Safety Science 171 (2024) 106384

Contents lists available at ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/safety

Exploring the grounds for cyber resilience in the hyper-connected oil and gas industry

Solveig Pettersen [a], Tor Olav Grøtan [b,*]

[a] Department of Industrial Economics and Technology Management (IØT), Norwegian University of Science and Technology (NTNU), Norway
[b] SINTEF Digital and Department of Industrial Economics and Technology Management (IØT), Norwegian University of Science and Technology (NTNU), Norway

A B S T R A C T

This paper explores the offshore oil and gas industry as a case of an industry operating in demanding conditions with an imminent potential for catastrophic failure, undergoing major transformations driven by advances in digital technologies while being exposed to an increasingly aggressive threat landscape due to geopolitical changes. It is also a case of cyber-physical systems with tight couplings between digital changes which might be incited from virtually anywhere, and real-world, physical consequences. The exploration is aimed at understanding, based on interviews, to which extent the existing cyber security practices in the industry carries the potential to be strengthened by the application of resilience principles. An enhanced level of cyber security, denoted cyber resilience, is regarded as a crucial part for the industry to become able to close a strategic agility gap, in which they are at risk of falling behind in their response repertoire, becoming stuck and stale while trying keep up with an increasing rate of shocks through classical modelling and simulation. Resilience is, however, a concept with many meanings, originating from a diversity of academic discourses. The paper demonstrates the usefulness of analyzing the empirical data through an analytical framework of cyber resilience, a "resilience ABC", accommodating a crucial distinction between robustness and resilience founded on adaptive capacities. Moreover, we find that closing the strategic agility gap requires a cyber resilience approach that is a mix of robustness and adaptive capacity, and that the gradual shift towards more emphasis on adaptive capacity requires a fundamental shift from seeing resilience-as-outcome as just an epiphenomenon of existing practice. In contrast, we see adaptive capacity as resilience-as-process, a phenomenon to study on its own terms. This also implies that cyber resilience management must move beyond a sheer assimilation with risk management. As access to real incident data may be limited, we also advocate the idea of training on scenarios at the boundaries of robustness.

1. Introduction

1.1. Cyber resilience, safety and security in hyper-connected cyber-physical systems

This paper investigates empirically how the Norwegian offshore petroleum industry deals with the implications from being connected to and dependent on a global information infrastructure for which the actual use needs to be guarded carefully to avoid unintended impact from virtually the whole world. The possible impact is not only of a direct technical and physical nature, but also indirectly related to competitive business processes, economic, social, and political change, and disruptions at a global scale. Moreover, this industry is also a *case of* an industry operating in demanding conditions with an imminent potential for catastrophic failure, undergoing major business transformations driven by advances in digital technologies (Gressgård et al., 2018) while being exposed to an increasingly aggressive threat landscape due to geopolitical changes (Norwegian National Security Authority, 2022). It is also a case of a cyber-physical system, i.e., a system that integrates computation with physical processes, and its behavior is determined by both the computational (both digital and other forms) and physical parts of the system (NIST, 2022). Threats to such systems, with tight couplings between digital changes which might be incited from virtually anywhere, and real-world, physical consequences, are also central in Enisa's foresight of cybersecurity threats towards 2030 (ENISA, 2023).

Like many other critical industries and infrastructures, the safety practices of the Norwegian oil and gas industry are traditionally founded on continuous improvement based on assessment of risks and on experiences (Norway Petroleum Safety Authority, 2017). This has increasingly been challenged by the urge to harvest the benefits from digital advances. Hyper-connectivity implies that the disruptive digital potential is no longer limited to challenging of existing safety practices and local security concerns, but bring to the doorstep a huge potential for hostile and adverse influence that may jeopardize safety design, conventions, and arrangements. Resilience Engineering (RE) is a concept that has been used to challenge safety conventions for nearly two decades, founded on the recognition of the need to address complexity (Woods & Hollnagel, 2006), not only uncertainty. Intuitively, RE appears to accommodate the combined safety and security challenge for a

* Corresponding author.
E-mail address: tor.o.grotan@sintef.no (T.O. Grøtan).

https://doi.org/10.1016/j.ssci.2023.106384
Received 8 March 2023; Received in revised form 13 October 2023; Accepted 17 November 2023
Available online 24 November 2023

broad range of hyper-connected industries and infrastructures, but the overarching concept of resilience also takes many forms. A substantial literature on Critical Infrastructure Resilience (CIR), e.g. (Rød, 2020), does not pay much attention to the distinctions between RE and other resilience concepts. In this paper, we demonstrate a novel way to investigate the resilience potentials in the cyber-physical domain of the oil and gas industry empirically. Moreover, we also use the findings to bring forth some novel conceptual dimensions that are crucial for the constitution of the emerging field of "cyber resilience" to support CIR, covering both safety and security issues in a hyper-connected world. Specifically, we argue that to strategically counter the rising cyber-physical complexity challenge, the industry must combine different resilience concepts in a specific manner.

1.2. Hyper-connectivity in the offshore oil and gas industry

The offshore oil and gas industry is persistently and increasingly adopting digital technologies that may contribute to more efficient operations and safer work (Gressgård et al., 2018). Examples include accessing offshore systems from shore for operations and maintenance instead of travelling offshore for physical access, automation of manual tasks and work processes and gathering and processing of data for improvement of production, maintenance, and safety. The connection to the global Internet however also implies an increase in potential vulnerabilities and threats emerging from all corners of cyberspace. Moreover, the integration of generic information technology (IT) and operational technology (OT) at installations increases complexity (Hanssen et al., 2021). According to the Norwegian National Safety Authority, the increased complexity of digital systems and value chains is a significant cause of digital vulnerabilities (The Ministry of Justice and Public Defence, 2020) which makes it harder to predict and prepare for the potential scenarios that may occur. A recent example is the so called log4j vulnerability, where an open-source software library had a critical weakness that left systems and organizations all over the world vulnerable to exploitation from hackers. With log4j being integrated in third party software, it was rendered unclear to many organizations whether they were exposed to the vulnerability or not. Critical OT safety systems were also vulnerable to exploitation under certain conditions (Lacy & Scott, 2021). This sole example signifies the need for perspectives and concepts that can aid in coping with the sociotechnical complexity of IT/OT systems.

The emerging vulnerabilities reflect a hyper-connectivity beyond the visible constraints of the oil and gas industry. The industry steadily grows more technologically complex, building on digital technologies used across sectors and industries. A common denominator is that their failure to deliver services will have severe economic and political consequences. Their potential failure is imminent due to sociotechnical complexities, and the current geopolitical situation implies an aggressive threat landscape with hostile motivation for triggering or amplifying threats, uncertainties, and raising fears of high-consequence failure. After the 2022 attacks on the Nord Stream pipelines in the Baltic Sea, maintaining control over the Norwegian offshore petroleum activity and Norwegian gas export to Europe has been declared as a foundational national interest (Hovland and Holmes, 2022), and it is therefore subject to the Norwegian Security Act (Norwegian National Security Authority, 2023). Hence, also the oil and gas industry must be regarded as a critical infrastructure, entangled in multiple networks at different levels, technical, organizational, social, or political. In such a complex, multi-layered hyper-connectivity perspective in which cascading effects are imminent, the locus of the trigger event is borderline insignificant, but the possibility of cyber-physical attacks being part of the cascading scenario is significant.

1.3. Strategic agility; a forward point for resilience of cyber-physical systems

Woods and Alderson (2021) argue that critical infrastructures are falling behind in their response repertoire and thus suffer from a Strategic Agility Gap (SAG), becoming stuck and stale while trying keep up with an increasing rate of shocks through classical modelling and simulation. To close this mismatch between velocities of change and velocities of adaptation, in which "*distributed networks of extensive tangles of interdependencies, are fundamentally brittle*" (p. 7), they argue that it is necessary to look further ahead towards resilience through *engineering of an adaptive capacity* that enables the necessary strategic agility to keep up with complexities that are impossible to anticipate, model and simulate in advance.

A major portion of the shocks encountered by cyber-physical systems may be attributed to inherent sociotechnical complexity, and a large proportion of undesired digital events occur unintentionally (The Ministry of Justice and Public Defence, 2020). However, the very same complexity also provides fertile grounds for intentional exploitation of vulnerabilities and brittleness. The ability to discriminate between the two possibilities is crucial. As IT, entangled with OT, is the (cyber-physical) infrastructure of infrastructures, potentially producing as well as conducing ripple effects and cascading impacts across various critical infrastructures, we argue that progress in cyber resilience, enabling adaptive maneuvering in a persistently complex cyber threat landscape, is at the core of closing the SAG for critical infrastructures in general. In times when global megatrends also add (criminal and political) aggressiveness to inherent cyber-related complexity, closing the SAG in a resilient manner is urgently needed for proper protection of critical infrastructures and national interests, inter alia, oil and gas installations.

In this paper, we aim to advance the understanding of cyber resilience through investigating its potential to close the SAG related to the severely accelerated cyber-physical security challenge in the oil and gas industry. Other infrastructures could also have been investigated for the same purpose. E.g., the electrical energy industry, for which Bochman (2018) argue that we actually are at the "end of cybersecurity" in the sense that standard IT security approaches are insufficient for dealing with advanced cyber-attacks towards the energy systems. Accordingly, the energy sector should take the opposite direction, refraining from taking the most advanced cyber solutions into use. However, regarding the option of reducing the tempo and scope of digitalization in the Norwegian oil and gas industry as unlikely, we direct our attention towards the ambitious, hypothetical prospect of closing the SAG for cyber-physical infrastructures through progress in cyber resilience, supporting the enhancement of existing cyber security practices.

The urgency for enhanced cyber security is signified by the trend of cyber-attacks directly aimed not only at industrial process control, but also at safety–critical systems in particular (Lee, 2017). Arguably, the scope for our endeavor into resilience for enhanced cyber security could be limited to the safety–critical OT systems guarding local health, safety and environment values. However, a controlled shutdown of an installation, which was earlier regarded a safe handling of a (cyber-related) disruption with an acceptable cost, will nowadays imply a threat to regularity, reliability and thus weaken the trustworthiness of the foundational national interest of gas export to Europe as referenced above (Norwegian National Security Authority, 2023). The cyber resilience challenge is therefore, ultimately, on the level of industrial (cyber) control for high reliability operation in a hyper-connected world, including but not confined to protecting OT safety–critical systems dedicated to ensuring safe shutdowns of singular plants or installations.

2. Aim, strategy and objective of the research

The overall aim of this paper is to empirically explore the potentials for cyber resilience in the Norwegian offshore oil and gas industry as a *case of* a hyper-connected cyber-physical system and increase the

conceptual clarity on how cyber resilience approaches can contribute to closing of the SAG in such systems. The research strategy is to explore the existing grounds and experiences from a sociotechnical perspective, acknowledging the potential positive human contribution and being aware of potential cultural differences between the IT and OT domains. We limit our attention to the combination of IT and OT, including protection of safety–critical systems, as the implications of hyper-connectivity expectedly raise the need for resilience in a very direct manner, also at this level. We make this limitation in confidence that increased insight at this level will have relevance for future studies of cyber resilience at a more business- and service-oriented level.

