical security Authentication Threat identification Change management procedure
Process medium leak through a closed ESD valve	Debris in valve seat	Hardware reliability	Leakage through closed position	Dangerous	BPCS PSV	No
Remote access of industrial networks	Phishing Spoofing	Poor access control Poor awareness	Disclosure of critical information	Literally Critical/Practically Non-critical	No	User authentication Cybersecurity culture Fire walls
Unexpected process shutdown	Tampering with instrument setting	Insecure protocol & blind trust of instrument reading	Spurious trip	Safe	No	Physical security Authentication Change management procedure
Unauthorized change of logic programming	Malware Human errors	Zero-day vulnerability	Fail to close	Dangerous	BPCS PSV	Patching Control network segmentation
	Malware	Zero-day vulnerability	Spurious trip	Safe	No	Intrusion detection system Patching Control network segmentation Intrusion detection system

may lead to human errors, can be caused by external unauthorized access if countermeasures of cybersecurity are inadequate. The harmonization of both safety functions and security countermeasures is key in building a defence-in-depth system.

The failure analysis also reveals that the same scenario may have different failure consequences. For example, in the scenario ‘Unauthorized change of logic programming’, failure consequences can be either dangerous or safe depending on the motivations of an attacker. Dangerous failures are the least favoured in all cases, but a safe failure often means economic losses, which will put companies in a vulnerable place if a ransom is also part of the play.

In addition to the potential for security breaches due to remote control through unauthorized external access, there can be latent security vulnerabilities emerging from common data platforms and applications through which operators and service providers stay connected both online and in real-time. Such conditions as, unfamiliar layers of interconnectivity, corrupted data inputs, erroneous commands, etc. can contribute in many ways to challenge the cybersecurity of SISs. Under such new and more demanding circumstances, institutionalization and strengthening of professional understanding, knowledge, and competencies have critical roles towards ensuring cybersecurity, particularly under dynamic digital contexts.

6.2 Deploy a Holistic Cybersecurity Strategy Related to SIS

Implementation of new technical and operational solutions in upstream and downstream processes was identified as the way forward towards digital oil fields since the early 2000s. Since then, the offshore Oil and Gas industry has been subjected to different types of changes continuously targeting business benefits. However, due to the accelerated nature of change processes that assets and critical systems are exposed to, O and G companies have continuously been advised to assess diverse safety effects associated with changing practices, particularly due to growing stronger fusions between IT and OT applications. This is also a very relevant concern in cybersecurity terms, due to gradually growing digitalization projects that consequently underlines the need of a consistent strategy related to design, implementation, and quality control/assessment of cybersecurity related issues and measures.

A holistic cybersecurity strategy in principle needs to adopt an organization-wide approach both laterally and vertically, ensuring stronger and secure interfaces between traditional disciplines and business partners. Figure 3 shows some principal elements towards a holistic cybersecurity strategy for Offshore oil and gas production assets and safety critical systems.

Many organizations are preoccupied with IT-driven measures to protect and safeguard offshore assets and systems, while other issues such as organizational communication patterns, traditional silo thinking within technical disciplines, inconsistent security measures among business partners, lack of normative practices, etc. have begun to play critical roles towards the integrity of countermeasures. In the context of SIS, the following specific measures are deemed important to consider when developing such holistic defensive strategies to safeguard critical safety systems:

- Flawless integration of different generations of IACS
- Testing and qualification regime for new solutions
- The context-sensitive security profile for multiple installations
- More specific and clear industry guidelines for an integrated framework for safety and cybersecurity
- Agile alert systems and alarms across core disciplines
- Distributed cybersecurity knowledge and know-how across roles and responsibility profiles

IACS have been evolving over five major generations, through dedicated hard-wire, Fieldbus technology, ethernet-based networks, industrial wireless networks, and currently through industry 4.0 that includes applications of the internet of things (Balador et al. 2018; Wollschlaeger et al. 2017). In general terms, offshore assets comprise diverse solutions from different generations for many reasons. Hence, there are considerable compatibility challenges for the application of new solutions, particularly during the integration of existing communication networks and data models (Sauter 2010; Wollschlaeger et al. 2017). As emphasised by Sauter (2010), such incompatibilities can also exist at the automation and management level and are not always limited at the field level.

