Rethinking Independence in Safety Systems

Vahiny Gnanasekaran[1], Tor Olav Grøtan[2] Maria Bartnes[1], and Poul E. Heegaard[1]

[1] NTNU - Norwegian University of Science and Technology, Trondheim, Norway
{Vahiny.Gnanasekaran|Maria.Bartnes|Poul.Heegaard}@ntnu.no
[2] SINTEF Digital, Trondheim, Norway
tor.o.grotan@sintef.no

Abstract. The independence in safety systems ensures that the rest of the OT system possesses the ability to resume normal operation or revert to a safe state during a failure. The requirement was previously sustained by isolating systems, mechanical sensors, and the fact that failures occur randomly and sporadically. However, IT/OT integration, the surge of outsourced IT/OT services, and cyberattacks are forcing the previous requirements to become superseded by rapid optimization and digitization of the safety functions, without addressing the consequences from a non-technical context. This paper presents an initial survey of the challenges in the independence requirements with non-technical (human and organizational aspects) and technical context. The main contribution is to identify future, research directions by using different perspectives, such as resilience, robustness, anti-fragility, and digital sovereignty for retaining independence.

Keywords: independence, safety systems, cybersecurity, IT-OT convergence

1 Introduction

The recent years, Operational Technology (OT) are developing from isolated networks with little to no outside access to becoming integrated into third-party applications and IT systems for increased efficiency, remote access, and simplifying production. Previously, sensors and actuators were powered by gravitational force and chemical reactions, which are currently replaced and controlled by industrial control systems (ICS), including essential safety functions (e.g., process, flaring, emergency shutdown, fire/gas detection, etc.). The rapid implementation of IT systems and cloud computing further increases the complexity and affects the independence of critical safety systems, which ensures that the process systems operate regardless of other systems failing. Even though the systems face rigorous risk and fault analyses backed up by statistics and historical data, they are subject to cascading effects (e.g., a failure in one system propagating as an error/failure into another system [1]) and joint use of a component or software (e.g., design flaws and software errors [2]). In addition, even geographically co-located, critical systems may pose a vulnerability from humans (e.g., accidental misconfiguration) or environmental impact (e.g., weather and natural disasters).

Previous work [3–6] emphasizes technical measures (e.g., redundancy), system integrations, and IT/OT convergence contributing to challenge the independence requirement. However, the ever-increasing threat picture, geopolitical issues, fewer personnel, and cyberattacks increase the necessity of exploring non-technical factors. The safety systems are expected to operate regardless of unintentional incidents or cyberattacks. The unpredictability of a failure (e.g., frequency, intensity, probability) highlights the importance of the OT system to "absorb" errors and failures, by observing, learning, and eventually anticipating future incidents [7]. The current technological era addresses the unambiguous need for non-technical factors and the utilization of interdisciplinary knowledge.

This paper aims to conduct an initial survey on the challenges in retaining independence between digitalized OT safety (sub)systems. The focus is primarily on challenges concerning non-technical aspects (e.g., human, organizational structures, and societal factors), in conjunction with the relevant technical aspects. One goal is to raise awareness in OT research community of the importance of a broad set of perspectives, including system resilience, robustness, anti-fragility, and digital sovereignty. Open research questions and directions are derived from the literature and industry reports, and summarized at the end of the paper.

2 Background

This section explains independence in a safety context and the current digitization of OT systems and the proceeding ramifications in the current circumstances. In addition, a brief introduction is given for relevant concepts, namely, robustness, (cyber-)resilience, anti-fragility, and digital sovereignty.

2.1 Independence Requirements of Safety Systems

In the traditional safety perspective, the independence requirements of safety systems are defined [5] as *"whose ability to function is not influenced negatively by other systems or its interaction with the environment"*.

Four dependency types are defined:

1. *Functional dependency*, denoting the need for another system function.
2. *Cascading failures*, i.e., failure in one system result in failure in other systems.
3. *Common components*, meaning that the same component of a subsystem is part of multiple systems.
4. *Common cause failures*, originating from environmental, operational, design, installation, and/or maintenance.

Independence requirements of safety systems are referred to *independence* in the remaining sections. It ensures that during a failure, the rest of the system can return to a (fail)safe state or continue normal operation [8]. Validating the independence between components/sub-systems is performed by (1) analyzing each component and then evaluating the total dependency in the system to

observe if it holds a certain threshold, or (2) applying a risk analytical approach to holistically assess if the requirements of the complete system's independence if met [9].