Several approaches to critical infrastructure resilience put alignment and integration with existing risk management practices as a key premise and goal (e.g. (Rød, 2020; Stavland & Bruvoll, 2019)). This appears motivated by the need for managerial attention, and resting on the presumption that the only path to managerial attention to resilience is through an assimilation with and extension of the institutionalized approaches to risk management. Our approach is different. We focus on adaptive capacity as a distinct type of phenomenon, which also clearly needs managerial attention. However, we do not see resilience and adaptive capacity as Homerian sirens that enforces us to bind our inquiry to the mast of risk management. Our emphasis on adaptive capacities rather than prescribed or standardized lines of action may appear to be abstract, academic, and distanced from daily work in cyber security, safety, risk management, and other relevant disciplines. Resting on the basic Resilience Engineering (RE) distinction between "work-as-imagined" and "work-as-done", our presumption is however that the core RE issue of adaptation – the possession of an *intrinsic ability to adapt (*Hollnagel, 2014*)* and the enabling conditions for it - is potential common ground between researchers and practitioners if we approach it cautiously. That is, we assume that the ability to adapt to some extent is already part of daily practice, despite that it is more than often banished to the shadows by the prevalence of compliance with rules and procedures to achieve safety and security (Grøtan, 2014). In our inquiry, we will seek empirical descriptions, signs, and traces of such adaptive practices, and their foundations. We also presume that any prospect of future progress on cyber resilience from a sociotechnical perspective will rely on, but also benefit from, coherence and connection with actual, existing (adaptive) work practices. We denote these presumed practices rudimentary resilience. Attempting to close the SAG without resonance with rudimentary resilience is regarded pointless. For that reason, our research strategy is founded on the exploration on how different resilience concepts relate to actual work practices, and practitioner's reflections on key (resilience) issues.

Resilience will however not unfold in a void. The Norwegian oil and gas sector is heavily regulated. In recent years, the cyber security issue and its potential impact on safety has gained increased attention from the Norwegian Petroleum Safety Authority (PSA), which also increasingly has employed terms and concepts that addresses the unexpected. E.g., the PSA states that preparedness for unforeseen events can be built by "robust solutions" with sufficient safety margins, as "a leeway which allows the business to handle unforeseen events" (Petroleum Safety Authority Norway, 2017, p. 19). Such concepts and statements may intuitively be interpreted to resemble resilience thinking. However, it is yet unclear to which extent this expresses an extension of risk management practices to include robustness and rebound capacity, or whether it actually addresses (and legitimizes) adaptive capacity in the RE sense. Our initial interpretation is on the former, despite that a study claim that RE has become a "hegemonic discourse" (du Plessis & Vandeskog, 2020) in safety issues related to the Norwegian oil and gas sector. We take the liberty to presume that their conclusion is based on a semantic confusion between robustness and resilience. However, if that presumption is wrong, we expect to be able to observe such a shift through our research strategy based on interviews with practitioners in the industry.

In any case, our research objective does not preclude that other, non-adaptive practices also contribute to safety and security. Given that there is a perceived need and potential for adaptive capacity to close the Strategic Agility Gap (SAG) and manage rapidly emerging cybersecurity risks in the oil and gas industry, a crucial issue is therefore how the principles of RE relate to and can be combined with other practices in the industry for managing cybersecurity risks, including how they relate to "resilience" concepts with different pragmatic meaning, emerging from other discourses. Hence, the overall research question that will be explored in this article is therefore: **How can different perspectives of becoming and remaining resilient contribute to closing the SAG related to cyber risks in the hyper-connected oil and gas industry?**

Regarding the closing of the SAG according to Woods and Alderson (2021) as an incitement for a resilience approach, and recognizing the variations in how resilience is framed in the academic community and the potential confusion related to this in the industry, we divide the overall research question into sub questions:

1) What are the established foundations for cyber resilience in the sector today?
2) To what extent does the industry recognize the need to close the presumed Strategic Agility Gap (SAG) as framed by Woods and Alderson (2021)
3) Is there a potential in the industry for developing adaptive capacities based on existing foundations, for closing the SAG?

Based on the introductory background above, we will in the next section present a theoretical framework accommodating various types of operationalization of cyber resilience.

3. Theoretical framework

3.1. Connecting agility and resilience

Woods and Alderson (2021) points to Resilience Engineering (RE) and adaptive capacity as a major step to close the Strategic Agility Gap (SAG). Originating primarily from the safety domain, RE is based on acknowledgement of complexity as a potential source of drift which may lead into failure, but which also provide fertile grounds for adaptive capacities that are needed to succeed in inescapably complex environments (Dekker, 2011). A prevalent definition of resilience in the RE tradition is that "a system is said to be resilient if it can adjust its functioning prior to, during, or following events and thereby sustain required operations under both expected and unexpected conditions" (Hollnagel, 2014, p. 183). To accomplish this, Hollnagel directs attention to an "intrinsic ability to adapt" under changing conditions (Hollnagel, 2011). Accordingly, a key aspect of RE is to recognise "things that go wrong" as the flip side of "things that go right", assuming that they are the result of the same underlying process. By turning the attention, understanding and efforts of improvement towards what goes right rather than unilaterally at the things that (might) go wrong, we *might* expect that the inherent performance variability that we have coined rudimentary resilience can be elevated into an adaptive capacity that absorb more change and disruption, and also allows us to exploit emerging opportunities. Hollnagel's (2009, 2014) operationalization of these resilience cornerstones, later denoted *potentials,* is expressed as four abilities; to respond, to anticipate, to monitor, and to learn. In this perspective, it is natural to think of resilience as a re-framing of the normal way of operation, simply paying more attention to "work-as-done".

RE has however emerged out of a safety perspective in which coincidence, randomness, underspecified work and unexpected sociotechnical combinations are the main sources of complexity. In the cyber domain however, the level of disruption must be expected to change radically. In addition to singular attacks and disturbances, we must also consider that inherent complexity might hide and even facilitate hostile, disruptive and subversive activity in a much more sophisticated manner

than the singular "hacking" event. The adversary might even be resilient in the sense of Hollnagel's definition, poised to constantly and patiently scout for opportunities and vulnerabilities to exploit. The obvious implication is an increased need for defenders to be oriented towards adaptive capacity, not resorting to passive defences against past or conceived incidents, and not limiting their scope of defence to generic robustness and the ability to rebound. The prospect of more advanced attacks and subversions however put additional strain on the adaptive capacity. We must therefore also ask questions on the limits of adaptive capacity. Resilience is thus not something organizations have; it is something they *do* (Woods, 2019), and cyber resilience will not be a "walk in the park".

Woods (2015, 2018, 2019) emphasise that adaptive capacities must sustain over time and display "graceful extensibility" in boundary conditions. That is, deal with situations beyond what is considered as normal performance variability. Most of the founding concepts of RE are generic rather than context-sensitive, but Woods (2018) takes this stance to the utmost position in search for adaptive patterns across domains by making a reference to the notion of the "adaptive universe", in which sociotechnical systems – and humans in them – must be constantly poised to adapt to ensure success rather than exhaustion and failure - "becoming stuck and stale".

From this, we can envisage that the turn towards cyber resilience as an adaptive capacity will be demanding. First, organizations need to recognize that they need resilience not only as another tool in the toolbox, but "as an intellectual and instrumental counterweight to an obsession with prediction" (Wildavsky et al., 1988). Moreover, it will require them to extend their capacity to adapt when surprise events challenge their boundaries (Woods, 2019). Cyber resilience will ultimately be about what they can cope with *despite not* being prepared for the unexpected situation that unfolds, rather than coping *because of* being well prepared based on prior anticipation or recognition.

Moreover, while RE as a safety discipline was founded on the presumption that front-line workforces ("work-as-done") understand more about the critical process than what the formal organization ("work-as-imagined") is ready or able to acknowledge, the events, constituents and dynamics of the cyber domain are by far more intangible and incomprehensible for the ordinary users than for the domain experts. Hence, the success of cyber resilience might rest on a narrower part of the workforce than ever anticipated by RE. On the other hand, when it comes to understanding the cyber-physical implications of events and incidents, domain knowledge will be even more crucial. To a substantial degree, these distinctions are formative for the needed collaboration between IT and OT professionals. In addition, when a diverse group of people act jointly on digital re-presentations of the physical world, there is always a chance that digital complexity may cause joint ignorance and forgetfulness (Grøtan, 2020), losing sensitivity to weak signals and small differences that actually might make a huge difference. Mutual understanding of the cultural differences between IT and OT professionals, guiding their sensemaking process, may be a crucial factor for joint success.

3.2. Risk and resilience affiliation; a possible deflection from adaptive capacity

RE is however not the only discipline in which the term "resilience" is applied in the broader safety domain. E.g., in both disaster resilience and critical infrastructure resilience (e.g., Linkov et al. (2022)) the term resilience is more narrowly focused on the rebound or recovery phase, on robustness, and on affiliation with traditional risk management practices.

One example of the latter is the US Department of Energy (DoE) Cyber Security Capability Maturity Model (C2M2) (U. S. Department of Energy, 2021) which describes operational (cyber) resilience as "*organization's ability to adapt to risk that affects its core operational capacities*", but also as "*an emergent property of operational risk management, supported and enabled by activities such as security and business continuity*" (p. 72). That is, resilience (the ability to adapt) purportedly emerges – apparently for free - from efficient risk management, emergency preparedness, and business continuity planning. In a related vein, the Norwegian Defence Research Establishment FFI (Stavland & Bruvoll, 2019) advocates an approach in which a key concern is to assimilate resilience into the risk management discourse.

With the absence of any argument explaining why this kind of experience increases the ability to deal with (fundamental) surprise in a complex context, the above risk-oriented assimilations of the resilience concept are rather contrary to the overall focus of RE which highlights the presence of adaptive capacities, rather than absence of failures implicating risk. It is beyond doubt that risk management practices can be foundational for design and planning of robustness, rebound and recovery processes, however Woods (2018, 2019) explicitly argue that focussing on robustness and rebound are deflections from the "real issue", namely adaptive capacity. Accordingly, a focus on robustness and rebound may jeopardize the adaptive capacities and lead systems to be more vulnerable to fundamental surprise, e.g., threats that cannot be foreseen and planned for. Woods (2015) coins this effect as "robust yet fragile". In that respect, Woods' stance resonates with Weick and Sutcliffe (2001) who point out that "coping with an event requires a different mindset than anticipating its occurrence".

Here, we do not reject the value of risk management affiliation, robustness and rebounding capabilities, but it is not sufficient for closing the SAG, and to avoid "being stuck and stale". The risk-oriented understanding of resilience does however enjoy a level of prevalence which we want to be able to recognise and reflect in our empirical inquiries. We therefore need a theoretical framework that spans wide enough to cover both the risk-oriented approach and adaptivity-oriented approaches, without hiding the potential tensions between them as expressed by Woods (2015) "robust yet fragile" warning. A major difference between these two main positions is that the risk-oriented approach seems to be more willing to place the rebound motif in the foreground. This manifests through the focus on a "resilience curve" (e.g., by Rød (2020); Stavland and Bruvoll (2019)) to signify the link between the risk management-based activities to build robustness to withstand disturbance, and the rebound and recovery process needed if, or when this is not enough. This stance corresponds with the prevalent IT security perspective that incidents are inevitable, hence effective incident management for recovery is the prime issue. For an OT professional focused on the integrity of a critical safety system, the consequences of downtime needed for rebound might be much less attractive.

Despite the semantic plurality of the term, in parallel with the increase in cyber threats, and along with digitalization and cyber physical systems becoming increasingly exposed, the concept of cyber resilience has gained increased attention within academia. The link to Resilience Engineering and adaptive capacity is however absent in most of the publications that mention cyber resilience in relation to critical infrastructures (Kilskar et al., 2020; Pettersen & Grøtan, 2021).

3.3. A "Resilience ABC"

As already indicated, the notion of "resilience" is widely used to address and characterise systems that exist in challenging environments, dealing with variability, disruptions, stress, shock, and surprise. Key properties associated with resilient performance include withstanding, absorbing, recovering and even returning stronger from unanticipated or abnormal stress and disruption. In various associations with critical infrastructures, the effect of resilient performance is often projected on a (valuable) function or service, from which a "resilience curve" can be deducted or imagined as a reduction and subsequent recovery of the (valuable) function or service over a time scale. Through this curve, the *outcome of* resilience can be affiliated with risk management, as an extension. However, the aspects and processes from which resilient performance is attributed varies largely, from material and technical

properties to organizational performance and human behaviour. For the latter type, the conceptual distance between RE and affiliation to risk (management) may be larger than for the former, as for RE, the potential human contribution in complex environments is related to the conception that performance variability, human sensemaking and ingenuity, rather than compliance with or violation of predefined rules, is the main issue.

