To be presented at the 13th IEEE International Conference of Cloud Computing
Technology and Science (CloudCom 2022), Bangkok, Thailand. Copyright (c) IEEE

A Survey on Cybersecurity Barrier Management in Process Control Environments

Knut Øien, Stein Hauge, Martin Gilje Jaatun, Lars Flå, and Lars Bodsberg
Software Engineering, Safety and Security
SINTEF Digital
Trondheim, Norway
{ knut.oien, stein.hauge, martin.g.jaatun, lars.fla, lars.bodsberg} @sintef.no

***Abstract*—The concept of *barriers* is well known in the safety domain that includes traditional process control environments. However, as critical infrastructures are moving to more interconnected scenarios connected to cloud computing service providers and the internet in general, an increased focus on security is necessary. In this paper we present a survey on how cybersecurity barriers have been presented in the literature, concluding that the concept has received little attention. More specifically, the aim of the paper is to survey the state of the art in cybersecurity barrier management and the integration with safety barrier management. Like the concept of cybersecurity barrier, the integration of safety and cybersecurity barrier management has received little attention. Most of the work focus on integration of safety and cybersecurity management in general, not on barrier management specifically. We eventually aim to integrate cybersecurity barrier management into the already existing safety barrier management regime.**

***Index Terms*—cybersecurity barriers, operational technology, petroleum, offshore**

I. Introduction

In this paper, we have performed a literature review on cybersecurity barrier management (CBM) and the integration with safety barrier management. The literature was selected through searches in the Scopus database, and the time period was limited from 2015 to present. A reason for selecting 2015 is that we believe the safety barrier concept emerged within the Norwegian oil and gas industry with regulations from 2001 (latest update from 2020 [1]). However, security was not explicitly referred to by the Petroleum Safety Authority until an update of their barrier memorandum in 2017 [2]. Thus, we believe it is not likely to find the most relevant literature on cybersecurity barriers before 2017. With some margin we decided on 2015 as the limitation. Search words included: *Cyber, security, barrier, countermeasure, OT, operational technology, ICS, industrial control system, IACS, industrial automation and control system, SCADA, supervisory control and data acquisition, inventory, requirements, status, panel, monitoring, assessment, levels, rating, program, maturity, evaluation, integrated, safety, management*.

Relevant literature has been identified and selected based on a set of search strings for each task, snowballing, and screening of literature based on title, abstract and entire paper/document.

About the term barrier, it should be noted that it has both positive and negative connotations. While the term barrier could be used to denote a security measure, it is also used to denote an obstacle as opposed to a protective measure. This include barriers to sharing of cyber security information [3], barriers to developing usable and secure software [4], or barriers to using IDS in safety systems [5]. A safety barrier is defined by the Petroleum Safety Authority as ”a measure intended to identify conditions that may lead to failure, hazard and accident situations, prevent an actual sequence of events occurring or developing, influence a sequence of events in a deliberate way, or limit damage and/or loss.” Typically, cybersecurity barriers could be e.g., access control or firewalls; however, we cannot equate cybersecurity barriers with e.g., security measures. It remains to define cybersecurity barriers exactly. We will not pursue this in the present paper.

We structure the findings according to four main topics. Section II discusses identification of barriers, section III discusses assessment of barrier status, section IV discusses security levels and section V discusses the integrated barrier management of safety and security.

II. Identification of cybersecurity barriers

To what extent is the term barrier used in cybersecurity literature? Does the literature cover identification of cybersecurity barriers (or alternatively using related terms)? Does the literature point to any specific approaches for identification of cybersecurity barriers? E.g., methods providing event sequences for which barriers are needed to interrupt the attack sequence; comprehensive examples of critical asset inventory; use of kill-chains or similar; resilience approaches; etc. Does the literature cover any research that is relevant for the identification of cybersecurity barriers? We will return to these questions. However, it should be noted that our focus is the identification of already implemented barriers, i.e., not on methods for identifying the need for barriers as part of risk assessments.

Knowles et al. [6] have provided a thorough survey of approaches for measuring and managing security in industrial control system environments, including an analysis of 22 standards and guidelines.

The AI&C (Asset Identification and Classification) criteria is particularly relevant for the identification of cybersecurity barriers, especially related to an asset inventory bottom-up approach. Note that NOROG 123 [7] is one of the relatively few publications where *”guidelines are outlined for identifying and compiling an inventory of industrial control system assets and/or the provision of a methodology for classifying assets (e.g., safety critical assets)”* [6]. NOROG 123 is used by Service Integration providers in projects for the Norwegian oil and gas industry.

Before we elaborate on NOROG 123, we include some of the conclusions in Knowles et al. [6]. They state that *”guidelines vastly outnumber standards for industrial control system security”*, and that *”U.S. publications dominate in both categories”*. *”IEC 62443 is the notable exception as an international standard; however, many of the publications in the series are working drafts.”*

They further conclude that *”a widespread failure to meet the analysis criteria was found across all risk management activities, with the exception of countermeasures (met by 21 of the 22 publications)”* and that this *”create significant barriers to implementing industrial control system security in the critical infrastructure sectors.”* (Here we have another example of using the term barrier in the negative sense).

The objective of NOROG 123 [7] is *”to contribute to the improvement of the overall information security of the offshore industry on the Norwegian Continental Shelf, specifically safety, regularity and integrity of operations.”* NOROG 123 is a supplement to NOROG 104 [8], which provides guidelines on information security baseline requirements for process control, safety and support (PCSS) ICT systems.