Functional dependencies are often a trade-off between adequate service and economic cost [5]. However, dependencies in physical components, equipment, or utilizing the same location are difficult to discover. Usually, the dependencies occur due to operational advantages, rapid technological advancements, standardizations, the use of common software modules, and an increasing amount of software upgrades. Achieving complete independence requires additional equipment, which advances the logical connections, thereby expanding the possibility of physical faults and complexity. Independence in a safety context denotes a reciprocation in sufficient redundancy and negative safety consequences.

Dependencies caused by non-technical factors are not discussed to the same extent as technical factors [8]. This stems from insufficient knowledge or a lack of adequate quantitative frameworks to assess the dependencies introduced by humans and processes. In addition, human actions are treated as being prone to faults and accidents and are usually regarded as the "weakest link" in cybersecurity. Safety often emphasizes random, mechanical defects and degradation as the primary causes of failure, but accidental misconfiguration and misunderstandings have been reasons for interrupted production [10, 11]. The rapid shifts in technology increase the possibility of the industry employees misunderstanding, creating inaccurate knowledge of the technology to accommodate the industry's needs.

2.2 OT/IT Convergence

Historically, OT systems were developed when online access was limited. The safety systems were designed considering the nature of the occurring faults and errors; they appear randomly and consecutively. Nowadays, OT systems have benefited from digitalization, thus allowing e.g., remote control during production or even maintenance on/offshore. However, the increasing amount of connections to public networks raises the likelihood of cyberattacks, since the adversary possesses an extended attack surface by using outdated software from commercial systems [12]. Latent errors may induce cascading effects, by affecting several systems and resulting in failure. Pure ICT systems usually resort to a system restart or reboot in such circumstances, while for OT systems the shutdown of a plant may result in prolonged downtime and severe production losses. In addition, equipment may be unnecessarily stressed during downtime, and leakages may occur during the restart. Ensuring an ongoing operation makes a shutdown the least viable option for OT systems.

This introduces a greater demand for cybersecurity measures and safety and reliability in barrier management. The issue has also been raised and resulted in standards, frameworks, and guidelines concerning cybersecurity within OT systems, such as IEC 62443 [13], NOROG 070 [14], and the NIST Cybersecurity Framework (CSF) [15]. The frameworks contribute to identifying cybersecurity threats by considering both IT and OT systems.

2.3 Current Safety Architecture

Independence is crucial in OT systems, in particular *Safety Instrumented Systems* (SIS). They consist of multiple *safety functions*, which automatically act to preserve the facility's safety during adverse conditions. *Process Control System* (PCS) monitors, regulates, and controls the ongoing operation for potential deviations, and may activate other SIS. *Safe and Automation Systems* (SAS) comprise PCS and SIS systems. Fig. 1 highlights the distinctions between SIS and SAS, and where independence is required. The SIS might deploy one or several *Safety Instrumented Functions* (SIF) while active, to safeguard against hazards [16]. Examples of various SISs are provided by a SINTEF report [17]:

1. **Process Shutdown System (PSD)** responds properly to incidents if the measurements (e.g., within the pressure, temperature, flow control, etc.) deviates from the default values, for instance, by blocking valves and shutting down pumps and compressors.
2. **Emergency Shutdown System (ESD)** isolates ignition sources, closes the safety valves, and shuts off the power supply to the facility. The plant equipment automatically proceeds to safe mode without power (e.g., electricity, air, hydraulic).
3. **Fire and Gas System (F&G)** detects fire or gas leakage at the facility. The system may initiate actions managed by the system itself (e.g., blocking air supply, and signaling other fire pumps and extinguishing systems) or the ESD system. When F&G invokes the ESD system, it removes any ignition sources and reduces pressure.

The purpose of SIS systems is to manage potential hazards, detect discrepancies, prevent abnormal conditions from developing into any hazardous incident(s), or decrease the consequences of the incident(s). Examples of hazardous incidents are Process Control System (PCS) malfunction, over-pressure, and leakage. All SISs comprise three sub-systems; sensors, logical controllers, and actuators [17]. Furthermore, the ESD and PSD system requires a *fail-safe* design, denoting the need for the systems to remain in a safe mode regardless of faults or failures. SISs are expected to operate independently despite the failure of other systems [17].