To capture this diversity, Grøtan et al. (2022) propose three distinct types of theoretical attributions of the origins of a resilient cyber system, i.e., on how to obtain the ability to "adjust functioning prior to, during, or following events" in the cyber domain. These are denoted Theory A, B and C, respectively.

As illustrated in Fig. 1, according to Theory A, resilience is an intrinsic part of the outcome or function ("curve") in the form of, e.g., redundancy, algorithmic adaptation, or fault tolerance in a technical sense. In Theory B, resilience will result from organized and dedicated resources and plans, the combination of, e.g., risk assessment, emergency preparedness and business continuity, elevating resilience to an "umbrella" concept (Stavland & Bruvoll, 2019; Øien et al., 2018). Here, resilience towards the unexpected is presumed to emerge from preparation for the imaginable. In contrast, in Theory C, resilience is attributed to the intrinsic ability to adapt, an adaptive capacity that enables coping with complexity and fundamental surprise, and thus emerging from situated (work-as-done) rather than imagined practice (work-as-imagined). According to the ABC model, the example from the C2M2 framework mentioned above (U. S. Department of Energy, 2021) might be an example of resilience in the form of Theory B, where adaptive capacity presumably emerges (for free) from risk assessment, emergency preparedness, and business continuity planning. It is tempting to characterize this as "resilience-as-imagined". On the other hand, Theory C corresponds with Hollnagels' (2009) resilience cornerstones, and a sustained adaptive capacity incorporating graceful extensibility as described by Woods (2015). Hence, attention is directed to normal performance bandwidths of "work-as-done", but not at least to their boundary conditions. Theory C points to the adaptive capacity rather than the actual adaptations, and explicitly highlights human initiative as a resource rather than a liability.

The relation between Theory B and Theory C encompasses a possible contradiction and tension. Woods (2015) argue that the focus on resilience as *rebound* and *robustness* (corresponding to Theory A and B) for specific and imaginable disruptions, misdirect the attention to specific response strategies and away from what he denotes the real issues: adaptive capacities that are required to handle events outside the boundaries of what the organization is prepared for. That is, focus on rebound may direct attention to how specific disruptions are responded to and managed, rather than to the adaptive capacities. Attempts to improve the resilience of a system by increasing its robustness will inevitably imply an increase of the scope of events that the system is designed to respond to, i.e., for known failure modes rather than successful operational (adaptive) patterns. Key issues that might be lost are how resources and capacities are deployed and mobilized to manage a surprise, e.g., an event that is outside the scope of events that the system is designed to respond to. Woods' third resilience concept, coined *graceful extensibility* is therefore a form of adaptive capacity in which a system stretches in the face of surprises (Woods, 2015, p. 7). Moreover, graceful extensibility is not limited to the rebound phase, but also includes the ability to foresee bottlenecks and potential disturbances in order to adjust responses in general.

3.4. Important intersections: Organizational and operational origins of resilience

Grøtan et al. (2022) further denotes the difference between Theory B and Theory C as the difference between organizational and operational resilience. This difference highlights not only the underlying logic of attribution of resilient performance, but also that the contributions originate from different loci in the overall system.

Hence, Theory B casted as managerial or *organizational* resilience signifies the presumption that resilience (in the sense of robustness or rebound) will result from personnel obeying rules and procedures ("work as imagined") developed through organizational and managerial processes of risk assessment, emergency preparedness and business continuity. "Obeying" may also imply modifying, bending or even breaking rules, but according to limits and criteria preconceived or imagined by the same organizational and managerial processes. In a broad sense, this also resonates with Leveson's (2020) concept of

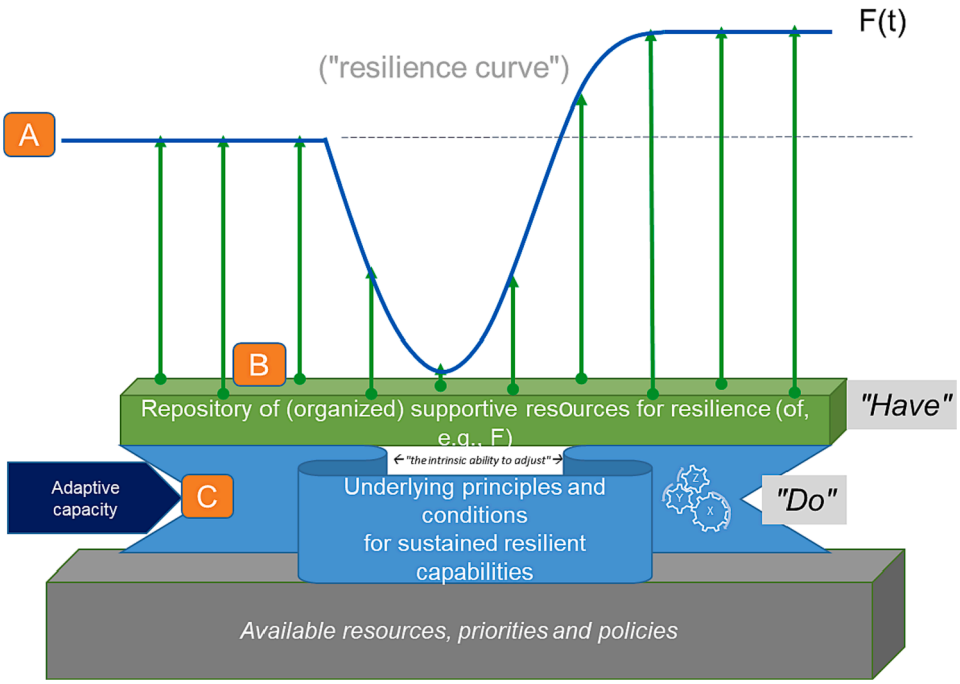

Fig. 1. Three types of origins of cyber resilience. Adapted from Grøtan et al. (2022).

"Safety-III", which emphasizes technical design to support people in preconceived situations. In contrast, *operational* resilience (Theory C) implies that the dynamics of the adaptive capacity emerges from a practitioner's sociotechnical and situated perspective ("work as done"). Here, rules and procedures are seen as resources but not obligations, and their bending and modification is only part of a broader repertoire of actions adapted to and from the actual situation. As an example of the implication of this distinction, the expectation of operational resilience emerging ("for free") out of operational risk management (U. S. Department of Energy, 2021) just cannot take place without employing both organizational and operational resilience in conjunction. The distinction between operational and organizational resilience also resonates with key traits for RE; seeing humans in the systems as a source of success, acknowledging that systems work because of humans' ability to identify design flaws and glitches and interpret procedures to match conditions and detect and correct situations that are about to go wrong (Hollnagel, 2014). Accordingly, too much organizational resilience will be a straitjacket for operational resilience (raising the stakes for becoming "robust yet fragile"), unless operational management is very closely engaged in day-to-day operation and monitoring. Nevertheless, operational resilience is beyond the grasp and reach of the managerial processes of, e.g., risk management and emergency preparedness, but these processes are in control of the resources, priorities and policies defining the framework conditions for the adaptive capacity. Hence, both the overall Theory A, B and C distinctions on attribution of resilient performance, as well as the distinction between organizational and operational resilience, constitute demarcation lines with respect to the grounds from which the SAG can be closed. Put simply, organizational resilience (Theory B) is necessary, but not sufficient in terms of effectiveness, and may impose a brittleness towards operational resilience. Theory C is therefore also necessary for effectiveness, but without a proper coexistence with Theory B, it may not be efficient, "inventing the wheel" again and again. Hence, a key implication from this framework is that the hypothesis that Theory C must be implemented in the context of Theory A and B. There is no either-or option.

Finally, this framework also highlights (as depicted in Fig. 2) that resilient performance does not come for free. It is not a walk in the park, it might be demanding and exhaustive. There is no guarantee for success, and it might be necessary be able to "stop in time" to avoid the cost of the treatment overriding the cost of the disease. The ultimate implication of the ABC model is also a dividing line regarding to which extent resilience is a phenomenon worth vile to study and develop on its own terms:

- Theory A and B implies that resilience is merely an epiphenomenon, an "umbrella" concept limiting attention to resilience-as-outcome (Stavland & Bruvoll, 2019), an outcome that emerges solely from practices of design (Leveson, 2020), risk management, emergency preparedness and business continuity planning.
- Woods (2015) warning of being "robust yet fragile" may thus be paraphrased as the implications of not taking the need for adaptive capacity seriously, by so to say enacting deflection by seeing resilience as an epiphenomenon.
- On the other hand, Theory C addresses resilience-as-process on premises acknowledging complexity as a major issue also for designed, sociotechnical systems, quite contrary to the way, e.g., Leveson (2020) positions the relevance of complexity theory as mainly limited to "natural" systems, not designed for a purpose. However, in Theory C, there is no attempt to hide that also resilient practices may be fallible, brittle or fragile. But it is a different kind of fragility than "robust yet fragile".
- Theory A and B are event-oriented, and thus prone to sequential attribution and phasing of resilient performance to different underlying phenomena (e.g., anticipation (that eventually fails), robustness (that dampens the loss of performance), recovery (to restore functionality) and adaptation (to avoid similar events in the future) as, e.g., by Rød (2020) adapted from Linkov et al. (2014))
- Theory C is not bound to such a timeline. As put by Woods and Alderson (2021), it is about being poised to adapt at any time, regarding resilience as a "verb in the future tense" (Woods & Alderson, 2021, p. 7)

3.5. Closing the SAG through Theory A, B and C

For highly complex critical infrastructures, the primary strategy according to Woods and Alderson (2021) have been modeling and simulations to analyze infrastructure and identify, assess and prioritize vulnerabilities and consequences in order to find correct measures to mitigate risks. This may be paraphrased as Theory A and B oriented processes of technological and organizational resilience. However, the scientific, technical and practical limits due to growth in complexity "leave organizations stranded in the Strategic Agility Gap" (p. 6), which represent the difference in how fast an organization may adapt to change and the emergence of new unexpected challenges. To cope with change and unexpected challenges, organizations need to develop and maintain adaptive capacities. In other words, operational, situated Theory C contributions need to be brought to the fore as a proactive sociotechnical capacity of the organization, not only residing in the shadows of Theory B. Interestingly, Woods and Alderson (2021, p. 9) suggest that there are three critical capabilities to support the adaptive capacity in order to narrow the Strategic Agility Gap. We argue that these three also indicates a strong relationship to the Theory ABC model:

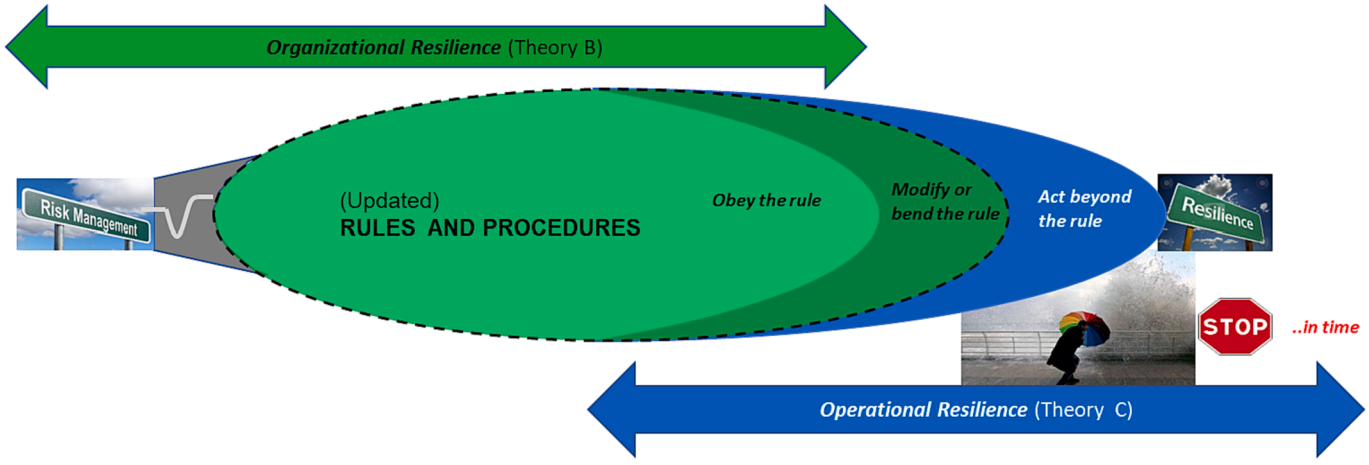

Fig. 2. Organizational and Operational Resilience (Grøtan et al., 2022).