The criticality assessment advocated in NOROG 123 is a consequence-only assessment. However, what is important in our context is what to include in the asset register (the ”OT critical assets”). Examples of criticality levels are only provided for broad systems such as Process Control Systems (PCS), Emergency ShutDown (ESD)/ Fire & Gas (F&G), Public Address (PA) system, Fiscal Metering, etc., whereas it is stated that a premise is *”a complete register of all ICT systems and communication devices installed in the production network, as well as all operational applications.”* The asset register is preferably *”a database used to register and manage all the information about systems and applications”* – the Configuration Management DataBase (CMDB). No further information on what assets to include in the register is provided.

Shilenge & Telukdarie [9] provide further information on what could be included in the CMDB, structured according to the ISA-95 system hierarchy levels.

The assets on Level 0 cover e.g., transmitters, analysers, actuators, converters, drives and wireless gateways, whereas assets on Level 1 and 2 include e.g., controllers, network servers, engineering stations, operator stations, network firewalls and network gateways. The level 1 Field Device Manager (FDM) asset data is logged through the ETL (Extracted, Transformed, and Loaded) process into the Operational Technology (OT) CMDB at levels 1 and 2. Configuration items on Level 0-2 include e.g., asset tag, status, and criticality.

Level 3 includes e.g., historian server and Manufacturing Execution Systems (MES) servers, whereas Level 4 includes e.g., IT CMDB, anti-virus server and Enterprise Resource Planning (ERP) Systems.

According to Hollis & Zahn [10], some solutions to the management of cyber assets on lower levels already exist. They refer to endpoint detection and response (EDR) as an additional layer of protection in the defence in depth strategy, due to the limitations of perimeter defences. The problem, though, with EDR in a Process Control Network (PCN) is the limited focus and coverage of cyber assets (approximately 20%).

The industrial endpoints, found in Level 0 and 1, include *”3rd Party Modules, Com Modules, Control Level Firewalls, Controllers, Foundation Fieldbus Devices, Hart Devices, IO Cards, Operator Stations, Profibus Devices, Wireless Devices, and Wireless IO Modules.”*

The problem is that *”there are no common protocols to interrogate them for configuration information”* and that *”sensitivity to process preservation drives cybersecurity decisions within a process control network. For instance, putting agents on proprietary ICS not only invalidates support, but it also violates process control engineering best practices.”*

Hollis & Zahn [10] refer to PAS Cyber Integrity as an endpoint-based cybersecurity software solution that provides *”automated inventory, configuration, patch, vulnerability, and compliance management as well as backup and recovery preparedness.”*

Although a solution, such as the PAS Cyber Integrity, can be used to detect and respond to e.g., active attackers, ICS-CERT vulnerabilities and inadvertent engineering changes, there are two crucial questions still remaining:

1) Exactly which cyber assets are captured, and which of these can be labelled cybersecurity barriers?
2) Exactly what status information can be provided?

Téglácy et al. [11] discuss diagnostic and diagnostic coverage for both safety and security barriers, as *”barrier monitoring is a central issue in both security and safety.”* They state that *”anomaly detection can possibly cover both [failure] diagnostic and intrusion detection,”* so perhaps the status information addressed in the second question above can include failure diagnostic. However, they also warn that security diagnostic is different from safety diagnostic in that diagnostic *”interfaces and services are mentioned as potential vulnerabilities”* which can give rise to security breaches.

Regarding the first question above, and also the question raised in the beginning to what extent the term barrier is used in cybersecurity literature, Téglácy et al. [11] is one of the few publications in our review that uses the term barrier (both safety and security barrier) extensively. They state that *”IEC 62443 uses boundaries as a synonymous definition to barriers.”* However, although IEC 62443-1-1 defines boundary as *”software, hardware, or other physical barrier that limits access to a system or part of a system”*, it does not mean that barriers are solely boundaries. It is stated in both Téglácy et al. [11] and IEC 62443-2-1 that barrier devices are typically firewalls, routers and layer 3 switches, i.e. they are more than boundaries. And the network segmentation itself is referred to as a security countermeasure.

It is only referred to what is ”typically” barrier devices, with a few examples, thus, the first question above still remains to be answered. We assume that also parts of what is generally termed security countermeasures in IEC 62443 can be labelled as security barriers or cybersecurity barriers.

A. Safety barriers / cybersecurity barriers – use of the terms

Apart from Téglácy et al. [11] and IEC 62443-2-1, to what extent is the term barrier used in cybersecurity literature? Is it mainly a phenomenon within the Norwegian oil and gas industry? Most standards and guidelines use other terms than barriers. What about the cybersecurity literature? Somewhat surprisingly, 20 of 71 reviewed publications (28 %) used the term security barrier or safety barrier, and 14 of 71 (i.e., 20 %) used the term security barriers. Only a minor part of the reviewed publications relates to the Norwegian oil and gas industry. Three of the 71 publications used the term barrier in a negative sense.

B. Identification of cybersecurity barriers – event sequences/attack trees, kill-chains, resilience, etc.

Attack trees, and similar security risk assessment methods, seems to have been forerunners to kill-chains. They try to model how an attacker may affect a system, and on the basis of this suggest counteractions and countermeasures. Attack tree is one of the most widely used non-state-space models for security analysis [12]. One of the publications on attack trees [13] gives a brief introduction to some of the development in the past.

This includes threat logic trees by Weiss [14], threat trees by Amoroso [15], basic attack trees by Schneier [16], extended attack trees by Moore et al. [17] and extended fault trees by Fovino et al. [18]. Further development focused on protection, e.g., defense trees by Bistarelli et al. [19] and protection trees by Edge et al. [20].