With the introduction of new IACS solutions, which also involves the use of remote access through mobile devices, the need for security analysis, testing, and qualification at diverse levels has also been growing at a steady pace. In most industrial application settings, the normative basis, compliance levels, and actual protection profiles of existing communication and data sharing networks are not unknown or unclear to other partners. This makes it difficult to practically assess and get a thorough overview of real security conditions. At the same time, the implementation of new concepts such as industry 4.0 on IACS, is bounded by the non-compromising terms and conditions about confidentiality, integrity, and availability, which in many cases act as critical obstacles for sharing security profiles. As Wollschlaeger et al. (2017) explain, one of the main ambitions of the industry 4.0 trend is the enhanced access of industrial data, through smart and portable devices and gadgets. Despite the growing use of mobile devices and web links towards sensitive data and applications, no specific guarantee can be provided that all necessary control functions and rules are enabled in such devices, under all conditions.

The offshore asset portfolios of operator companies consist of assets, systems, and equipment with highly varied operating patterns, modification and upgrade histories, lifecycle profiles, and partnership structures. This implies that even assets, systems, and equipment, from relatively comparable generation, may have different technical and operational conditions, unique communication networks, and specific guidelines that all stakeholders must manage and comply with. Moreover, the development and implementation of digital oil field concepts have taken place in different scales with varying levels and practices of offshore-onshore connectivity. Under such conditions, there is a growing interest as to how to adapt context-dependent cybersecurity practices. For instance, the PSA general audit report (Petroleum Safety Authority Norway 2017b) had emphasised that mobile offshore units often facilitate remote access provided that the access is controlled by personnel on board.

Fig. 3 Some principal elements towards a holistic cybersecurity strategy

Given the sensitivity of context-specific attributes towards overall cybersecurity of specific assets as well as overall inter-connected systems, an effective cybersecurity strategy for assets in the portfolio should also take into consideration, for example, different field development concepts, operating scenarios, technical and operational histories, regulatory regime, etc.

The offshore oil and gas sector has developed strong and mature safety traditions and regimes over decades of extensive work due to the high-risk nature of the O and G production process. However, the cybersecurity domain is at a much lower level of maturity, often kept under the IT domain where a separate set of standards, guidelines, and regulations, apply. However, with the continuous establishment and steady growth of a more open and shared industrial communication infrastructure, it has become more and more important to align and integrate safety and security requirements and regimes moving forward from classically distinctive industry guidelines and regulations. For instance, on the NCS, the Norwegian oil and gas association's guidelines have been suggested by the petroleum safety authority for managing functional safety and cybersecurity (Petroleum Safety Authority Norway et al. 2019a). According to NOG guideline 070 (2020), signal and data transmission and data flow directions should be specified to enhance security characteristics. For example, there should be no data flow from process shutdown functions to ESD systems or fire and gas systems, and there shall be an independent hardwired signal to enable manual activation of safety functions.

Finally, as aforementioned, in addition to technical and operational measures elaborated above, the establishment of a stable and sensitive cybersecurity culture within offshore oil and gas production systems has also been gradually gaining timely and practical importance. The development of such a security-minded culture has many facets that should be able to enhance both organizational and human sensitivity towards digital abnormalities and negative trends. In this regard, dedicated digital security knowledge management strategy across all levels of organizational or asset-dependent responsibility matrices, as well as a change-conscious alert mechanism of abnormal conditions and breaches play pivotal roles. This in principle should be geared to capitalize on both up-to-date knowledge regime and organizational alertness as two strong defensive measures, due to the critical and

indisputable role of the human in ensuring cybersecurity, particularly in high-risk industrial sectors, in a similar manner as that matters for ensuring a long-lasting and strong safety culture.