- Woods and Alderson points to "the ability to **revise previous models** and methods to recognize emerging new vulnerabilities as interconnections change"; *this implies that Theory B (organizational resilience) needs to know its boundaries and limits to avoid becoming "robust yet brittle", and that there must exist a supplementary capacity with a different logic to create the new (*i.e.*, resembling the role of Theory C)*
- Woods and Alderson points to "the ability to **synchronize activities** over multiple roles and layers of a network to scale responses to the scope of challenges"*; this is consistent with the assertion that Theory B is organizational, and Theory C is operational,*
- Woods and Alderson points to "the ability to **anticipate challenges ahead** to recognize emerging new challenges, vulnerabilities and threats before capabilities are overloaded or oversubscribed." *this process of anticipation may be associated with both the presumed fragility of Theory B, but also the inherent limits of Theory C as a fallible practice.*

4. Methodology

This paper is part of the TECNOCRACI project which is dedicated to investigating to which extent resilience concepts can be useful in the (IT/OT) cyber domain as an extended protection towards complex vulnerabilities and an increasingly aggressive threat landscape. This exploration does not take place in a theoretical void, it can draw on a number of promising concepts from other domains, but none of them are considered sufficiently mature to be a basis for deduction and elaboration of practice in the cyber domain. At the same time, our presumption is that also in the cyber domain, adaptive practices (rudimentary resilience) exist out of sheer necessity, and that theoretical progress on this will benefit from "connecting" with these practices through empirical investigations, and subsequent theoretical reflection. This calls for an abductive research approach.

The overall issue of this paper is to explore how the different perspectives of becoming and remaining resilient in the management of cyber security are reflected in practice, and how we can utilize these findings for closing the SAG in the oil and gas industry.

The research was initiated by document review of relevant standards and industry reports followed by interviews with representatives from the industry. The purpose of the interviews was to understand how the industry works ("as done") to manage cyber risk, without being biased by the "imagined" way of working. The informants were either employed in oil companies or working in consultancy or advisory service companies working for the industry, either with the management of OT systems, IT systems or both. The interviews were performed using a semi-structured interview guide and lasted approximately 60–90 min each. The topics in the interview guide were developed for us to obtain an understanding where cybersecurity work is going on and how this work is organized, how the organizations worked with standards and guidelines, how the informants assessed their ability to prepare for and prevent cyberattacks and necessary adaptations in this work. In total, eight interviews were performed. Six of the interviews were performed during November and December 2021, while two interviews were performed in late May and beginning of June 2022. The informants all had extensive experience and knowledge within the field of OT and IT operation in the oil and gas industry. The interviews were performed digitally, recorded and transcribed verbatim. The transcribed interviews were organized and analyzed through the qualitative data analysis software, NVivo.

The data analysis began with an open coding process. In order to not impose own theoretical understanding on the informants, the informants own terms were used in formulating the initial codes (Gioia et al., 2013). The preliminary concepts were formulated as gerunds, further directing the analysis into the informant perspective (Charmaz, 2014). In the next step, the initial codes were compared to find similarities and differences. Examples of codes are "Ability to prepare for successful attacks", "Establishing controls", "Managing situations with increased risk" and "Capabilities for adaptations". After the initial coding, the data analysis transitioned from being inductive to a form of abductive research, through consulting the existing theory on cyber resilience as a source for discovery of resilience in practice. The grouping of codes emerged based on the observation that the initial codes represented activities that clustered together represented activities within the resilience phases, as defined in the resilience curve (Stavland & Bruvoll, 2019). The fifth phase "adapt and learn" is not included as the data material did not reflect the material for this phase.

While the interviews and the data analysis has been the basis for investigating the three first research questions, the material has been analyzed from different perspectives, as summarized in Table 1 below.

5. Findings

The chapter presents the data analyses, where interviews have been the primary source supported by industry reports and audit reports from authorities.

The empirical context common to the interviewees is illustrated in Fig. 3. There is currently a large focus on digitalization in the petroleum industry, and the industry is increasingly getting more dependent of digital systems and technology. According to Gressgård et al. (2018), the development is primarily related to remotely and autonomously operated equipment and vessels, integrated operations where operations or selected systems on the facility can be performed from shore, autonomation of drilling operations and the gathering of data and use of software and data analysis to increase production efficiency, maintenance as well as safety of operations. The digitalization implies that Information Technology (IT) is connected to Operational Technology (OT) which is defined as technology that supports, controls and monitors industrial production, control and safety functions (Hanssen et al., 2021). The table below includes a short description of the type of systems included within IT, OT and physical equipment, and key characteristics of these systems, providing an overall context for the discussion of the findings. Fig. 3).

The findings are organized into the four first resilience phases in the resilience curve (Stavland & Bruvoll, 2019), i.e., describing the activities performed to manage cyber security in each phase.

5.1. Understanding risks

The subchapter describes findings from interviews regarding the activities informants carry out to obtain an understanding of potential threats and their likelihood, and the informants system knowledge.

Several informants shared the view that the risk understanding is distributed among actors, and one informant used the three-factor model as a basis for his explanation. The three-factor model states that the total risk may be understood by evaluating the threat, the

Table 1
Research method along sequence of research questions.

RQ no.	RQ Description	Method for investigation
1	What are the established foundations for cyber resilience in the sector today?	Document studies Interviews. Analyses based on the overall theoretical framework. Looking for traces of resilience from a Theory A, B and C perspective.
2	To what extent does the industry recognize the need to close the Strategic Agility Gap	Interviews. Analyses based on the overall theoretical framework. Looking for examples of SAG-related issues.
3	Is there a potential in the industry for developing adaptive capacities based on existing foundations, for closing the SAG?	Interviews. Analyses based on the theoretical framework, with emphasis on the Theory B and C interaction.

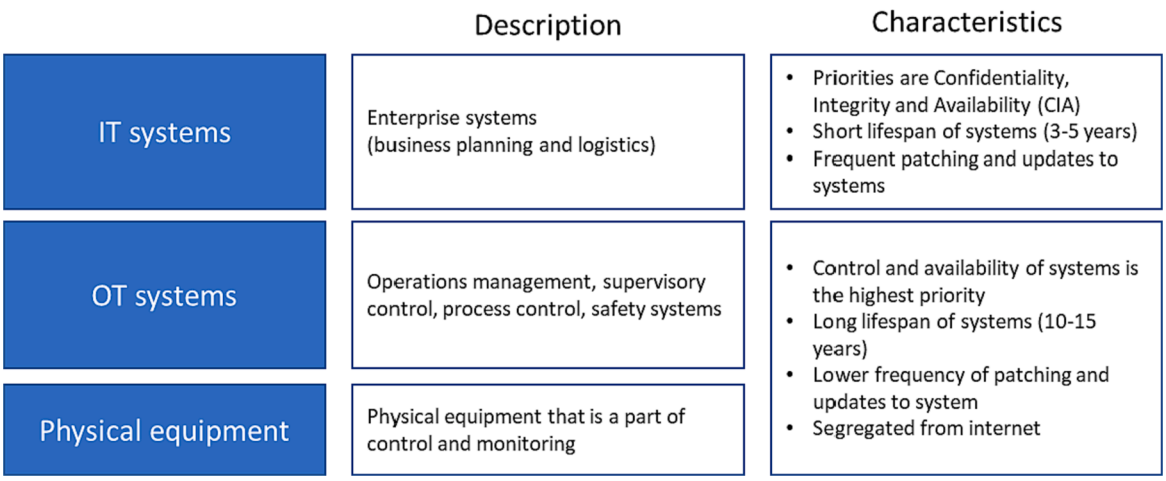

Fig. 3. Description of IT, OT and physical systems. Based on Jaatun et al. (2021).

vulnerabilities and the asset value. The risk understanding is distributed as different actors hold different understandings of these three elements. While the threat actors themselves hold the most accurate view of the threats, national security agencies and security companies also have overall representations of the threats. Vulnerabilities and how to exploit them is best understood by the IT-professionals in the company, while the asset value is best understood by the OT professionals and the ones working on the facilities often referred to as those 'sitting on the bomb'. The 'asset value' involves the consequences of a breach of availability, integrity, and confidentiality. The differences in risk understanding would typically come to the surface in situations where the IT workforce would like to push through typical IT controls (such as continuous patching of vulnerabilities, only personal account etc.), while the OT workforce saw it as an increased risk for loss of availability of production, increased workload or not possible to implement in a practical manner. As illustrated by the following quote:

Informant 4: *"(…) For example that you should change the password every third month, you should have personal admin accounts. We estimated that if, out on one our facilities there is no Active Directory (AD), and we might have 100 different servers offshore. If someone were to go out and change passwords every trip offshore, he wouldn't do anything else for 14 days. (…) We have the same wish of following the security principles within IT, we want the same controls. But we sometimes have to implement them differently."*.

To compensate for this difference in perspectives, clear boundaries for areas of responsibility was considered necessary, but also bringing resources together in assessments. The informants shared that they found risk assessment processes within the cybersecurity domain as challenging, particularly evaluating likelihood of specific events. There were also indications of that the risk was differently evaluated with regards to digitalization initiatives. One Informant described that bringing in more IT into safety and process control systems led to more uncertainty and complexity in systems and could make it more difficult to set stop criteria. Another Informant described that "OT-people" were in general more skeptical:

Informant 1: *"(…) Those who work with OT systems are much more skeptical in general, than those working with IT. The "requirement" to push data to the cloud does not come from OT. (…) None of them see the real benefits of it yet. And in addition, if you would harvest the real benefits of it, then you have to push data back into the system, and then the "cup of vulnerabilities" is something else than just pushing data out. So, OT-people are in general more skeptical than IT-people."*.

After the cyberattack against the Norwegian Parliament spring 2021 and other attacks, cybersecurity experts have warned that it is impossible to fully prevent cyberattacks, and that organizations should increase their efforts on minimizing damage through emergency preparedness and business continuity processes. The ability to avoid cyberattacks were also discussed in the interviews, and the participants were directly asked if they believed that it was possible to fully prevent cyberattacks. As illustrated by the quotes below, informants seemed to share the view that it was very difficult to fully prevent, especially if an attacker was sophisticated enough.:

Informant 3: *"The answer to that is clearly no, but I believe we should discuss the causes. (…) I would believe it would be more difficult when your systems are secured in the way ours are, but if the attackers have the right resources and capacities, they will succeed in unbelievable ways, although it is not easy."*.

Informant 5*: "Our experience, based on having SOC (Security Operations Centre) operating (…), is that yes, but not against everything. If advanced threat actors would like to harm us, we would struggle, and I believe most would do."*.

Thus, informants experienced that the measures that were implemented were effective, and prevented most attempts, but that one could never be fully protected due to weaknesses in controls or an insider threat facing an attacker with advanced capabilities.