Ji et al. [13] themselves propose an attack-defense tree (ADTree), which is claimed to provide *”an effective means of risk assessment and countermeasures evaluation in the evolutional process of security management for cyber-physical system security.”*

Cook et al. [21] include the use of kill-chains as part of their ”cyber defense triage process”. They state that *”there are many ways to express an antagonistic cyber-attack. Two commercial methods were considered during this analysis; the Lockheed Martin ’Kill-Chain’ [22] and the Mandiant Attack Lifecycle [23]. Both techniques fitted within the process, but in this example, we used the Mandiant method, as the ’Weaponization’ phase of the Lockheed Martin model would be opaque to a defender. The Mandiant lifecycle comprises eight stages.”* This is quite similar to the Course of Action Matrix based on the original Lockheed Kill Chain Model [22].

It should be noted that the methods referred to above are used as part of risk assessments to identify the need for ”cybersecurity barriers” (or countermeasures). They are not methods for systematically identifying existing cybersecurity barriers. In order to monitor and manage the cybersecurity barriers – similar as for safety barriers – we need to identify the ”inventory of cybersecurity barriers”. It is not within the scope of this paper to identify the need for and select necessary cybersecurity barriers. With ”existing”, we do not only mean brownfields; it can also be greenfields, but after the stage that cybersecurity barriers have been chosen.

None of the methods covered in this literature review provide a systematic approach for identifying all (existing) cybersecurity barriers for a given facility. This includes the use of resilience approaches.

III. Assessing the status of cybersecurity barriers

Literature that discusses methodology for assessing the status of cybersecurity barriers is limited. A few relevant papers have however been discussed below.

The survey of Knowles et al. [6] is already mentioned. It focuses on available models/frameworks, tools, and publications, including a discussion of available ”security metrics” for measuring and managing ICS security. The paper points out the scarcity of quantitative metrics as compared to qualitative metrics. A broad spectrum of metrics is included in the survey, and they find that the main focus has been on metrics for criticality analysis in relation to risk assessment. Criticality is important but provides no information in itself on the security of a system, which is the role of a vulnerability assessment. However, the survey (from 2015) concludes that few IACS security metrics are found on this topic. Here, IEC 62443-1-3, which is currently cancelled, is mentioned explicitly as a publication that provides metrics for assessing different aspects of security (e.g., operational, organizational and technical).

Knowles et al. [6] also discuss the *”ambiguity on how to achieve consistent and meaningful metrics measurements. Metrics guidance largely takes the form of scoring characteristics on 0–100 (quantitative) or low to high (qualitative) scales.”* Furthermore, metrics frequently omit benchmarks (”where on a scale from 0 – 100 should we preferably be?”) and it is pointed out that *”a scale is not an adequate substitute for a benchmark.”* The survey concludes that further research into the area of application of security metrics is required.

Whereas Knowles et al. [6] do not go into details on actual metrics, Pendleton et al. [24] present a survey specifically on security metrics and suggest classifying these into four categories, which they state as being *”metrics for measuring the system vulnerabilities, metrics for measuring the defenses, metrics for measuring the threats, and metrics for measuring the situations.”* The background for this split is *”that situations (or outcomes of cyberattack-defense interactions) are caused by certain threats (or attacks) against systems that have certain vulnerabilities (including human factors) and employ certain defenses”* (barriers). The authors state that to the best of their knowledge, this is the first broad survey on security metrics. The metrics are presented on a very general level, however with some additional discussion on how to measure and references to source publications. The metrics however need further operationalization and domain specification.

Pendleton et al. [24] have also performed a follow-up survey on security metrics on a system level. The same framework as described above has been applied and the metrics generally seem to be on a similar format.

Knowles et al. [25] describe assurance techniques for ICS. An assurance technique is defined as a method of assessing some assurance target and is applied to generate evidence as to whether implemented security controls are consistent with organizational risk postures. A distinction is made between two types of assurance techniques:

(1) *”Those which assess security controls (e.g., penetration testing).”*
(2) *”Those that assess the competence requirements for using those assurance techniques (e.g., a multiple choice or lab-based exam).”*

The paper uses interviews with security practitioners to assess how ICS security assessments are conducted in practice and focuses particularly on the operational phase. The paper suggests five governing principles (abbreviated PASIV) for ICS security assessments of operational environments covering the following classes of requirements: Proximity, Accessibility, Safety, Impact and Value.

Furthermore, the assurance techniques for the different phases (22 in total) have been mapped towards the high-level security control categories (35 in total) of ISO/IEC 27001:2013. The purpose of this has been to develop *”holistic compliance evaluation criteria for the security controls in future assurance schemes”*, but also as part of *”overcoming the criticism of many assurance schemes: that there is inadequate technical validation of the implemented security controls.*” For more details concerning this mapping, reference is made to the paper itself.

A stated limitation of the work is that the opportunity to use an assurance technique says nothing about its effectiveness. The authors have however addressed this in a separate referenced publication (this work is however for IT systems in general, rather than ICS especially, and is not further discussed here).

IV. Security levels

The topic of security levels in OT systems has received relatively little attention in the academic literature, and often ”security level” is referred to in a very abstract and non-quantitative way.

Śliwiński et al. [26] present an approach where they try to map Common Criteria Evaluation Assurance Levels (CC EALs) to IEC 62443 Security Assurance Levels (now Security Protection Rating) and our own Secure Safety onion model [27]. Unfortunately, this attempt can most charitably be described as misguided, for a number of reasons:

- The defense-in-depth approach of SeSa does not imply that the level of security at an outer level is any less than any of the levels further in.
- The CC EAL is completely independent of the Security Functional Requirements implemented; it is possible to specify a Protection Profile with only minimal SFRs, and yet evaluate this to the highest EAL, since the EAL is only an indication of what level of certainty (assurance) there is that the (minimal) SFRs have been implemented correctly.