The SIS systems are realized according to the *barrier model*, where each barrier possesses one task (*barrier function*), which is further deconstructed into *barrier sub-functions* [18]. The sub-function denotes a task performed by SISs. The Norwegian Petroleum Safety Authority states that *"Where more than one barrier is necessary, there shall be sufficient independence between barriers"* [19]. Nonetheless, the current safety design contains some known dependencies to reduce the economic and operational toll [5]. The safety systems rely mostly on the same firewalls, network components, configuration tools, and domain controllers. In addition, the critical safety systems rely on each other by using the same components (e.g., valves and pumps).

The recent years the *Purdue model* has been adopted in ICS [5, 20]. In general, the network topology model ensures that non-critical systems, such as office and

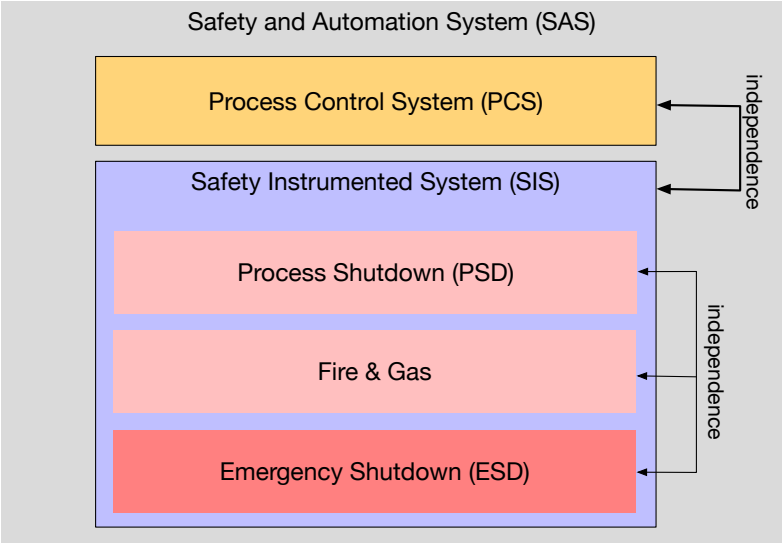

Fig. 1. Independence of safety systems and functions

IT systems are located at the top layer, while OT systems are placed in lower layers. *The demilitarized zone (DMZ)* is located between OT and IT systems to provide adequate segregation (e.g., firewall, dedicated communication channels, access control, etc.). In addition, *zones* is placed across layers, while *conduits* grant secure connections between the zones [13].

The lower OT layers contain a distinct collection of modern and legacy equipment. Since legacy systems are constructed with the assumption of being isolated, they possess limited security controls. When digital services (e.g., cloud, remote access, data analytics) are directly connected to the lower layers, they could easily be exploited by adversaries. The zones and conduits contribute to increasing the overall, security protection against spoofing, but it does not guarantee that the requirements of independence are met [5]. This increases the possibility of an adversary discovering exploitable dependency, targeting and eavesdropping on the secure channel, and attempting to modify data. Thus, the independence is compromised since the proposed "air-gapping" between critical layers diminishes.

2.4 Robustness, Resilience & Anti-fragility

In Munoz et al. [21], a taxonomy triangle is introduced, which is applied in this paper to discuss different desired properties of a safe and secure system:

- *robustness* - avoid being affected
- *resilience* - bounce back quickly
- *anti-fragility* - bounce back stronger

Robustness depicts a system's ability to maintain operations after an incident [21]. The term implies that strategic and contingency plans are already incorporated into the system, such that any consequences of certain (known) accidents are accounted for. Robustness is key for safety barriers since each barrier attempts to ensure safe operation regardless of abnormal conditions [6]. In addition, redundancy (e.g., additional components or alternative procedures) or different locations contributes to enhancing robustness.

Cyber-resilience denotes the research field increasing a socio-technical system's combined preventive and adaptive nature to ultimately tolerate cyberattacks [22]. Resilience explains the ability to "bounce back" to its general functionality succeeding an abrupt incident and implies a fostering of the *intrinsic ability* inherent in a system or organization [22]. The difference between robustness and resilience is that resilience operates proactively in continuously absorbing and improving to prepare for upcoming incidents.

A main challenge in achieving cyber resilience is the discrepancy between measures required by the system defenders versus the perpetrators; it is simply not enough for an organization to introduce general security mechanisms (e.g., adequate password hygiene, performing system updates, patching, etc.), and develop sufficiently extensive incident plans. The adversaries only require one opportunity to exploit newly identified vulnerabilities. In addition, the defender may struggle to distinguish if a disturbance is due to a technical malfunction or hostile intentions.