7 Conclusion

The paper tried to systematically explore specific cybersecurity and safety challenges that industrial control systems face in the new context of digitalization and increased connectivity, with a focus on safety instrumented systems of the offshore O and G production sector. It defined and elaborated on five principal attributes related to cybersecurity of SIS namely: governing standards and regulatory frameworks, risk intelligence, barrier design, continuous revision and management, change control, surveillance, and system's resilience, and industry sector-specific cybersecurity culture. The study explored a range of issues and challenges with regard to the management of SIS and IACS, from the cybersecurity perspective. The identified issues and challenges are not unique to one operator but seemingly are general to the whole offshore industry. The paper also emphasised the inherent complexities of key factors hidden behind the topics, as well as growing interdependencies, which generate latent effects on the safety and security of an industrial control system under modern conditions of industrial growth. The paper pointed out that it requires an industry-wide effort to improve current practices and performance levels, considering the lack of a clear, effective, and most importantly an integrated approach for the safety and security of SIS. A couple of strategic steps were proposed towards the end as initial steps towards developing a more holistic framework to manage the cybersecurity of SISs in a dynamic and complex industrial context that is subjected to rapid digitalization efforts. In such an effort, due considerations are also needed on integration levels of old and new technologies, dynamics of human involvement with different digital skill levels, digital work processes, changes in operations management systems, data and information flow patterns, and diversity of stakeholders. In general, current conditions and developments call for a change of safety and security regimes to strengthen both defensive and resilience characteristics of asset critical systems.

Acknowledgements This paper is an extended version of a paper previously presented in ESREL 2020 (Zhu and Liyanage 2020). It is a continuation of an applied research study related to data-driven decision support for safety instrumented systems (SIS) conducted in close cooperation with industry (Zhu 2020).

References

- AkerBP (2019) Ivar Aasen now operated from Trondheim. <https://www.akerbp.com/en/ivar-aasen-now-operated-from-trondheim/>. Accessed 10 Feb 2020
- Albright D, Brannan P, Walrond C (2010) Did Stuxnet take out 1,000 centrifuges at the Natanz enrichment plant? Institute for Science and International Security, Washington
- ANSI/ISA (2017) ISA-TR96. 05. 01-2017, Partial stroke testing of automated valves. International Society of Automation, North Carolina