Interpretations of the IEC 62443 Security Protection Rating (SPR) approach has also received criticism from the industry [28], where some claim that using the attackers' level of sophistication to describe the SPR suffers from imprecise definitions – what do phrases such as ”sophisticated means” or ”moderate resources” actually mean? Note however that IEC 62443 currently uses ”low”-”medium”-”high”-”very high” risk reduction as the SPR descriptions, which is still qualitative and subject to interpretation, but may lend itself to standardization over time.

Knowles et al. [6] do not really get into discussing security levels, beyond an illustration that seems to suggest that security levels would tend to decrease with time, something that intuitively seems correct, considering that new vulnerabilities in software keep being discovered.

Iaiani et al. [29] seem to fall down on the side of letting attacker sophistication guide the definition of security levels by stating ”the higher the complexity of the attack and the higher the security level” – but do not attempt to codify this in any way.

Lisova et al. [30] performed a review on combined safety and security analysis and refer to security levels based on HARA and STRIDE analysis, as well as SySML modelling to achieve ”an adequate [. . .] security level”, but do not go into details on formulating how such levels would be determined.

Cook et al. [21] present the CARVER matrix which can be used to assess assets/processes according to Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognisability. This does not translate directly into security levels but could possibly be used to calculate an aggregate risk value that could be used to determine which security level (or, as in IEC 62443, Security Protection Rating) is required for each (sub-)system. Hashimoto et al. [31] describe a system of security zones where they ”automatically” calculate the security level of each zone. However, it is not obvious that this classification fits the purpose, as the calculation is not intuitive. The concept of defining security levels for different zones is also explored by Iaiani et al. [32], but they make no attempt at defining such levels.

V. Integrated safety and cybersecurity barrier management

There is an abundance of literature addressing approaches of combining safety and security for ICS, but very little on combining or integrating safety and (cyber)security barrier management. In our literature review, 16 publications were considered as relevant for this sub-topic. Three of these are surveys or reviews, which we will start with, followed by 13 publications on specific approaches, methods or problems.

Lisova et al. [30] performed a systematic literature review on safety and security co-analyses covering 33 relevant publications. They motivate such co-analyses stating that *"bringing together safety and security work is becoming imperative, as a connected safety-critical system is not safe if it is not secure."* They classified the publications in unified (joint) and parallel safety and security approaches, and whether they were combined safety and security approaches, security informed safety approaches, or safety informed security approaches. The latter was not identified for any of the publications, and it was a somewhat similar share between the two other categories (19 and 14). Somewhat surprising, compared to Kriaa et al. [33], which we will come back to, was that 26 publications were unified approaches, and only 7 parallel approaches.

Overall, Lisova et al.'s study shows that the combination of safety and security analysis is still an emerging domain. They also state that "*in general, we have noticed that the identified approaches do not focus on the fact that security is dynamic in its nature. This dynamic nature implies frequent system updates as a response to a new attack being developed or a new vulnerability being exploited."* [30]

Kriaa et al. [33] performed a survey of approaches combining safety and security for industrial control systems and made a comparative analysis of the 37 selected publications. They distinguished between unification approaches and integration approaches and found that only 7 were unified approaches and 32 were integrated approaches (two were categorized as being both), compared to the 26 versus 7 resulting from the Lisova et al. [30] study.

In the analysis of the different approaches, they highlight combination of fault trees and attack trees, referred to as extended fault trees, as an approach to combine safety and security in the risk management process. The main limitation of the methods based on fault and/or attack trees is related to their static nature. They further discuss methods such as Boolean logic Driven Markov Processes (BNMPs), Bayesian Belief Networks (BBNs), Petri nets, UML-based approaches (UMLsafe/ UMLsec), SysML, SysML-sec, STPA-sec, etc. They conclude that despite academic interest in the safety-security interactions in systems, there were few concrete achievements.

Knowles et al. [6] found that security-related literature generally does not take safety issues into account. Of the 22 publications they covered, 17 described a link between security and safety, but closer inspection revealed that these were statements to the importance of safety in industrial control systems (which would seem obvious). Any recommendations for ensuring safety when ensuring security seemed missing.

Timpson & Moradian [34] propose a methodology to enhance ICS security, that also takes safety into account. The study indicates that aligning and deconflicting technical measures alone are not sufficient for harmonisation of safety and security requirements, requiring also the consideration of non-technical factors and organisational context.

Zhou et al. [35] present a scheme for designing cyberattack-resilient ICSs, with the aim to prevent intrusions into or interference with ICSs. Unlike the traditional concept of fault protection, the cyber attacker is a human with intent. Thus, in addition to dealing with known attacks, the system should also be resilient against evasion tactics. This highlights the need for systemic approaches to addressing cyber security challenges in ICSs. The hierarchical protection ranges from policies to intrusion response. It is an integration of prevention-centric and tolerance-centric defences. Threats in the process of intrusion are countered with both passive and active protection mechanisms. Depending on the extent of threats to the target system, these mechanisms react to malicious events with measures of different strengths.

Although there are many similarities between safety and security [36], there are important differences as well. One challenge is that the two disciplines are practised by distinct professions, who do not always communicate well [37]. Zhou et al. propose investigating this from three approaches: 1) improved understanding of the interdependencies between safety and security; 2) modelling safety and security in a unified framework; and 3) integrating safety and security into the system life cycle [35].