Anti-fragility represents *graceful extensibility* from resilience [23]. Not only should the system possess the capability to return to the ordinary state, but be able to thrive in adverse conditions, by increasing its tolerance for disruptions [24]. Regardless of any assessment and validation, misconfigurations and defects in the safety systems always exist. Hence, the systems should always exist in some form of stressful state to not extensively rely on automated systems.

Munoz et al. [21] distinguish between the robustness, resilience, and anti-fragility of a system, depending on how it behaves after an adversary (undesired) event. Fig. 2 illustrates the taxonomy triangle. Although robustness depicts insensitivity towards instability, resilience describes the ability to fully recover from incidents, after a larger decrease in performance. However, resilience seeks to minimize the exposure to volatility, and anti-fragility *pursues* the volatility and exploits it towards positive gain. The three distinct properties suggest potential approaches to observing, mitigating, and gaining an advantage from a cyberattack.

2.5 Digital sovereignty

Digital sovereignty is an emerging research field discussing the ability to maintain services while protecting them from structural dependencies [25]. The dependencies are entrenched in economic autonomy, competition, political interests, and/or individual self-determination. US ban on TikTok and other Chinese

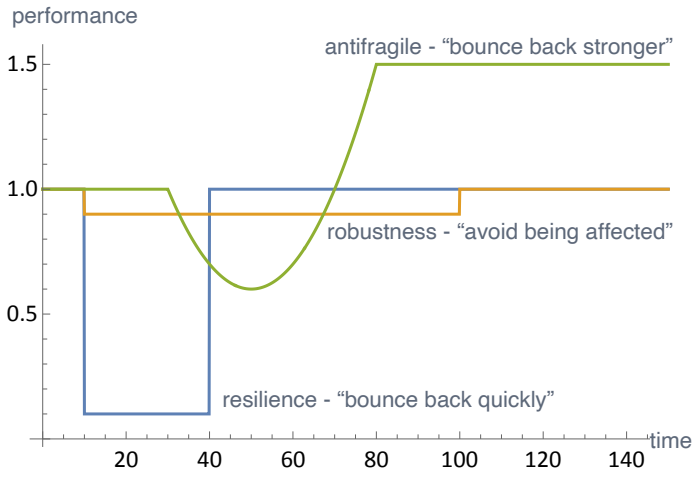

Fig. 2. After an adversary / failure

apps, and prevention of US commercial actors to benefit from European customers' data are two instances related to digital sovereignty [26]. A recurring challenge within digital sovereignty is the *turn-key solutions* provided by a system vendor [27]. Such solutions include the entire integrated IT/OT system, maintenance, service, and upgrades, and are economical and effortless for the benefiting industry actors. However, they are reliant on the same vendors to ensure operations and safety systems in an industry-wide emergency. Hence, the industry actors are compelled to surrender their potential experience and knowledge in exchange for receiving third-party turn-key solutions.

3 Key Safety Independence Challenges

The following section provides a brief introduction to the challenges in determining compliance with the independence requirements in a technical and non-technical context, respectively.

Technical Challenges

Concurrency. Safety literature [8, 6] assumes that safety incidents occur one at a time. The initiating causes are random, and the barriers degrade independently. Simultaneous incidents (i.e., breaching multiple barriers) occur rarely in safety (e.g., black swans). In contrast, this is highly probable in a cybersecurity context, where seemingly unintentional faults might be triggered by an adversary. The attacker could potentially sabotage the operations, in addition to gaining access to sensitive information. The cyberattack of multiple barriers could thus make the safety system easier to compromise and lead to malfunction, affecting independence.

Consequences of increasing digital connections. Cloud services, remote control, and data analytics increase the possibility of the industry being targeted by cyberattacks. If an attack occurs at the respective service providers, this could hold unprecedented consequences for the operations on site. The reliance on digital services from external providers and the consequences of a cyberattack on their premises should be considered a part of the independence requirements.

Control of the digital supply chain. Independence is further affected by digital sovereignty and the issue of selecting only one manufacturer for the critical components. The industrial actors usually consider a partnership with one SIS system vendor, due to cost and convenience. However, such integrated solutions are condemned, due to the high risk of cyberattacks, unintentional failures, and increasing complexity [3]. Alternatively, adopting solid-state SIS systems and pursuing quality assurance evidence in the product, relevance, management, and software are advocated, since complete control of the hardware, interactions, and software is vital to ensure independent safety operations. Nonetheless, it remains challenging to pursue the trade-off between the number of vendors and the cost of maintaining sufficient independence.