- Balador A, Kouba A, Cassioli D, Foukalas F, Severino R, Stepanova D, Sukuvaara T (2018) Wireless communication technologies for safe cooperative cyber physical systems. *Sensors (basel)* 18(11):4075
- Carrapico H, Farrand B (2020) Discursive continuity and change in the time of Covid-19: the case of EU cybersecurity policy. *J Eur Integr* 42(8):1111–1126
- Di Pinto A, Dragoni Y, Carcano A (2018) TRITON: the first ICS cyber attack on safety instrument systems. *Proc Black Hat USA* 2018:1–26
- DNV-GL (2017) DNVGL-RP-G108, Cyber security in the oil and gas industry based on IEC 62443. Høvik
- DNV-GL (2019) Regelverk og tilsynsmetodikk (Regulations and auditing methods). Høvik.
- Equinor (2018) Joint offshore digitalisation. <https://www.equinor.com/en/news/07mar2018-joint-offshore-digitalisation.html>. Accessed 10 Feb 2020
- Forrester (2021) How to manage the human risk in cybersecurity, <https://www.forrester.com/report/how-to-manage-the-human-risk-in-cybersecurity/RES58010?objectid=RES58010>. Accessed 1 Nov 2021
- Gcaza N, von Solms R (2017) Cybersecurity culture: an ill-defined problem. In: IFIP World conference on information security education. Springer, Cham, pp 98–109
- Haber E, Zarsky T (2016) Cybersecurity for infrastructure: a critical analysis. *Fla St UL Rev* 44:515
- Halgamuge MN, Liyanage JP, Mendis P (2010) Wireless technologies for integrated e-operations in offshore environments. *EJSE Special Issue Wirel Sens Netw Pract Appl Special Issue*, 100–112
- Humayun M, Niazi M, Jhanjhi NZ, Alshayeb M, Mahmood S (2020) Cyber security threats and vulnerabilities: a systematic mapping study. *Arab J Sci Eng* 45(4):3171–3189
- Iaiani M, Tugnoli A, Bonvicini S, Cozzani V (2021) Analysis of cybersecurity-related incidents in the process industry. *Reliab Eng Syst Saf* 209:107485
- IEC 61511 (2016) IEC 61511. Functional safety-safety instrumented systems for the process industry sector. Part 1–3. International Electrotechnical Commission, Geneva
- IEC 62443-1-1 (2009) IEC 62443-1-1:2009, Industrial communication networks—network and system security—Part 1–1: terminology, concepts and models. International Electrotechnical Commission, Geneva
- IEC 62443-2-1 (2010) IEC 62443-2-1:2010, Industrial communication networks—network and system security—Part 2-1: establishing an industrial automation and control system security program. International Electrotechnical Commission, Geneva
- IEC 62443-3-3 (2013) IEC 62443-3-3:2013, Industrial communication networks—network and system security—Part 3-3: system security requirements and security levels. International Electrotechnical Commission, Geneva
- IEC 62443-4-2 (2019) IEC 62443-2-4:2015, Security for industrial automation and control systems—Part 4-2: technical security requirements for IACS components. International Electrotechnical Commission, Geneva
- IEC TR 63069 (2019) Industrial-process measurement, control and automation—framework for functional safety and security. International Electrotechnical Commission, Geneva
- International Society of Automation (2017) ISA-TR84.00.09-2017, Cybersecurity related to the functional safety lifecycle. International Society of Automation, North Carolina
- ISO 14224 (2016) ISO/TC 67, ISO 14224:2016, Petroleum, petrochemical and natural gas industries—collection and exchange of reliability and maintenance data for equipment. International Organization for Standardization, Geneva
- ISO/IEC 27000 (2018) Information technology—security techniques—information security management systems—overview and vocabulary. International Organization for Standardization, Geneva
- Kobes P (2017) Guideline industrial security: IEC 62443 is easy. Vde Verlag GmbH
- Lars B, Britta H, Øyvind D, Tor OG, Martin GJ, Marie M, Onshus T (2018) Kunnskapsprosjekt IKT-sikkerhet; Industrielle kontroll- og sikkerhetssystemer i petroleumsvirksomheten (Knowledge project ICT—security, industrial control and instrumented systems in the petroleum industry). SINTEF, Trondheim
- Lars B, Tor OG, Martin GJ, Tor Onshus IW (2019) IKT-sikkerhet – fjernarbeid og HMS (ICT security—remote work and HSE). SINTEF, Trondheim
- Liyanage JP (2008) Integrated e-operations-e-maintenance: applications in north sea offshore assets. In: *Complex system maintenance handbook*. Springer, Cham, pp 585–609