5.2. Preparing and anticipating

The subchapter describes findings from interviews regarding the activities the informants carry out to anticipate and prepare for cyberthreats, specifically how the informants decide what security measures that is to be implemented and what digitalized solutions that should be permitted, and the evaluation involved in these processes.

The uncertainty experienced when evaluating risks propagates to when preparing for resilience in the form of establishing controls. Informants expressed that it was difficult to find a good balance in measures. Some informants considered that one could always be stricter, but also that implementation of additional controls would impose higher costs, or reduced income in case of production shutdown. One example that was highlighted was automatic removal of potential viruses. A false positive may remove critical files for the control system, and thereby cause loss of availability of production as illustrated by the quote:

Informant 4*: "We have detection only, or monitoring only, on some systems. That means that if someone plants a ransomware, it will spread. We have turned off removal, so even if it detects it, it will spread. It is a calculated risk. But the alternative is that [the control system vendor] (name removed) or others pushes out a new software, and then the antivirus removes it because happens to match a signature, so it believes it is a virus. We believe that that risk is larger, because we've seen it, that there has been false positives and files have been removed."*.

Other informants shared that some measures would increase control and overview but could also actually increase the attack surface. Other

informants expressed that the difficult part with cybersecurity was never knowing when it was good enough, and in the end, it boiled down to how much resources that the company was willing to spend. However, the informants experienced that available industry standards were very useful in this work. Particularly the Recommended Practice (RP) "Cyber security in the oil and gas industry based on IEC62443" (DNVGL-RP-G108) developed by the industry in a Joint Industry Project, led by the company DNV. According to informants, the RP represent a more practical approach to the principles described in IEC62443 which was considered easier to understand and implement which fits well with the way the industry is working with cybersecurity, rather than the standard which is described as more theoretical and very time consuming to grasp. Others used the guideline from the Norwegian Oil and Gas Association, Guideline "104 – Norwegian Oil and Gas recommended guidelines on information security baseline requirements for process control, safety and support ICT systems" (Norwegian Oil and Gas Association, 2016), as a basis for an annual review of all facilities which they experienced contributed to continual improvement of cybersecurity. A positive side effect experienced from working with standards, was increased awareness among the personnel working to implement controls, from better understanding of the reason for implementing controls. Others expressed that the standards eased the implementation within the organization, and that there was less resistance towards measures if implementation was done with basis in a standard.

The importance of not increasing complexity was also brought up by several participants, as a factor to evaluate when selecting and dimensioning cybersecurity. The informants were worried that if they added more complexity in the form of advanced monitoring or other tools it would be difficult to maintain overview and make the systems less predictable:

Informant 3:"*If you have to many variables, you may lose control because when some variables occur on the same time, you may have consequence you would not have foreseen. And that is something that I am a bit afraid of, what I feel is something of the balance here, in what tools I should introduce. (…) One example is monitoring, (…), in order to get better asset information, for all our OT systems. On third party systems, (…) we chose [name of system removed], a simpler, less complicating and not that comprehensive. Instead of a large complicated system that would be used in IT. So I am always a bit, I am positive, but I hold back a bit, I will not be the front runner, and not go to the most complicated solutions because it can get too complicated"*.

Some shared that they deliberately chose old technology, because failure modes were understood, and operators would have a better possibility of understanding what's going on and find the correct measure in case of errors. As illustrated by the following quote:

Informant 7: (…) they chose proven technology, or they keep proven technology in the form of very old IT systems. So, they are well known, but not as robust. But they are predictable, they have Windows XP, Windows 2003 and maybe Windows 98, but it is predictable that they will have a blue screen or have memory loss. So, it is something that operators and engineers understand, and it is just a restart required and it will be 10 days until the next blue screen. But with newer systems with machine learning, big data, windows 11, with advanced algorithms, we are not able to understand the weird outcomes that one may experience.".

To clarify our understanding, the informant was asked if it was better to have proven but old systems that might come with vulnerabilities. The Informant argued that the events that will occur in an old but proven are predictable and "known knowns", i.e. identified in risk assessment and understood well enough so that procedures and plans can be established to manage such events. If the complexity was too high, the result will be 'unknown unknowns', events that would be difficult to predict in risk assessment and understand how to manage. The Informant argued that the uncertainty associated with newer systems is too high when the downside risks are loss of lives or the facility.

The informants identified several opportunities unleashed by digitalization. In the oil and gas industry, the opportunity to work remotely was considered to reduce both costs and accident risk exposure, for instance when a service engineer from the US may do necessary maintenance on the control system remotely, instead of travelling offshore to the Norwegian continental shelf. Other digitalization initiatives involve gathering data about operations and systems to optimize maintenance or forecast the safety of a facility. The informants seemed very aware of that although the initiatives come with large benefits, there are also risks connected to allowing access to systems and exporting data. All companies had done a thorough evaluation of whether they would allow for remote work, and while some ended up not allowing for remote work accessing control systems, others had implemented strict controls for regulating access management with several gate keepers. The consequences of not having control of remote work could lead to both safety consequences, due to conflicting work, and security consequences, if unauthorized personnel were to obtain access to the control system. The offshore personnel therefore had a critical role as gate keepers, and it was stressed by the informants that offshore personnel were instructed to not grant access "if they were uncomfortable with the situation". As illustrated by the quote:

"Informant 8: (…) It is important that our employees understand, "this is suspicious", that you are attentive towards (…) unusual things, things that seem strange. We see from time to time, it happens when new users are getting remote access, if it is then users that they are not familiar with, or if they believe it is strange that personnel are getting access on a Saturday, then I have been sent questions regarding that. "Who is this person, it seems a bit strange", and they do an extra check. We have become a bit like that, everyone in the company. ".

Awareness among offshore personnel regarding cyberthreats was therefore seen as important.

The informants had also established plans and procedures for cybersecurity events and reported that the procedures to a large degree covered the scenarios and situations that occurred. There were however need for operating outside the procedures from time to time. One element that several were aware of was that over time, assumptions made regarding how the system functioned might not be correct anymore. As illustrated by the following quotes:

Informant 5: *" We have implemented several security tools, but then there are users that have needs that does not fit completely, and then you have to make an exemption, and in the end you make a lot of exemptions from many security tools, which then again, if you have a risk picture and that security control should mitigate that risk, then you have drifted and have a higher risk than what you believe. "*.

Informant 4*: "We believe that our firewall is intact, because we have control over the changes. But it is not always like that. The control of the firewall status is often weak (…) because you haven't done audit and you don't have a real time analysis."*.

Other examples were that procedures or instructions developed such as the backup procedure does not work because someone changed the backup system, or that a new system was brought in that does not fit into existing rules and exceptions are made, and not necessarily documented.

5.3. Absorb and withstand

The subchapter describes findings from the interviews regarding the activities the informants carry out to absorb and withstand cyberthreats, specifically through managing situations with increased risk, and how potential incidents are detected and managed.

Situations with increased risk are situations where no incidents have occurred yet, but there are weaknesses or conditions in place that might increase the likelihood or the consequence of an attack. A recent example is the Log4j vulnerability, where it for many of those affected was unclear whether they were exposed or not. Faced with vulnerabilities such as the log4j, organizations need to understand the impact and evaluate measures to implement until a patch, typically a software update, is available. With regards to the Log4j vulnerability, to avoid exploits, the Norwegian National Security Authority advised organizations

to take down services until patching was possible (Norwegian National Security Authority, 2021). For some organizations, particularly those responsible for delivering functions critical for society or in organizations where the cost of unavailability is high, such as the oil and gas industry, the threshold for shutting down services is high. Upon incidents like this, the process typically starts with a mapping:

Informant 6: "*When a zero-day or another critical vulnerability appears (…), the process is quite generic. We start with a mapping, to figure out whether we are affected, and then go into dialogue with those who operate those systems to check if they are in control, or to what degree they have control. If they are affected, we ask what they do to mitigate the situation (…).*".

Another informant pointed to that during the management of the log4j vulnerability, a lot of organizations learned that they had difficulties investigating whether they were affected or not. «Knowing what you have», or asset inventory management is an essential part of information security management, and is a requirement in both ISO27001 (ISO/IEC, 2013) and a part of the Norw. National Security Authority's basic principles for information security (Norwegian National Security Authority, 2020). And according to the quote, many companies experienced that their overview was missing.

Informant 1: *"(…) during the management of log4j, that was a really large vulnerability, then most discovered that, firstly, they didn't know where they had it. They had to ask their vendors if it was installed on their systems. They did not know where they had it, if they had it, and they had no way to find out whether they were vulnerable or not. (…) It was not as vulnerable as it looked like in the first place, but that was just luck. It could have been much worse. But it made companies discover that they lacked this and that, and overview. And also, when the vendor says, "now it is fixed", how can we verify that?"*.

After the invasion of Ukraine early 2022, the Norwegian National Security Authority (2022) (NSA), posted a warning that advanced threat actors and criminal groups might pose a threat against critical infrastructure and both the National Security Authority and the Petroleum Safety Authority Norway (2022) proposes measures to prioritize in response to potentially increased threats in the petroleum sector as a consequence of the war in Ukraine petroleum sector. In essence, the proposed measures were the same as referred to normally (e.g. for the oil and gas industry the guideline from the Norwegian Oil and Gas Association (2016) and for IT in general the basic principles of ICT security given by Norwegian National Security Authority (2020)), but companies were asked to increase their vigilance and given prioritized list of measures to reinforce the control of. One of the informants shared theirs's response:

Informant 2: *"We were luckily in a position where we felt that we were in control and had already done a lot. We've had penetration tests and audits, and closed the gaps identified. (…)"*.

The organization were therefore in a position that, based on many security initiatives during the last years, enabled them to focus on checking and reinforcing key controls, and reassuring both operators and management to avoid panic.

Informant 2: *"A lot of my work in this phase were to reassure those around us. (…) In the control room with operators and those working there (…) because there were so much written in the media about everything, we had a session the first 14 days (…) to inform them about what they actually work with, and all the things that they cannot see in their daily work but which is operating in the background, and what we have done so far. (…) And it was also up for discussion in, in the management in the company, my job was to reassure those too."*

Another example of a potential hazardous situation that was brought up during the interview, was a situation where there was a virus observed in a platforms' non-critical systems, and despite this the organization was able to continue normal production after a thorough evaluation in cooperation with vendors:

Informant 4: "*Our main priority was to protect the main control system. There were no signs of attack and there had never been any signs. And secondly, it meant nothing to us whether the (affected) system was up or down. (…) It was a discussion between owner and vendor and we agreed to remove it the next time we went out. It was considered low risk. Low risk for the (oil) production and the rest of the field. We normally do assessments that way. But now we are in a lucky situation, for most fields, the network is segmented."*

For many safety incidents, it is often clear whether you have an incident or not. The criteria for confirming gas leakages are normally that two detectors are triggered, while other incidents may be more directly observable. For cyberthreats, the picture might not be that clear, and in many situations, organizations and systems are breached but the attackers go undetected for a long period of time. Most of the informants interviewed had implemented some form of monitoring of OT systems, either internally or via an outsourced Security Operations Centre (SOC) or Security Incident and Event Management (SIEM) service to detect threats early. According to informants, the most common way of detecting potential incidents would be through the SIEM solutions, which again would notify the organizations. The technical monitoring solutions, typically consisting of network and/or endpoint monitoring is set up both to deny all other traffic than traffic defined on the "allowlist", and to recognize "signatures" of attack techniques and vulnerability exploitation. The challenge with these monitoring solutions, is that the quality depends on what is added into them, and consequently "what you look for is what you'll find" and the things you cannot imagine will not be detected. One informant raised the point of "defenses in dept" with regards to monitoring:

Informant 1: *"(…) you always need more places to detect. Because network is one part, but you also need something on endpoints, and be able to observe it on your network equipment, typically firewall logs, so when you have those, not firewall logs necessarily but all types of logs. When you have those three, you have a much better overview, and if you then could see and correlate events on those three, you will have a pretty good overview."*.