Assessment of the technical independence requirement. Lastly, the assessment of independence (e.g. the probability of being compliant with the independence requirement) is seemingly a remaining, critical issue, due to the increasing complexity of OT/IT systems [28]. The development of novel safety independence assessments is necessary since the underlying safety assumptions are constantly being challenged. Onshus et al. [5] raises the question of whether the Purdue model and zones from IEC 62443 are still sufficient to provide independence of the safety systems since it does not provide all communication within the associated zone/layer. Although the report presents alternative solutions, such as dedicated, secure communication channels, and encryption, it remains to observe whether these measures are sufficient, or need improvement to increase independence (reduce the probability that the independence requirement is violated).

Non-Technical Challenges

Organizational structures and roles. The upsurge of cybersecurity incidents is not reflected in the tasks and expected knowledge of the OT personnel [29, 20, 30]. The OT personnel and operators perceive any system anomalies but struggle to identify the origin of the anomaly (e.g., (un)intentional faults). This challenge is particularly apparent for ICAS operators, which usually carry a lead role in all emergency responses [31]. Previously, their responsibility concerned monitoring and operating the physical processes, while nowadays, it has extended to ensuring the behavior of the ICAS system itself [32].

Knowledge and competence gap. The necessary competencies within the OT personnel address the safe usage of the process systems, without clearly highlighting potential cybersecurity risks (e.g., open ports, unidentified 4G dongles/USB

sticks). This increases the need of cybersecurity knowledge required by the ICAS operator and demands considerable cooperation between the rest of the IT and OT personnel, and coordination with external actors (e.g., Critical Emergency Response Team (CERT), Security Operations Center (SOC)).

Unclear responsibility of OT system vendors. OT system vendors delay the deployment of system patches from known security vulnerabilities, thereby leading to neglected procedures [33]. The maintenance and patching may also consider only the OT processes running on the IT components, such that the IT components are completely disregarded. Overlooking the IT components might result in exposure to known IT system vulnerabilities, which makes the OT processes no more secure than the weakest IT component. Thus, the independence might be in jeopardy if the IT part of the OT-IT converged systems is vulnerable.

Procurement of proprietary components and equipment. Selecting various vendors with distinct production locations could limit any economic or environmental disruptions (e.g., financial crisis, natural disasters) [3]. During critical malfunctions demanding a rapid component replacement, or using the same IT services places dependencies on external circumstances, ultimately affecting the independence. possessing distinct manufacturers and service providers reduce the dependency on one system/actor, which implies more autonomy and an increase in safety independence.

Geopolitical picture and national interests. Vendors could be bribed to possess back-doors to retrieve information on behalf of others. In addition, the data might not only be monitored by a foreign state but also subject to modification, causing damage to critical infrastructure [26]. Even relying on production in one state might affect operations, if the transportation, economy, or labor is weakened due to external circumstances. The independence is challenged by digital sovereignty; the ever-growing globalization and its reliance on multi-national trading and innovation.

Increased human contribution. Since the attacker is human and subject to personal motivation, a human defense might improve the issue, to better gauge the adversary's motivation and anticipate potential targets [34]. Furthermore, the converged IT/OT system still includes technical staff to work separately [20]. Industrial actors should emphasize the importance of collaboration during unforeseen incidents. Disclosing the competence, experiences, and safeguarding techniques across the staff may improve the detection, identification, and mitigation of future cyberattacks with fewer consequences to the system's independence.

4 Plan and Prepare with Robustness, Cyber-Resilience & Anti-fragility in Mind

This paper argues that cyberattacks, digital services, and increasing system complexity are highly affecting the independence requirement of safety systems. This

section presents how robustness, (cyber-)resilience, and anti-fragility could contribute to ensure that the independence requirement in the current digitalization context from a non-technical perspective is sustained.

The cyber-incident management system in ICS must be robust and resilient and should even learn from attacks and failures and become stronger (i.e., an anti-fragile system) [23, 24]. In the safety system, isolation, protection, and barriers are present to reduce the spatial consequences (e.g., the number of affected objects or users), while detection and mitigation reduce the temporal consequences (e.g., the time from an attack until the system returns back to normal operation). Further, the incident management system in ICS depends on an efficient communication sequence of information exchange between the different stakeholders and roles (e.g., process-control operators, SOCs, vendors). The key roles have to be well-defined and well-known to all stakeholders. Communication must be available for knowledge and experience sharing for all stakeholders.