Śliwiński et al. [26] propose an integrated scheme for safety and cyber security analysis, including a method for SIL (Safety Integrity Level) verification that is also elaborated in Śliwiński [38]. The system design phase derives safety and security requirements from the functional requirements, and uses these to define the system architecture. Subsequently, interference analysis is performed to identify the impact the requirements may have on each other. Existing methods to derive technical requirements and analyse the system architecture include qualitative and quantitative Fault Tree Analysis (FTA) and Failure Mode and Effects Analysis (FMEA). A Safety Instrumented System (SIS) management system should include the aspects specific to SISs.

Steiner & Liggesmeyer [39] propose an approach on how to extend the safety analysis by security aspects using component fault trees (CFTs) and attack trees (ATs). A CFT is extended by ATs which model attacks that can cause events in the CFT. When the whole tree is analysed, the result is a CFT that contains safety events as well as security events.

Januario et al. [40] propose a distributed multi-agent framework for resilience enhancement in cyber-physical systems (CPSs). In the context of CPSs, resilience stresses the ability to accommodate faults or events, which otherwise may compromise the stability of the system. Moreover, in the design stage, resilient frameworks should also consider all possible threats, namely physical and cyber threats, while maintaining an acceptable level of operational normalcy. If, despite of a local fault or attack, the system is capable of maintaining a given admissible performance, the whole system is referred as being resilient.

Iaiani et al. [29] have developed an operating methodology, PHAROS (Process Hazard Analysis of Remote manipulations through the cOntrol System), to address the identification of major accident scenarios due to remote manipulation of the physical components of the plant (e.g., remotely controlled valves, pumps, compressors, etc.). PHAROS employs a reverse-HazOp concept, including specifying barriers aimed at the prevention and mitigation of such scenarios. The development was motivated by the lack of operating procedures for assessing the actual link between malicious manipulations of the Basic Process Control System (BPCS) and the SIS (OT systems) and the major accidents that can be induced. PHAROS is further described in Iaiani et al. [41]. In this framework, major accidents triggered by attacks to the control system are becoming an issue that process industry can no longer disregard [42]. Due to the particular nature of this industrial sector, a full security analysis of this specific threat to process plants requires two complementary parts. The application of the methodology to a representative case study highlighted that, when redundant active/procedural safeguards (APSs) are installed as required by safety standards, a successful attack has to infect both the BPCS and the SIS in order to give rise to critical events. Actually, the attackers must not only tamper with the physical components of the plant (e.g. valves, pumps, compressors, etc.), but they must also bypass the APSs. The results can be used to identify the critical elements of the control system that may need dedicated cybersecurity countermeasures, and the design of human barriers.

A similar method, POROS (Process Operability analysis of Remote manipulation through the cOntrol System, is described in Iaiani et al. [32]. POROS is integrated with IEC 62443-3-2.

The next three publications from Téglácy et al. [11], Onshus et al. [43] and Grøtan et al. [44] have certain similarities. They are mainly rooted in the SINTEF/NTNU research environment, relate to the oil and gas industry, and address safety and cybersecurity barrier management. However, they do this differently. Téglácy et al. [11] prepare the ground for future research into a unified safety and security barrier framework. Onshus et al. [43] discuss independence of process safety and control systems and recommend, e.g., future development of cybersecurity barrier management based on experiences with safety barrier management. Grøtan et al. [44] refer to the work on safety barrier management, but argue for a need to supplement this with a resilience approach.

Onshus et al. [43] argue that the definition of barriers should be expanded from controlling energy to also include the information area, e.g., that protection against unwanted data flow and the subsequent negative impacts is treated as a barrier function (with corresponding ICT barriers). This is in line with the work of Carreras Guzman et al. [45] describing the Uncontrolled Flow of Information and Energy (UFoI-E) concept.

The integration of the so-called Cyber-Physical System (CPS) master diagram and the UFoI-E concept constitutes the UFoI-E method for combined safety and security risk analysis of CPSs. In Carreras Guzman et al. [46], the work is extended to include a new toolkit for risk identification termed Cyber-Physical Harm Analysis for Safety and Security (CyPHASS) consisting of an extended bow-tie and a database of risk sources and barriers. In practice, the bow-ties in CyPHASS enable the identification of risk scenarios using a causal analysis methodology. The first step involves identifying the Uncontrolled Flow of Energy (UFoE) as a hazardous event, whereupon identification of sequential causes can be performed in a step-by-step manner, tracing backwards to the root cause. Subsequently, possible safety and security barriers can be identified at different stages, preventing or mitigating impacts in a layered fashion [46]. However, no definitions for barriers are provided, neither for safety barriers nor security barriers.

Téglácy et al. [11] discuss the barrier concept, and as already mentioned, they have prepared the ground for future research into a unified safety and security barrier framework. This is the only ongoing research that to our knowledge has this focus. The main differences, though, is that we eventually aim to integrate cybersecurity barrier management into the already existing safety barrier management regime (including functional safety), with a particular focus on monitoring the status or conditions of the cybersecurity barriers (in addition to, or combined with, the monitoring and follow-up of the safety barriers).

Grøtan et al. [44] refer to the Secure Safety (SeSa) project and the SeSa method completed in 2006 [27], [47], which describes a combined safety and security approach to assess whether a given technological solution for remote access to SIS is acceptable. They also refer to the prolonged (from SeSa) ongoing attempt to advance the barrier model originating from the safety domain into the cybersecurity domain. Although the heritage from SeSa may not be that obvious, they argue for a need to supplement the work on cybersecurity barrier management with a resilience approach, as part of a roadmap for future SeSa work.

Similar as the term barrier, the term resilience was not shown any profound attention in the SeSa approach. It was only mentioned in terms of diversity of firewalls (using different manufacturers), which would provide additional resilience.