If an attack goes undetected by monitoring solutions, there is a potential for an attack being detected by the control room personnel offshore. The role of the control room personnel is normally to monitor the production process and monitoring status of control and safety systems. The personnel are tuned in on looking for irregularities in the operation, "things that seems strange", through wariness. Some informants expressed that, based on this role and the awareness, the control personnel would quickly detect abnormal situations. Although the control room personnel would not immediately suspect a cyberattack, they would bring their concern forward to the offshore automation engineer or other specialists to examine the situation further. If the situation remains unexplained, OT resources onshore would be involved and further the SIEM vendor and/or control system vendor. It was therefore seen as important to building awareness to establish, as one Informant expressed it, "wariness" to things that seemed different from normal operations, and by that detect potential attacks early and avoid larger events.

Informant 1: *"A really easy thing to do is ask the operators "would you react to this as an IT-security event, or would you think that something was wrong with your equipment?". In 100 % of all cases they will respond that "there is something wrong with the equipment". (…) It is natural, because it is operation and availability which is "alpha and omega", and that is what they live for and it has been instilled into them for decades"*.

The Informant further stressed that operators should be given training that enables them to easier identifying attacks. Informants however seemed to disagree whether detection by control room personnel was a realistic scenario, especially where sophisticated methods are applied, such as modification of the Human Machine Interfaces (HMI) on the control screens, to deliberately mislead the control room personnel.

Informant 4: *"I believe that the human factor is limited, in sophisticated hacking at least, but not in many other scenarios, where it is observed that things are not going as they should. And that's what we are trying to teach in cybersecurity courses, to report if you see something abnormal. (…) I am*

skeptical that we can protect ourselves from on that level (sophisticated hacking). But of course, on many other levels. Who you give access to, what you ask people coming offshore about. It is an enormous potential for personnel being aware and report issues.".

Other informants highlighted the importance of the humans in the system experiencing something out of the ordinary, without getting the information from sensors and detectors, but based on intuition and understanding developed based on experience from working with the physical systems in daily work, perhaps via noise, vibration or other sensations.

Informant 7: *"We talk about that in the oil business, that operators out there know the facilities so well that once they are onboard they feel that something is wrong. But is not vibration, it is not temperature and it is not sound or anything that sensors can detect, but the operators that have lived with these facilities for years, they feel in on their gout (Norwegian expression)"*.

Informant 8: *"A lot can be done in a cyberattack, that may not be detected for months, and maybe it is the control room that first detects that something seems abnormal. And they will contact the SAS (the one offshore responsible for Safety Automation System). (…) A type of event like that will typically be escalated, and then emergency preparedness resources are scrambled, and all, control system vendors, it-vendors and 1., 2., and 3. Line"*.

5.4. Respond and recover

The subchapter describes findings from interviews regarding the activities the informants carry out to respond and recover from cyberattacks, through preparing and planning for incidents and how they organize for managing events when they occur.

All companies interviewed had developed plans and procedures for cyberattacks, including plans for both the shore and offshore organizations. Emergency preparedness and business continuity is an essential part of cybersecurity, and as presented earlier, the informants seemed to share the belief that it was impossible to fully prevent cyberattacks. Being prepared for the handling of potential attacks is therefore seen as important. The preparations include both establishing a plan that included an emergency preparedness organization, and training. For recovery, the maybe most important, and simple measure mentioned was an offline backup. But backup alone is not enough, organizations need to ensure that they also practice on using backup for restoring systems, and that the restoration procedures are effective.

For the offshore organization, cyberattacks were included as a part of the companies 'Defined Situation of Hazard and Accidents' (DSHA), and thereby included as a part of their regular training regime. All informants reported that they had frequent exercises on the emergency response procedures, often involving both onshore and offshore resources. The value of the exercises was found in better understanding of systems, roles and responsibility and communication between roles, exemplified in the following quote:

Informant 6: When there is a drill, one needs a specific scenario to practice for the drill itself. (…) But what we really practice is incident management. Independent of the scenario. We could have sat down and listed down quite many scenarios, and practiced those, but we wouldn't do anything else. And still we wouldn't practice the scenario that in the end hits us. (…) We practice roles and responsibilities, communication between roles and responsibilities. Who is involved, where does the instructions come from, what is the decision basis? So, interaction between the involved parties".

The informant stressed the importance of having an open mind in these exercises in order to not interpret an anomaly or strange event into something known and to build the response strategy on wrong terms:

Informant 7: *"Within the oil and gas industry, the training is to improve robustness, and on known events, and I believe I see tendencies of when you then bring out an anomaly, a crazy anomaly, to practice that, those who have practiced robustness the most and has it as a reflex immediately interprets the scenario into what they already known. They try to interpret it into an existing DSHA, and manage the event on autopilot. And that's what we don't want them to do."*.

The informants described the incident management process as multidisciplinary, and some as a "source for resilience" when bringing in personnel with varied competence. Within the operator organization resources include operators and management offshore and IT and OT responsible onshore. Resources outside companies, would typically include the control system vendors, SOC, SIEM or other security services, and in some cases also security authorities.

Informant 7: *"I have seen many examples where it is the operators offshore that really make the difference, those who know the machinery and the factory and the daily smell of the factory, they can make a big difference. But in the next situation it might be the IT-people that are able to explain the numbers that the operators see on the screen."*.

Cooperation with other organizations was governed by agreements and bridging documents or common procedures between the companies, and a key element of the emergency preparedness plan is to notify vendors and secure the availability of resources. If an incident was confirmed, it was the Offshore Installation Manager (OIM) which held the overall responsible for safety and operations and together with his/her team that determined the response strategy in case of incident. In order to determine the best strategy, the offshore team was dependent on support and advice from onshore resources. Examples of measures could be to shut down production, initiate the General Alarm to muster personnel, and in worst case, to evacuate the platform.

Informant 8: *"It is the OIM that has the responsibility. In an emergency, the OIM is the emergency preparedness leader. And if one sees that the situation might not go well, then the facility is shut down, and they go to shut down mode immediately, based on how they assess it."*.

Informant 2: *"What we are really clear on is (process) integrity, and it is the emergency preparedness leader (local), which is the decision-making authority."*.

With multiple actors involved in the response, clear communication lines were by one of the informants raised as an important issue.

Informant 2: *"I relate to the local emergency preparedness leader, and the SOC. The SOC team does not have contact information to local personnel on site, in order to shield them. So, I will get information from the SOC, they will contact me, they will never call the control room. Then I will make further contact, and then I would contact the SAS team (…) to check out things, and then eventually escalate things"*.

Although the organizations have external resources available, it was seen as very important to have specific system understanding and a critical mass of competence inhouse.

Informant 2: *"We have an agreement with [control system vendor] that will help us, in addition to having own resources. But if we experience an attack, the IT side will probably be the first thing to go down. And then you will struggle with external support. You need some competence to manage it locally. "*.

Informant 4: "*We have a contract with [external resources], that will assist in emergencies. (…) But in addition, we need an inner trained core that can organize, and that understands the consequences, what is important and what is less important. Technical competence is not enough, you need good system understanding of how things are connected and what is important. (…) It is an element that must be in place. You cannot have an army without any local knowledge, you need a team that knows the facility (…), that is a precondition"*.

Several informants stressed that potential events would most likely play out very differently than envisioned or planned for, and the management of incidents and the potential combat strategies would require adaptations. Based on that adaptations were required; the participants were also asked what the enabling factors for adaptations were. Sufficient resources, experience and knowledge of systems were by several described as described as crucial:

Informant 1: *"It is primarily a question about resources. You need, what shall I say, enough resources to do something unforeseen. (…) When all is cut down to the bone you have no buffer capacity (…). That is the first part. But*

beyond that (…) it is the boring answer, the boring part about if you "know what you have", you have control of what's going on, you have practiced and you have plans, then you will be able to make yourself flexible enough. Then you can do most things. But you will also discover, just like during practices, that there are elements missing.".

Informant 5: "If an event would occur, it would most likely play out differently from what we have practiced. And that we just need to accept. But it is clear the more knowledge you have of the system and of the architecture and "what we have", it will be easier to manage (…).".

The experience and competence of personnel offshore were also brought up, as they through the extensive emergency preparedness training regime for regular safety events, are trained and prepared for making decisions outside procedures and under uncertainty.

Informant 8: "*The OIMs are well trained. They are often very experienced. They have the emergency preparedness management with them in such a decision (shutting down)"*.

Also, several informants brought up the importance of physical and "unhackable" barriers against cyberattacks, barriers that are not dependent on software or firmware.

Informant 4: *"You should make sure you have physical controls that rescues you in the last instance. If you have a boiler or something and it is a valve that does that if you reach a certain pressure it opens. It is unhackable. You can build physical things in the safety system that is not based on software. But is it software, it can be hacked, and is it firmware then vulnerabilities may be exploited. There is no way of protecting yourselves 100 % today."*.

Other examples given were shut down through electrical wiring or physical overflow protection of tanks in order to create robustness.

6. Discussion

The overall research question for this article was: **"How can different perspectives of becoming and remaining resilient contribute to closing the SAG related to cyber risks in the hyper-connected oil and gas industry?".** The research question was further divided into three sub-questions which each is discussed in separate subchapter below.

6.1. RQ1: Established foundations for cyber resilience in the oil and gas industry

In order to evaluate the first research question, what the foundations for cyber resilience in the oil and gas industry are, the empirical data has been interpreted with a basis in Theory A, B and C (Grøtan et al., 2022).

The empirical data indicates that the rudiments of resilience observed in cybersecurity work is primarily related to Theory A and B. We do, however, observe rudiments of Theory C, that potentially could be nurtured and strengthened. It should be noted that we do not advocate a position where Theory C is seen superior to Theory A and B, but rather seeks to investigate how the theories may be combined, and how a Theory C approach may build on Theory A and B, which is seen as essential to become resilient.

From a Theory A perspective on Resilience, resilience is integrated in the technical system, in the form of redundancy or fault tolerance. The informants largely based the type of technical controls that they implemented on existing standards, such as the DNVGL-RP-G108 (DNV GL, 2017) and the Norwegian oil and gas guideline 104 (Norwegian Oil and Gas Association, 2016). The maybe most clear version of Theory A resilience is found in what the informants referred to as un-hackable barriers, barriers that are physical, and independent of software of firmware. The empirical data also revealed that informants in some cases were reluctant to implement new technology, that potentially could improve the security of systems, because it also added complexity. Their worry was that the increased complexity would lead to transverse vulnerabilities, by connecting systems closer together, and that unknown vulnerabilities would be more difficult to understand and compensate for by operators in the system. Older technology, considered as proven, was therefore used, but compensated for by plans and procedures describing how to manage these known shortcomings or faults. In some cases, stricter enforcement of controls through technical and automatic processes that potentially could improve security was not implemented due to potentially unintended consequences for safety or availability, and rather enforced by manual processes. The empirical data indicates that the trust in the technical controls is too low to rely on them entirely, and that resilience cannot be based on Theory A alone.

A key assumption behind Theory B is that resilience can be achieved as a result of efficient risk assessment, emergency preparedness and business continuity processes, as a combination of technical, organizational and human controls. By mapping and understanding risks, the necessary controls may be implemented, in both preventive forms through controls that reduce the likelihood for attackers successfully obtaining the necessary access and control, and in corrective forms through controls reducing the consequence of breaches.

A prerequisite for this theory is that the system scope can be modelled and "linearized" in a realistic way, in order to implement the right controls. The empirical data illustrates that the participants experienced establishing a sound basis for the implementation of controls as difficult, as the risk understanding is distributed among the actors. Different actors hold different and more or less accurate understanding of consequences, threats and vulnerabilities which leads to different views of what controls to implement and how the controls should be implemented, both preventively and in situations with increased risk.