Reducing the consequences of cyberattacks on safety operations requires early identification and sending of appropriate alerts to all involved stakeholders, and the provision of means to continue (safe) operations of OT during an attack. The latter is extremely challenging because the attack might trigger physical accidents, or modify values, which might put the system in an unsafe operation mode. Reducing the impact of escalating faults originating from cyberattacks requires organizational procedures, access to information, well-defined roles, and point-of-contacts [29]. The operation might be able to withstand the attack and still continue its operations if the frontline staff (e.g., key personnel closest to the attack) have means, knowledge and skills to perform appropriate mitigation.For instance, if an OT provider is not affected by an ongoing cyberattack, disconnecting the OT from the ICS and running the system in *island mode* ensure continuous operation, provided that island mode functionality is enabled.

Mitigating consequences requires a swift and resilient response to disruptions since cyberattacks inevitably occur in ICS, ultimately affecting the independence requirement of safety functions. Multidisciplinary knowledge contributes to raising awareness among the initial response team to identify and detect safety incidents that originate from the cyber domain. Furthermore, frequently practicing preparedness exercises where the personnel is trained to understand and identify possible alternatives might improve their resilient behavior. The joint effort between OT and IT personnel and external service providers requires training and exercise to communicate effectively. This reduces the time spent on the rescue, by increasing the staff's tolerance for disruption, expanding their experience in bouncing back from cyberattacks. Withstanding severe cyberattacks allow graceful extensibility by overstretching the adaptive capacity to manage surprises [23].

The steps acquired after the cyberattack are crucial in how the upcoming attacks are managed and affect safety independence requirements. Anti-fragility urges the organization to grasp the feedback and learn from the incident to improve the countermeasures [24]. The phases towards returning to normal operations could be provided through debriefs. The system changes and updates

should be examined through risk analysis to estimate how the system changes influence safety independence. Due to the increasing complexity of OT systems, these experiences should be shared across stakeholders at all levels. Although organizations are weary of disclosing cyberattacks, all relevant actors should share experiences to develop sufficient measures to minimize the impact on safety independence.

5 Future Research Directions

The independence requirement was designed based on previously held assumptions about the existing technology, paradigms, and incidents occurring in the industry. Due to emerging technologies, and rapid digital implementation, these foundations need disruption to address the imminent challenges. The following section presents future research directions that should be considered by the ICS cybersecurity community.

Challenging the Independence Requirement. Since digital IT/OT systems are more interconnected, and the OT industry is more reliant on third-party software, components, and standardized systems, it is necessary to revisit the independence requirement. The existing safety regulations demand independence levels not quite reflected in the current solutions. Cyberattacks further inflate the issue, since they are subject to intentional motivation. This raises the issue of whether the independence itself should be assessed to accommodate the current digital advancements [5]. Achieving true independence is cumbersome and expensive, and not always necessary. However, incorporating non-technical aspects, such as personnel, exchanging competence and experiences, choice of vendors, and even the geopolitical picture as a part of the independence might prove essential in the upcoming safety systems. Exploring the proper validation and assessment of safety independence could contribute to an improved holistic perspective of the IT/OT systems.

Silent Knowledge in IT/OT. If the Purdue model fails to satisfy the independence requirement, there might be other approaches suitable for increasing the independence, outside the existing literature. The industrial actors might possess solutions or practices within their organizational processes that could contribute to clarifying their procedures ensuring that the independence is met. Furthermore, the work culture influences the ICAS operator's performance on critical tasks. The skill and know-how acquired during operations among the facility personnel are usually not written but could be extracted with qualitative studies. Observations and interviews with relevant operators could provide previously unknown insights and solutions to preserve safety independence.

Multi-Role Coordinated Knowledge Exchange. Necessary actors do not possess sufficient knowledge to retain independence. First, OT personnel lacks the relevant competency to identify cyberattacks. Second, service providers and system

integrators require knowledge to provide customized cybersecurity services and design OT systems with security controls. By increasing the level of knowledge of all involved actors, they foster their cybersecurity and OT awareness, which increases collaboration and common understanding before, during, and after a cyber incident. Stability is key to providing good integration in the business processes, along with increased consistency. Future research should explore the sufficient knowledge needed by all involved parties to preserve the independence of ICS.