The concept of resilience is used in many different ways, and Grøtan et al. [44] argue that there is *”a need for additional measures for countering unexpected and surprising events from the complex security threat landscapes.”* This indicates that the focus is mainly on the unexpected, with strong links to the branch of Resilience Engineering (RE). They also refer to the so-called ”Safety-II” approach.

Resilience is an increasingly used concept and term, but often with a more general meaning, such as ”resilience against cyber-attack” [33], ”resilience of safety-critical systems” [5], and ”resilience through electric power redundancy” [48], just to mention a few examples from the literature review. In our literature sample, 18 of 71 publications used the term resilience (even 4 in the title); however, none of the publications referred to RE or Safety-II in the text, except Grøtan et al. (2020). One other publication [40] referred to RE literature in the reference list. Also when we refer to a ”resilience approach”, we use the term in a broader sense, i.e., using an ”umbrella definition” as elaborated in Øien et al. [49].

Takagi et al. [50] describe an approach for strategic security protection of ICS. They do not use the term resilience, but state that ”multi-layer protection is a common measure against unknown threat.” Several zones are constructed, and the different conduits to the controllers are protected with a number of measures including firewalls, filtering using whitelists and so on. This multi-layer protection is similar to deploying guards at the gate of the factory, more guards at the building entrance, access control systems protecting the door to enter a room, and finally a combination lock to open the safe. In this metaphor, the ICS is kept in the safe. If a specific vulnerability is discovered relating to any of the layers, the other layers should be able to remain secure and the unauthorized operation of the controllers could be prevented.

Integrated safety and cybersecurity barrier management is addressed to a very minor degree in existing literature. Télácy et al. [11] have prepared the ground for future research in this area, and Onshus et al. [43] and Grøtan et al. [44] are only mentioning the CBM concept. Most of the reviewed publications address approaches for combining safety and security related to ICS in general, not barriers specifically. Still, a review of this work is useful, because focusing only on barrier management may be sub-optimal. It may be useful to consider this as part of risk management.

A common classification is to distinguish between a unified and integrated/parallel approach for safety and security of ICS. Although some practical challenges are mentioned as reason for not choosing a unified approach, it is somewhat surprising that none of the publications mentions confidentiality as a reason, i.e., that cybersecurity risk assessments and other assessment are confidential. If they were combined (unified) with safety risk assessments, then the safety assessment must also be confidential.

To the extent the combined safety and security approaches are used for identifying cybersecurity barriers (or countermeasures), they identify the need for countermeasures, but do not identify the ”inventory of cybersecurity barriers” already existing (or designed). A safety and cybersecurity barrier integration approach, even if successful, will obviously not solve all problems. Returning to the ”SeSa paper” [44], they refer to the challenge to effectively deal with hidden, dynamic and emergent threats and vulnerabilities. Dealing with a changing security threat landscape is closely linked to the threat intelligence activities and it is also related to the DevOps approach highlighted by Grøtan et al. [44].

Moreover, the first point on the ”SeSa roadmap” list [44] highlights the issue of Hardware/firmware vulnerability being an area deserving of more attention. With more commercial-off-the-shelf equipment related to, e.g., 5G and Industrial Internet of Things (IIoT), supply chain security related to potential vulnerabilities becomes an important consideration.

VI. Summary and conclusions

Integrated safety and cybersecurity barrier management is not something that has received a lot of attention until now. We believe that this is a research gap, and we will continue to explore the idea of cybersecurity barriers in the following years.

Even with existing technology, supply chain security is a challenge in ICS with its multiple vendor/ supplier environment, especially when entering into the operations phase and the responsibility is handed over from the service integrator provider to the asset owner. This may well call for an increased attention to supply chain cyber resilience.

Acknowledgements

Contribution to the survey presented in this paper is based on the Cybersecurity Barrier Management project (number 326717) funded by the Norwegian Research Council.

References

[1] P. S. A. Norway, “Regulations relating to management and the duty to provide information in the petroleum activities and at certain onshore facilities (the management regulations),” 2020.

[2] A. Eltervåg, T. B. Hansen, E. Lootz, A. Myhrvold, E. Rasmussen, E. Sørensen, B. Johnsen, J. E. Heggland, Ø. Lauridsen, and G. Ersdal, “Barrier memorandum 2017 - principles for barrier management in the petroleum industry,” Petroleum Safety Authority Norway, Tech. Rep., 2017.

[3] A. Zibak and A. Simpson, “Can We Evaluate the Impact of Cyber Security Information Sharing?” in *2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*. IEEE, 2018, pp. 1–2.

[4] D. D. Caputo, S. L. Pfleeger, M. A. Sasse, P. Ammann, J. Offutt, and L. Deng, “Barriers to usable security? Three organizational case studies,” *IEEE Security & Privacy*, vol. 14, no. 5, pp. 22–32, 2016, publisher: IEEE.

[5] C. W. Johnson, “Barriers to the use of intrusion detection systems in safety-critical applications,” in *International Conference on Computer Safety, Reliability, and Security*. Springer, 2014, pp. 375–384.

[6] W. Knowles, D. Prince, D. Hutchison, J. F. P. Disso, and K. Jones, “A survey of cyber security management in industrial control systems,” *International journal of critical infrastructure protection*, vol. 9, pp. 52–80, 2015, publisher: Elsevier.