The data also indicate that the personnel involved, from a Theory B perspective, is seen as important barriers against cyberattacks. Remote access was also allowed by some informants, and the offshore crew had an important role in this process. All informants emphasized the importance of awareness among the personnel that in some form worked with computer systems and instructed them to be extra watchful if things seemed a bit outside normal. All informants had developed plans and procedures for cyberattack, including bridging documents with vendors and other contractors that will aid them during an incident.

The maybe most visible trace of resilience as Theory C was apparent through how the informants viewed the role of people in the system and their potential contribution. The informants seemed to agree that a potential event would most likely play out differently than planned for, and the way to compensate was the presence of wary and competent personnel that had good understanding of systems in scope, and a multidisciplinary incident management process. Who these people that contribute positively are varied from scenario to scenario, in some cases the IT personnel and in other parts of the offshore crew. For instance, in detecting attacks, sometimes monitoring systems does not alert, but personnel may sense that something as abnormal. But a key premise is that the right resources is available, both external expertise on control system and IT-system, but also an "inner organized core" that has good system understanding and understand what's important. The empirical data suggests that the informants based their ability to withstand, respond and recover on what Grøtan et al. (2022) denote as operational resilience, by modifying and bending rules and acting beyond rules in situations that demands it. The data can also be interpreted to that the informants designed their systems, both technical and procedural in order to cater for personnel's positive contribution through adaptive capacities, for instance through aiming to reduce complexity of systems in order to give humans in the systems a better chance to understand what's going on and through designing emergency procedures and plans without micromanagement of tasks, but rather focus on which roles that should be involved and what areas of responsibilities these have, and rather let the response emerge based on the situation and the competence of the resources in the team.

The empirical data however also suggest that building robustness through having an up-to-date asset inventory (i.e., "knowing what you have"), system understanding, having emergency preparedness

procedures in place, left the organization with a capacity for being flexible and adaptive based on what the situation required. This was particularly evident in the situations with increased risk, exemplified with the informants' experience from the management of log4j vulnerability and the increased threat situation during 2022. In other words, informants found having a sound Theory B basis, as a source of adaptive capacities, and thereby a source for resilience in the form of Theory C. This view corresponds to the C2M2 framework (U. S. Department of Energy, 2021) and Stavland and Bruvoll (2019) view, that the ability to adapt emerges from efficient risk management and emergency preparedness.

6.2. RQ2: Recognizing the Strategic Agility Gap

The second research question was to explore to what extent the industry does recognize *the need to narrow* the Strategic Agility Gap (SAG) (Woods & Alderson, 2021), which describes the gap between how fast an organization may adapt to change and the emergence of new unexpected challenges. In the article, the authors argue that the current strategy to maintain control of critical infrastructure by modeling and simulation, mapping vulnerabilities and consequences and implementing controls is insufficient due to the growth of complexity. To investigate whether the industry experienced a need to narrow the SAG, the empirical data was examined to see if the challenges described by Woods and Alderson (2021) could be observed in the empirical data.

There were several findings that give indications that the informants experience a strategic agility gap. Firstly, based on that the informants had experienced challenges in modelling systems and finding the correct measures to prioritize. The informants expressed difficulties in estimating risks, which again resulted in challenges to select and dimension security measures and controls, and informants generally expressed that it was difficult to evaluate when the level of protection was "good enough". Others also mentioned, upon the discovery of a critical vulnerability, that it takes time to understand if and how they are exposed, as both own and vendors' systems need to be mapped. As illustrated after the log4j vulnerability, where many spent a lot of time on mapping if they were exposed or not, indicating that it is difficult to maintain an updated overview ("knowing what you have"). As described, the log4j vulnerability, was a critical vulnerability in an open-source library which often is integrated in third party software, so mapping if the organization is exposed meant mapping own systems in use, but also vendors, and vendors' vendors to check if the library was in use, and how they responded to the situation. I.e., having a correct and up to date asset inventory is a complex task. In addition, for IT systems at least, the asset inventory is normally the outspring for the risk assessment which thereby will influence the controls implemented. Assuming that the asset inventory and risk assessment represent a "model of the reality", the challenges described by Woods and Alderson (2021) are observable in the data material. The data material also reveals that several informants expressed that controls might deteriorate over time, and that controls in reality were weaker than assumed, although the general perception was that the control was strong. Although informants believed that they had secured their systems in a good manner, and that they were able to prevent a lot, there seemed to be a consensus that they would struggle towards a disruptive and subversive attacker with sufficient resources, capabilities and persistence, who often is assumed to be one step ahead.

Acknowledging that the model is incomplete may be an important realization that could contribute to building adaptive capacities and compensate for the "robust yet fragile" effect where systems are robust with regards to events they are prepared to handle, but fragile towards unexpected events. The findings indicate that although establishing a model for the systems is seen as very important, but also challenging, the informants are aware that there are shortcomings that will require adaptations during actual incidents.

6.3. RQ3: Is there a potential in the industry for developing adaptive capacities based on existing foundations, for closing the SAG?

Here, we ask to which extent the empirical material reflects a potential in the industry to develop the observed foundations and rudiments into a more developed or full-fledged adaptive capacity, denoted Theory C in the theoretical framework.

This research question is also partly addressed in RQ1. Here, we found traces of Theory C through how the informants viewed the role of people in the system and their potential contribution, seemingly agreeing that a potential event would most likely play out differently than planned for, and that compensation depending on varied competence and good understanding of systems in multidisciplinary incident management processes. Moreover, they pointed out that in detecting attacks, sometimes sensors and detectors do not alert, but personnel may sense something as abnormal. But a key premise is that the right resources are available, through an "inner organized core". This enables modifying and bending rules and acting beyond rules in situations that demand it. There are signs that the informants designed their systems, both technically and procedurally, to cater for personnel's positive contribution through adaptive capacities.

One of the informants stated explicitly that "*training is to improve robustness, and on known events, and I believe I see tendencies of when you then bring out an anomaly, a crazy anomaly, to practice that, those who have practiced robustness the most and has it as a reflex immediately interprets the scenario into what they already known. They try to interpret it into an existing DSHA, and manage the event on autopilot*". In other words, the training is founded on Theory B, the informant sees the need to expose the trainees for surprises requiring a Theory C capability, but is disappointed to see that the trainees react by trying to cast the situation into Theory B. From this we can infer that at least one informant:

1) recognizes the need for Theory C capability do deal with inevitable surprises,
2) regards it as natural to impose the surprise from a Theory B training context,
3) anticipates a potential "robust yet fragile" effect when the trainees try to interpret the situation into an existing DSHA, and concludes that "*that's what we don't want them to do*".

Most importantly, the findings show that the informants do not envisage the closing of the SAG as a direct leap leaving the "old" behind, as but a gradual shift in which the "old" is the context of the new adaptive capacities. This corresponds with the theoretical presumption (Fig. 2) that Theory C capabilities should be gradually explored and developed from a Theory B context.

Seeing the empirical findings in retrospect, it is striking that it felt natural to organize them as a timeline, namely prepare/anticipate, absorb/withstand, and respond/recover. Does this counter our presumption that Theory A and B reflects a view of resilience-as-outcome as an epiphenomenon? Our position is that the sequential way of thinking about accidents and incidents manifests as "hegemonic" because it is a natural way of narrating and inquiring safety and security issues in the first place, and, not at least, so to say institutionalized by the risk management paradigm. Adaptive capacity is a much less prevalent way of thinking, but by using the Theory ABC framework, we have been able to identify connections between the informants' views and experiences, and adaptive capacity as a distinctive concept.

7. Conclusion

With the above discussion in mind, we can recall the overall research question: **How can different perspectives of becoming and remaining resilient contribute to closing the SAG related to cyber risks in the hyper-connected oil and gas industry?**

We have found signs of practices of diverse kinds, reflecting both

Theory A, Theory B and Theory C according to our analytical framework (Fig. 1). All practices seem to carry a development potential, but there is also a pronounced skepticism to rely too much on technological solutions (Theory A). Importantly, we find support for the theoretical position that adaptive capacity (Theory C) needs to be explored from a robustness (Theory B) position, while we also observe a crucial attention to the potential "robust yet fragile" effect.

Investigating the research question has facilitated new empirical and theoretical insights, ref. Fig. 4. With regards to empirical novelty, we have provided rich descriptions of cybersecurity practices in the oil and gas industry, as a "case of" a hyper-connected industry going through transformation to harvest from digital technologies, while at the same time being aware of increased threats. We additionally provide insight into that the oil and gas industry recognize that their models are incomplete and that adaptations are necessary to manage risks in line with Woods and Alderson (2021). With regard to theoretical contribution, our research contributes in three ways. Firstly, we have learned that the conceptualization of Theory A, B and C by Grøtan et al. (2022) is useful for investigating resilience as practice. Secondly, Theory ABC - show that the closing of the SAG is not a direct leap, but a necessary detour, facilitating a gradual shift in which the "old" is the (fading) context of the "new" adaptive capacities. I.e., the adaptive capacity must be built in the context of Theory A and B capabilities. And thirdly; the gradual shift towards more emphasis on adaptive capacity also requires a fundamental shift from seeing resilience-as-outcome as just an epiphenomenon of existing practice (resilience as characterized by Cooper (2022)), to seeing resilience-as-process as a unique phenomenon to address specifically, and on its own terms.

Further conclusions on the solidity of the theoretical understanding requires more extensive empirical data, preferably from real incidents, with more detail. This is not straightforward. One of the authors have experienced that a large industrial company, after being subject to a severe cyber-attack through which it positively displayed adaptive capacities according to Theory C, preferred to present their trajectory of actions through a robustness (Theory B) narrative. Presumably, the premise of being forced into boundary conditions, of being able to adapt *despite* rather than *because*, is not an uncontroversial narrative for a commercial company.

An alternative approach to gather specific data in the intersection between organizational (Theory B) and operational (Theory C) resilience may be to conduct realistic training arrangements in which diverse groups of personnel, across IT, OT, risk, and management professionals, are exposed to scenarios sufficiently beyond established preparedness, to trigger their rudimentary adaptive capacities, and to use the results for further analysis.

The current, increasingly aggressive threat landscape in the new hyper-connected geopolitical context offers a pipeline of challenges that can serve as raw material for this kind of training. For instance, the "Pipedream" toolbox for hackers (Dragos, 2022) implies a hitherto unmatched level of sophistication. However, we do not see the end of that pipeline, hence the cyber resilience discipline cannot allow itself to be complacent in the foreseeable future.

As a final remark on the needed transition to close the SAG through cyber resilience, we want to point out that this also will require managerial reorientation. In that respect, it is important to keep in mind that:

1) One of the major and most highlighted implications of putting the oil and gas industry under the Norwegian Security Act, is that industrial executives get access to classified information about threats (Hovland and Holmes, 2022). This might be necessary and useful to make a specific adaptation in a specific situation, but it is a long haul from being informed by classified information on threats, to create the conditions for sustained adaptive capacity.
2) Recognizing the need for managerial attention to enforce resilience, Rød (2020) and Stavland and Bruvoll (2019), advocates the view that risk management and resilience management should be framed similarly. To paraphrase Woods (2018), our comment is that such an approach could effectively be another way of "deflecting from the real issues".

Cyber resilience surely needs management attention, but it would be fatal if such attention is limited to casting resilience as a managerial epiphenomenon, rendering the SAG wide open.

CRediT authorship contribution statement

Solveig Pettersen: Writing – review & editing, Writing – original draft, Methodology, Formal analysis, Conceptualization. **Tor Olav Grøtan:** Conceptualization, Writing – Original draft, Writing – Review and editing, Visualization, Funding acquisition.