Human Factors. Humans face the same criteria as technical safety measures, however, it is nearly impossible to satisfy the independence requirement in human factors [8]. They are prone to fatigue, mood changes, changing energy levels, and stress levels. Likewise, cybersecurity usually regards humans performing malicious actions. However, in contrast to technical systems, humans possess the ability to suggest brilliant strategies that become crucial during a cyberattack. Utilizing human knowledge and experience in handling unforeseen incidents increases the possibility of rapidly returning to a normal state. Upcoming work should consider humans as a potential solution in redefining safety independence in the context of cyber-attacks.

6 Concluding remarks

The IT/OT integration, the increasing digital connections, and the upsurge of cyberattacks change the inherent premise for independence in safety-critical systems. This paper presents potential, non-technical research directions challenging independence, by introducing the related technical challenges and assessing the current literature and industry reports. Perspectives from robustness, resilience, anti-fragility, and digital sovereignty provide insights into future work. Non-technical factors should be included to propose a novel and viable assessment method for the revised independence requirement. Securing the current independence is a collaboration between traditional safety and cybersecurity measures, and between humans, processes, and technology.

Acknowledgments

This research was funded by the Norwegian Research Council through the Cybersecurity Barrier Management project, grant number 326717.

References

1. Buldyrev, S.V., Parshani, R., Paul, G., Stanley, H.E., Havlin, S.: Catastrophic cascade of failures in interdependent networks. Nature 464(7291), 1025–1028 (2010)
2. Avizienis, A., Laprie, J.C., Randell, B., Landwehr, C.: Basic Concepts and Taxonomy of Dependable and Secure Computing. IEEE transactions on dependable and secure computing 1(1), 11–33 (2004)

3. Donnelly, P., Abuhmida, M., Tubb, C.: The drift of industrial control systems to pseudo security. International Journal of Critical Infrastructure Protection 38(November 2021), 100535 (2022), https://doi.org/10.1016/j.ijcip.2022.100535
4. Kriaa, S., Pietre-Cambacedes, L., Bouissou, M., Halgand, Y.: A survey of approaches combining safety and security for industrial control systems. Reliability Engineering and System Safety 139, 156–178 (2015), http://dx.doi.org/10.1016/j.ress.2015.02.008
5. Onshus, T., Bodsberg, L., Hauge, S., Jaatun, M.G., Lundteigen, M.A., Myklebust, T., Ottermo, M.V., Petersen, S., Wille, E.: Security and Independence of Process Safety and Control Systems in the Petroleum Industry. Journal of Cybersecurity and Privacy 2(1), 20–41 (Feb 2022)
6. Hauge, S., Øien, K.: Guidance for barrier management in the petroleum industry. Tech. Rep. September 2016, SINTEF (2016)
7. Hollnagel, E., Woods, D.D., Leveson, N.: Resilience engineering: Concepts and precepts. Ashgate Publishing, Ltd. (2006)
8. McLeod, R.W.: 16 - Human factors in barrier thinking. In: McLeod, R.W. (ed.) Designing for Human Reliability, pp. 235–253. Gulf Professional Publishing, Boston (2015), https://www.sciencedirect.com/science/article/pii/B9780128024218000163
9. Hauge, S., Onshus, T., Øien, K., Grøtan, T.O., Lundteigen, M.A., Jersin, E.: Uavhengighet av sikkerhetssystemer offshore – status og utfordringer. Tech. rep., SINTEF, Trondheim (2006)
10. U.S. Chemical Safety Board: U.S. Chemical Safety Board Concludes "Organizational and Safety Deficiencies at All Levels of the BP Corporation" Caused March 2005 Texas City Disaster That Killed 15, Injured 180 (Mar 2005), https://www.csb.gov/u-s-chemical-safety-board-concludes-organizational-and-safety-deficiencies-at-all-levels-of-the-bp-corporation-caused-march-2005-texas-city-disaster-that-killed-15-injured-180, [Online; accessed 26. Jan. 2023]
11. Macalister, T.: Piper Alpha disaster: how 167 oil rig workers died. The Guardian (Feb 2018), https://www.theguardian.com/business/2013/jul/04/piper-alpha-disaster-167-oil-rig
12. Jaatun, M.G., Wille, E., Bernsmed, K., Kilskar, S.S.: Grunnprinsipper for IKT-sikkerhet i industrielle IKT-systemer. Tech. rep., SINTEF (2021)
13. Industrial communication networks – Network and system security – Part 1-1. Standard, International Electrotechnical Commission (Mar 2009)
14. Application Of IEC 61508 And IEC 61511 In The Norwegian Petroleum Industry. Standard, Norwegian Oil and Gas Association (2001)
15. Shen, L.: The NIST cybersecurity framework: Overview and potential impacts. Scitech Lawyer 10(4), 16 (2014)
16. Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and application programming requirements. Standard, International Electrotechnical Commission (Aug 2017)
17. Myklebust, T., Onshus, T., Lindskog, S., Ottermo, M.V., Lundteigen, M.A.: Datakvalitet ved digitalisering i petroleumssektoren. Tech. rep., SINTEF, Trondheim (2021)
18. Johansen, I.L., Rausand, M.: Barrier management in the offshore oil and gas industry. Journal of Loss Prevention in the Process Industries 34, 49–55 (2015), http://dx.doi.org/10.1016/j.jlp.2015.01.023
19. Petroleum Safety Authority: The Management Regulations § 5 Barriers. Regulation, Petroleum Safety Authority (2001), https://www.ptil.no/en/regulations/all-acts/the-management-regulations3/II/5