[7] “Recommended guidelines for classification of process control, safety and support ICT systems based on criticality,” Norwegian Oil and Gas Association, Guideline NOROG 123, 2014. [Online]. Available: https://www.norskoljeoggass.no/en/working-conditions/retningslinjer/integrated-operations/123-recommended-guidelines-for-classification-of-process-control-safety-and-support-ict-systems-based-on-criticality/

[8] “Norwegian Oil and Gas recommended guidelines on information security baseline requirements for process control, safety and support ICT systems,” Norwegian Oil and Gas Association, Guideline NOROG 104, 2016. [Online]. Available: https://www.norskoljeoggass.no/arbeidsliv/retningslinjer/integrerte-operasjoner/104-anbefalte-retningslinjer-krav-til-informasjonssikkerhetsniva-i-ikt-baserte-prosesskontroll--sikkerhets--og-stottesystemer-ny-revisjon-pr-05.12.2016/

[9] M. Shilenge and A. Telukdarie, “4IR integration of information technology best practice framework in operational technology,” *Journal of Industrial Engineering and Management*, vol. 14, no. 3, pp. 457–476, 2021, publisher: OmniaScience.

[10] S. Hollis and D. Zahn, “ICS Cybersecurity: Protecting the Industrial Endpoints That Matter Most,” 2017. [Online]. Available: https://www.controlglobal.com/assets/wp_downloads/pdf/1711-CG-rotecting-the-industrial-endpoints-that-matter-most.pdf

[11] B. Z. Téglásy, B. A. Gran, S. Katsikas, V. Gkioulos, and M. A. Lundteigen, “Clarification of the Cybersecurity and Functional Safety Interrelationship in Industrial Control Systems: Barrier Concepts and Essential Functions,” in *Proceedings of the 29th European Safety and Reliability Conference (ESREL)*, 2020.

[12] A. Roy, D. S. Kim, and K. S. Trivedi, “Attack countermeasure trees (ACT): towards unifying the constructs of attack and defense trees,” *Security and communication networks*, vol. 5, no. 8, pp. 929–943, 2012, publisher: Wiley Online Library.

[13] X. Ji, H. Yu, G. Fan, and W. Fu, "Attack-defense trees based cyber security analysis for CPSs," in *2016 17th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*. IEEE, 2016, pp. 693–698.

[14] J. D. Weiss, "A system security engineering process," in *Proceedings of the 14th National Computer Security Conference*, vol. 249, 1991, pp. 572–581. [Online]. Available: https://csrc.nist.gov/CSRC/media/Publications/conference-paper/1991/10/01/proceedings-14th-national-computer-security-conference-1991/documents/1991-14th-NCSC-proceedings-vol-2.pdf

[15] E. G. Amoroso, *Fundamentals of computer security technology*. Prentice-Hall, Inc., 1994.

[16] B. Schneier, "Attack trees," *Dr. Dobb's journal*, vol. 24, no. 12, pp. 21–29, 1999.

[17] A. P. Moore, R. J. Ellison, and R. C. Linger, "Attack modeling for information security and survivability," Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst, Tech. Rep., 2001.

[18] I. N. Fovino, M. Masera, L. Guidi, and G. Carpi, "An experimental platform for assessing SCADA vulnerabilities and countermeasures in power plants," in *3rd International Conference on Human System Interaction*. IEEE, 2010, pp. 679–686.

[19] S. Bistarelli, M. Dall'Aglio, and P. Peretti, "Strategic games on defense trees," in *International Workshop on Formal Aspects in Security and Trust*. Springer, 2006, pp. 1–15.

[20] K. S. Edge, "A framework for analyzing and mitigating the vulnerabilities of complex systems via attack and protection trees," Ph.D. dissertation, Air Force Institute of Technology, 2007. [Online]. Available: https://core.ac.uk/download/pdf/322583062.pdf

[21] A. Cook, H. Janicke, R. Smith, and L. Maglaras, "The industrial control system cyber defence triage process," *Computers & Security*, vol. 70, pp. 467–481, 2017, publisher: Elsevier.

[22] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," *Leading Issues in Information Warfare & Security Research*, vol. 1, no. 1, p. 80, 2011.

[23] C. Velazquez, "Detecting and Preventing Attacks Earlier in the Kill Chain," SANS Institute, Tech. Rep., 2015. [Online]. Available: https://www.sans.org/white-papers/36230/

[24] M. Pendleton, R. Garcia-Lebron, J.-H. Cho, and S. Xu, "A survey on systems security metrics," *ACM Computing Surveys (CSUR)*, vol. 49, no. 4, pp. 1–35, 2016, publisher: ACM New York, NY, USA.

[25] W. Knowles, J. M. Such, A. Gouglidis, G. Misra, and A. Rashid, "Assurance techniques for industrial control systems (ics)," in *Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy*, 2015, pp. 101–112.

[26] M. Śliwiński, E. Piesik, and J. Piesik, "Integrated functional safety and cyber security analysis," *IFAC-PapersOnLine*, vol. 51, no. 24, pp. 1263–1270, 2018, publisher: Elsevier.

[27] M. G. Jaatun, M. B. Line, and T. O. Grøtan, "Secure Remote Access to Autonomous Safety Systems: A Good Practice Approach," *International Journal of Autonomous and Adaptive Communications Systems*, vol. 2, no. 3, pp. 297–312, 2009.

[28] "OT:ICEFALL – the legacy of "insecure by design" and its implications for certifications and risk management," Vedere Labs, Tech. Rep., 2022. [Online]. Available: https://www.forescout.com/resources/ot-icefall-report/

[29] M. Iaiani, A. Tugnoli, G. Landucci, and V. Cozzani, "A Systematic Methodology for the Identification of Major Accidents Induced by Malicious Manipulation of the Bpcs and the Sis in a Process Plant," *Chemical Engineering Transactions*, vol. 82, pp. 319–324, 2020.

[30] E. Lisova, I. Šljivo, and A. Čaušević, "Safety and security co-analyses: A systematic literature review," *IEEE Systems Journal*, vol. 13, no. 3, pp. 2189–2200, 2018, publisher: IEEE.