- Liyanage JP, Bjerkebaek E (2007) Use of advanced technologies and information solutions for North Sea offshore assets: ambitious changes and Socio-technical dimensions. *J Int Technol Inf Manag* 15(4):1–10
- Liyanage JP, Langeland T (2009) Smart assets through digital capabilities. In: *Encyclopedia of information science and technology*, 2nd edn. IGI Global, pp 3480–3485
- MITRE ATT&CK (2021) ATT&CK for industrial control systems, https://collaborate.mitre.org/attacks/index.php/Main_Page. Accessed 1 Oct 2021
- National Institute of Standards and Technology (2018) Framework for improving critical infrastructure cybersecurity. Maryland
- Narayanan SN, Ganesan A, Joshi K, Oates T, Joshi A, Finin T (2018) Early detection of cybersecurity threats using collaborative cognition. In: 2018 IEEE 4th international conference on collaboration and internet computing (CIC), pp 354–363
- Norsk Hydro (2019) Cyber-attack on Hydro. <https://www.hydro.com/en-NO/media/on-the-agenda/cyber-attack/>. Accessed 20 Feb 2020
- Norwegian Oil & Gas Association (2016) Norwegian oil and gas 104—Norwegian oil and gas recommended guidelines on information security baseline requirements for process control, safety and support ICT systems. Norwegian Oil & Gas Association, Stavanger
- Norwegian Oil & Gas Association (2020) Norwegian oil and gas 070—application of IEC 61508 and IEC 61511 in the Norwegian petroleum industry. Norwegian Oil & Gas Association, Stavanger
- Petroleum Safety Authority Norway (2017a) Risk level in Norwegian petroleum activities (RNNP) method report. <http://www.ptil.no/om-rnnp/category720.html>. Accessed 20 Feb 2020
- Petroleum Safety Authority Norway (2017b) Rapport etter tilsyn med aktørenes håndtering av IKT-sikkerhet (PSA general audit in 2017). Stavanger
- Petroleum Safety Authority Norway (2020a) PSA audit reports. <https://www.ptil.no/tilsyn/tilsynsrapporter>. Accessed 20 Feb 2020
- Petroleum Safety Authority Norway (2020b) IKT-sikkerhet - Robusthet i petroleumssektoren 2020 (ICT Security—robustness in the petroleum sector 2020). Stavanger
- Petroleum Safety Authority Norway, Norwegian Environment Agency, Norwegian Directorate of Health, Norwegian Food Safety Authority, & Norwegian Radiation and Nuclear Safety Authority (2019a) Guidelines regarding the facilities regulations. Stavanger
- Petroleum Safety Authority Norway, Norwegian Environment Agency, Norwegian Directorate of Health, Norwegian Food Safety Authority, & Norwegian Radiation and Nuclear Safety Authority (2019b) Regulations relating to management and the duty to provide information in the petroleum activities and at certain onshore facilities (The management regulations). Stavanger
- Samtani S, Abate M, Benjamin V, Li W (2020) Cybersecurity as an industry: a cyber threat intelligence perspective. In: *The Palgrave handbook of international cybercrime and cyberdeviance*, pp 135–154
- Sauter T (2010) The three generations of field-level networks—evolution and compatibility issues. *IEEE Trans Ind Electron* 57(11):3585–3595
- Simon J, Omar A (2020) Cybersecurity investments in the supply chain: coordination and a strategic attacker. *Eur J Oper Res* 282(1):161–171
- Stankovski S, Ostojić G, Baranovski I, Babić M, Stanojević M (2020) The impact of edge computing on industrial automation. In: 2020 19th International symposium Infoteh-Jahorina (Infoteh), pp 1–4
- The NIS Directive (2016) Directive (EU) 2016/1148 of the European parliament and of the council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC. Accessed 7 July 2021
- UcedaVelez T, Morana MM (2015) Risk centric threat modelling: process for attack simulation and threat analysis. John Wiley & Sons, New Jersey
- Uchendu B, Nurse JR, Bada M, Furnell S (2021) Developing a cyber security culture: current practices and future needs. *Comput Secur* 109:102387
- Von Solms R, Van Niekerk J (2013) From information security to cyber security. *Comput Secur* 38:97–102
- Wollschlaeger M, Sauter T, Jasperneite J (2017) The future of industrial communication: automation networks in the era of the internet of things and industry 4.0. 11(1):17–27

- Zhu P (2020) Safety instrumented systems in low demand mode in oil and gas production process: data-driven decision support for improvements in operation and maintenance practice. PhD thesis, University of Stavanger, Stavanger
- Zhu P, Liyanage JP (2020) Cybersecurity of safety instrumented systems in the context of digitalization: some issues and challenges within oil and gas production assets. In: Proceedings of the 29th European safety and reliability conference, ESREL 2020. Research publishing, Venice
- Zimmermann V, Renaud K (2019) Moving from a 'human-as-problem' to a 'human-as-solution' cybersecurity mindset. *Int J Hum Comput Stud* 131:169–187

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Authors and Affiliations

Pengyu Zhu¹ · Jayantha P. Liyanage²

✉ Pengyu Zhu
pengyu.zhu@safetec.no

Jayantha P. Liyanage
j.p.liyanage@uis.no

¹ Department of Reliability and Optimization, Safetec Nordic AS, Stavanger, Norway

² Department of Mechanical and Structural Engineering and Materials Science, University of Stavanger, Stavanger, Norway