20. Zanutto, A., Shreeve, B., Follis, K., Busby, J., Rashid, A.: The Shadow Warriors: In the no man's land between industrial control systems and enterprise IT systems. pp. 1–6. USENIX (7 2017)
21. Munoz, A., Billsberry, J., Ambrosini, V.: Resilience, robustness, and antifragility: Towards an appreciation of distinct organizational responses to adversity. International Journal of Management Reviews 24, 181–187 (4 2022)
22. Grøtan, T.O., Antonsen, S., Haavik, T.K.: Cyber Resilience: A Pre-Understanding for an Abductive Research Agenda. In: Resilience in a Digital Age, pp. 205–229. Springer (2022)
23. Woods, D.D.: Four concepts for resilience and the implications for the future of resilience engineering. Reliab. Eng. Syst. Saf. 141, 5–9 (Sep 2015)
24. Taleb, N.N.: Antifragile: Things that gain from disorder, vol. 3. Random House (2012)
25. Edler, J., Blind, K., Frietsch, R., Kimpeler, S., Kroll, H., Lerch, C., Reiss, T., Roth, F., Schubert, T., Schuler, J., Walz, R.: Technology sovereignty: From demand to concept. Tech. rep., Fraunhofer Institute for Systems and Innovation Research ISI, Karlsruhe (2020)
26. Floridi, L.: The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. Philosophy and Technology 33(3), 369–378 (2020)
27. H+M Industrial EPC: Turnkey Project Advantages And Disadvantages: What To Know Before Signing A Contract. Insights (2021)
28. Wäfler, J., Heegaard, P.E.: Interdependency Modeling in Smart Grid and the Influence of ICT on Dependability. In: Bauschert, T. (ed.) Advances in Communication Networking. pp. 185–196. Springer Berlin Heidelberg, Berlin, Heidelberg (2013)
29. Green, B.R., Prince, D.E., Roedig, U., Busby, J.S., Hutchison, D.: Socio-Technical Security Analysis of Industrial Control Systems (ICS). In: Proceedings of the 2nd International Symposium for ICS & SCADA Cyber Security Research. pp. 10–14 (2014)
30. Michalec, O., Milyaeva, S., Rashid, A.: When the future meets the past: Can safety and cyber security coexist in modern critical infrastructures? Big Data and Society 9(1) (2022)
31. Green, B., Krotofil, M., Hutchison, D.: Achieving ICS resilience and security through granular data flow management. In: CPS-SPC 2016 - Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and PrivaCy. pp. 93–101. Association for Computing Machinery, Inc (oct 2016)
32. Miyachi, T., Yamada, T.: Current issues and challenges on cyber security for industrial automation and control systems. Proceedings of the SICE Annual Conference pp. 821–826 (2014)
33. Hanssen, G.K., Onshus, T., Jaatun, M.G., Myklebust, T., Ottermo, M., Lundteigen, M.A.: Principles of digitalisation and IT-OT integration. Tech. rep., SINTEF (2021)
34. Bodsberg, L., Grøtan, T.O., Jaatun, M.G., Wærø, I.: HSE and Cyber Security in Remote Work. In: 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA). pp. 1–8 (2021)