[31] Y. Hashimoto, T. Toyoshima, S. Yogo, M. Koike, T. Hamaguchi, S. Jing, and I. Koshijima, "Safety securing approach against cyber-attacks for process control system," *Computers & Chemical Engineering*, vol. 57, pp. 181–186, 2013, publisher: Elsevier.

[32] M. Iaiani, A. Tugnoli, P. Macini, and V. Cozzani, "Outage and asset damage triggered by malicious manipulation of the control system in process plants," *Reliability Engineering & System Safety*, vol. 213, p. 107685, 2021, publisher: Elsevier.

[33] S. Kriaa, L. Pietre-Cambacedes, M. Bouissou, and Y. Halgand, "A survey of approaches combining safety and security for industrial control systems," *Reliability engineering & system safety*, vol. 139, pp. 156–178, 2015, publisher: Elsevier.

[34] D. Timpson and E. Moradian, "A methodology to enhance industrial control system security," *Procedia computer science*, vol. 126, pp. 2117–2126, 2018, publisher: Elsevier.

[35] C. Zhou, B. Hu, Y. Shi, Y.-C. Tian, X. Li, and Y. Zhao, "A unified architectural approach for cyberattack-resilient industrial control systems," *Proceedings of the IEEE*, vol. 109, no. 4, pp. 517–541, 2020, publisher: IEEE.

[36] M. B. Line, O. Nordland, L. Røstad, and I. A. Tøndel, "Safety vs security?" in *PSAM Conference, New Orleans, USA*. sn, 2006.

[37] M. G. Jaatun, M. Bartnes, and I. A. Tøndel, *Zebras and Lions: Better Incident Handling Through Improved Cooperation*. Cham: Springer International Publishing, 2016, pp. 129–139. [Online]. Available: http://jaatun.no/papers/2016/i4cs.pdf

[38] M. Śliwiński, "Safety integrity level verification for safety-related functions with security aspects," *Process Safety and Environmental Protection*, vol. 118, pp. 79–92, 2018, publisher: Elsevier.

[39] M. Steiner and P. Liggesmeyer, "Combination of Safety and Security Analysis - Finding Security Problems That Threaten The Safety of a System," in *Proceedings of Safecomp 2013*, 2013. [Online]. Available: https://hal.archives-ouvertes.fr/file/index/docid/848604/filename/7_-_main.pdf

[40] F. Januário, A. Cardoso, and P. Gil, "A distributed multi-agent framework for resilience enhancement in cyber-physical systems," *IEEE Access*, vol. 7, pp. 31 342–31 357, 2019, publisher: IEEE.

[41] M. Iaiani, A. Tugnoli, S. Bonvicini, and V. Cozzani, "Major accidents triggered by malicious manipulations of the control system in process facilities," *Safety science*, vol. 134, p. 105043, 2021, publisher: Elsevier.

[42] H. W. Thomas and J. Day, "Integrating Cybersecurity Risk Assessments Into the Process Safety Management Work Process," in *Poster Session, AiChe 2015 Spring Meeting & 11th Global Congress on Process Safety*, 2015. [Online]. Available: https://aiche.confex.com/aiche/s15/webprogram/Paper396442.html

[43] T. Onshus, L. Bodsberg, S. Hauge, M. G. Jaatun, M. A. Lundteigen, T. Myklebust, M. V. Ottermo, S. Petersen, and E. Wille, "Security and Independence of Process Safety and Control Systems in the Petroleum Industry," *Journal of Cybersecurity and Privacy*, vol. 2, no. 1, pp. 20–41, 2022, publisher: MDPI. [Online]. Available: https://www.mdpi.com/2624-800X/2/1/3

[44] T. O. Grøtan, S. Petersen, T. Myklebust, and G. K. Hanssen, "Secure-Safety; state-of-the-art and remaining challenges," in *Proceedings of the 29th European Safety and Reliability Conference (ESREL)*, 2020.

[45] N. C. Guzman, D. K. M. Kufoalor, I. Kozine, and M. A. Lundteigen, "Combined safety and security risk analysis using the UFoI-E method: A case study of an autonomous surface vessel," in *Proceedings of the 29th European Safety and Reliability Conference, Lower Saxony, Germany*, 2019, pp. 22–26.

[46] N. H. C. Guzman, I. Kozine, and M. A. Lundteigen, "An integrated safety and security analysis for cyber-physical harm scenarios," *Safety science*, vol. 144, p. 105458, 2021, publisher: Elsevier.

[47] T. O. Grøtan, M. G. Jaatun, K. Øien, and T. Onshus, "The SeSa method for assessing secure remote access to safety instrumented systems," SINTEF, Tech. Rep. A1626, 2007. [Online]. Available: https://www.sintef.no/globalassets/upload/teknologi_og_samfunn/sikkerhet-og-palitelighet/rapporter/sintef-a1626-sesa-report-final.pdf

[48] D. Trimble, J. Monken, and A. F. L. Sand, "A framework for cybersecurity assessments of critical port infrastructure," in *2017 International Conference on Cyber Conflict (CyCon U.S.)*, 2017, pp. 1–7.

[49] K. Øien, L. Bodsberg, and A. Jovanović, "Resilience assessment of smart critical infrastructures based on indicators," in *Safety and Reliability–Safe Societies in a Changing World*. CRC Press, 2018, pp. 1269–1277.

[50] H. Takagi, T. Morita, M. Matta, H. Moritani, T. Hamaguchi, S. Jing, I. Koshijima, and Y. Hashimoto, "Strategic security protection for industrial control systems," in *2015 54th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE)*. IEEE, 2015, pp. 986–992.