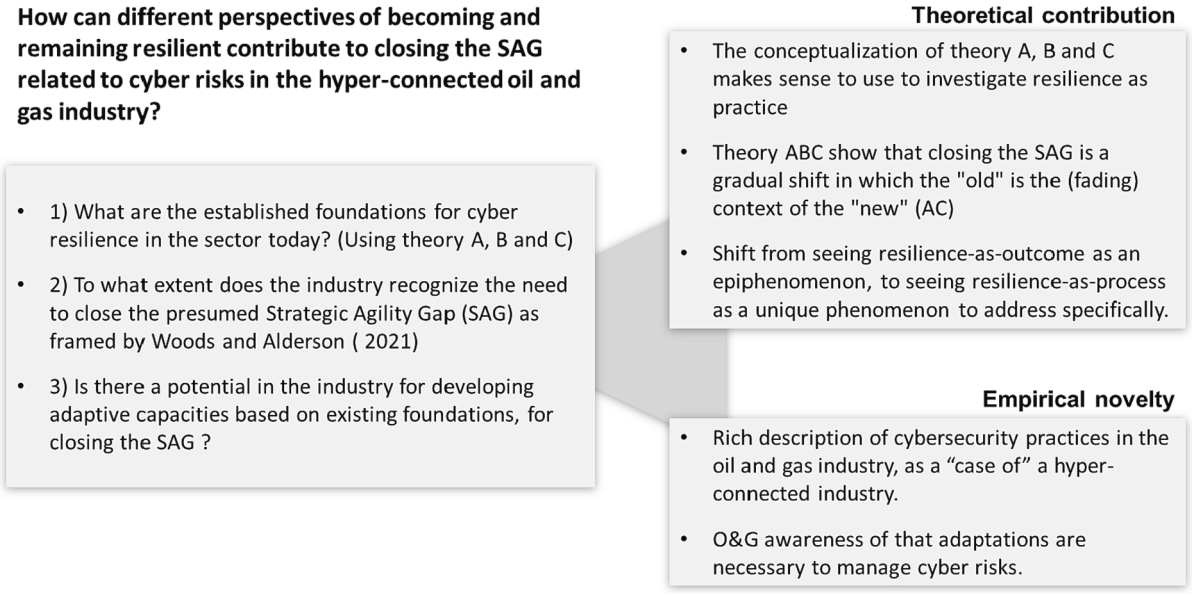

Fig. 4. Cohesion between RQ, theoretical contribution and empirical novelty.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The authors do not have permission to share data.

Acknowledgements

The paper is written by support from the Theoretical Advances of Cyber Resilience (TECNOCRACI) project, funded by the Norwegian Research Council, grant no 303489.

The authors want to thank Professor Trond Kongsvik at the Norwegian University for Science and Technology (NTNU) for valuable feedback.

References

Bochman, A., 2018. The end of cybersecurity. H. B. Review. https://store.hbr.org/product/the-end-of-cybersecurity/BG1803.

Charmaz, K., 2014. Constructing grounded theory (2nd ed. ed.). Sage.

Cooper, M.D., 2022. The Emperor has no clothes: A critique of Safety-II. Saf. Sci. 152, 105047 https://doi.org/10.1016/j.ssci.2020.105047.

Dekker, S. (2011). Drift into failure : from hunting broken components to understanding complex systems. Ashgate.

Dragos. (2022). CHERNOVITE's PIPEDREAM Malware Targeting Industrial Control Systems (ICS). https://www.dragos.com/blog/industry-news/chernovite-pipedream-malware-targeting-industrial-control-systems/.

du Plessis, E.M., Vandeskog, B., 2020. Other stories of resilient safety management in the Norwegian offshore sector: Resilience engineering, bullshit and the de-politicization of danger. Scand. J. Manag. 36 (1), 101096 https://doi.org/10.1016/j.scaman.2020.101096.

ENISA. (2023). *ENISA Foresight Cybersecurity Threats for 2030*.

Gioia, D.A., Corley, K.G., Hamilton, A.L., 2013. Seeking qualitative rigor in inductive research: notes on the Gioia methodology. Organ. Res. Methods 16 (1), 15–31. https://doi.org/10.1177/1094428112452151.

DNV GL. (2017). DNVGL-RP-G108 Cyber security in the oil and gas industry based on IEC 62443. In.

Gressgård, L.J., Melberg, K., Risdal, M., Selvik, J.T., Skotnes, R.Ø., 2018. Digitalisering i petrleumsnæringen. P. S. A. Norway. https://www.ptil.no/contentassets/50e7e658ebfa4bf2b52a8f94ef52a2ce/digitalisering-i-petroleumsnaringen.pdf.

Grøtan, T.O., 2014. Hunting high and low for resilience: Sensitization from the contextual shadows of compliance Safety, Reliability and Risk Analysis: Beyond the Horizon ESREL 2013.

Grøtan, T.O., Haavik, T.K., Antonsen, S., 2022. Cyber resilience: a preunderstanding for an abductive research agenda In F. Matos, P. M. Selig, & E. Henriqson (Eds.), Resilience in a Digital Age: Global Challenges in Organisations and Society. Springer International Publishing. 10.1007/978-3-030-85954-1.

Grøtan, T.O., 2020. Understanding HSE implications of remote work through a digital complexity perspective. The 30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference (ESREL2020 PSAM15.

Hanssen, G.K., Onshus, T., Jaatun, M.G., Myklebust, T., Ottermo, M., Lundteigen, M.A., 2021. Premisser for digitalisering og integrasjon IT-OT. https://www.ptil.no/globalassets/fagstoff/prosjektrapporter/ikt-sikkerhet/id6-premisser-for-digitalisering-og-integrasjon-it-ot_sintef-rapportnr-2021-00057-feb–signert.pdf.

Hollnagel, E., 2014. Safety-I and safety-II: The past and future of safety management. Ashgate.

Hollnagel, E., 2009. The Four Cornerstones of Resilience Engineering. In C. P. Nemeth, E. Hollnagel, & S. Dekker (Eds.), Resilience Engineering Perspectives, Preperation and Restoration (pp. 117-133). CRC Press. 10.1201/9781315244389.

Hollnagel, E., 2011. Prologue: The scope of resilience engineering. In (pp. xxix-xxxix).

Hovland, K.M., Holmes, M., 2022. Equinor og Gassco lagt under sikkerhetsloven: – Naturlig at vi skjerper beredskapen. E24. https://e24.no/energi-og-klima/i/xg8Awn/equinor-og-gassco-lagt-under-sikkerhetsloven-naturlig-at-vi-skjerper-beredskapen.

ISO/IEC (2013). ISO27001:2013, Information technology, Security techniques, Information security management systems Requirements. In. Switzerland.

Jaatun, M.G., Wille, E., Bernsmed, K., Kilskar, S.S., 2021. Grunnprinsipper for IKT sikkerhet i industrielle IKT systemer. https://www.ptil.no/globalassets/fagstoff/prosjektrapporter/ikt-sikkerhet/id4-grunnprinsipper-for-ikt-sikkerhet_sintef-rapportnr-2021-00055-feb—signert.pdf.

Kilskar, S.S., Branlat, M., Grøtan, T.O., Fiskvik, J., 2020. Making sense of the many understandings of cyber resilience. TIEMS Annual Conference, Paris, France.

Lacy, S., Scott, A., 2021. Implications of Log4j Vulnerability for Operational Technology (OT) Networks. https://www.dragos.com/blog/industry-news/implications-of-log4j-vulnerability-for-ot-networks/.

Lee, R.M., 2017. TRISIS: Analyzing Safety System Targeting Malware. https://www.dragos.com/resource/trisis-analyzing-safety-system-targeting-malware/.

Leveson, N., 2020. Safety III: A Systems Approach to Safety and Resilience.

Linkov, I., Bridges, T., Creutzig, F., Decker, J., Fox-Lent, C., Kröger, W., Lambert, J.H., Levermann, A., Montreuil, B., Nathwani, J., Nyer, R., Renn, O., Scharte, B., Scheffler, A., Schreurs, M., Thiel-Clemen, T., 2014. Changing the resilience paradigm. Nat. Clim. Chang. 4 (6), 407–409. https://doi.org/10.1038/nclimate2227.

Linkov, I., Trump, B., Trump, J., Pescaroli, G., Mavrodieva, A., Panda, A., 2022. Stress-test the resilience of critical infrastructure. Nature, 603(7902), 578-578. 10.1038/d41586-022-00784-2.

NIST. (2022). NIST Special Publication - NIST SP 800-160v1r1 - Engineering Trustworthy Secure Systems. In: NIST.

Norway Petroleum Safety Authority, 2017. Sikkerhet og Ansvar.

Norwegian National Security Authority, 2020. Grunnprinsipper for IKT-sikkerhet 2.0. Retrieved from https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/introduksjon-1/.

Norwegian National Security Authority, N., 2022. Varsel om russiske trusler mot kritisk infrastruktur https://nsm.no/aktuelt/varsel-om-russiske-trusler-mot-kritisk-infrastruktur.

Norwegian National Security Authority, 2023. Oversikt over innmeldte grunnleggende nasjonale funksjoner. Retrieved 10.10.2023 from https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnleggende-nasjonale-funksjoner-gnf/grunnleggende-nasjonale-funksjoner/oversikt-over-innmeldte-grunnleggende-nasjonale-funksjoner/.

Norwegian National Security Authority, 2021. Oppdatering: Kritisk sårbarhet i Apache Log4j. https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/varsler-fra-ncsc/oppdatering-kritisk-sarbarhet-i-apache-log4j.

Øien, K., Bodsberg, L., & Jovanović, A., 2018. Resilience assessment of smart critical infrastructures based on indicators. In (1 ed., pp. 1269-1277): CRC Press.

Petroleum Safety Authority Norway, 2017. Safety, status and signals 2016-2017: Reversing the trend.

Petroleum Safety Authority Norway, P. (2022). *Krigen i Ukraina* https://www.ptil.no/fagstoff/utforsk-fagstoff/fagartikler/2022/ukraina/.

Pettersen, S., Grøtan, T.O., 2021. Framing Cyber Resilience for Critical Infrastructure in the Context of Resilience Engineering – A Literature Study The 31st European Safety and Reliability Conference, Angers, France. https://www.rpsonline.com.sg/proceedings/9789811820168/html/363.xml.

Rød, B., 2020. Operationalising Critical Infrastructure Resilience. From Assessment to Management UiT The Arctic University of Norway].

Stavland, B., Bruvoll, J.A., 2019. Resliens - hva er det og hvordan kan det integreres i sikkerhetsstyring. https://www.ffi.no/publikasjoner/arkiv/resiliens-hva-er-det-og-hvordan-kan-det-integreres-i-risikostyring.

The Ministry of Justice and Public Defence. (2020). Meld. St. 5 (2020-2021) Samfunnssikkerhet i en usikker verden. https://www.regjeringen.no/no/dokumenter/meld.-st.-5-20202021/id2770928/.

U. S. Department of Energy (2021). *Cybersecurity Capability Maturity Model (C2M2)*.

Weick, K.E., Sutcliffe, K.M., 2001. Managing the unexpected: assuring high performance in an age of complexity. Jossey-Bass.

Wildavsky, A., Bowling Green State University Social, P., & Policy, C. (1988). Searching for safety (Vol. 10). Transaction Books.

Norwegian Oil and Gas Association, 2016. INTEGRERTE OPERASJONER 104 Anbefalte retningslinjer krav til informasjonssikkerhetsnivå i IKT-baserte prosesskontroll-, sikkerhets- og støttesysteme. In.

Woods, D.D., 2015. Four concepts for resilience and the implications for the future of resilience engineering. Reliab. Eng. Syst. Saf. 141, 5–9. https://doi.org/10.1016/j.ress.2015.03.018.

Woods, D.D., 2018. The theory of graceful extensibility: basic rules that govern adaptive systems. Environ. Syst. Decis. 38 (4), 433–457. https://doi.org/10.1007/s10669-018-9708-3.

Woods, D.D., Alderson, D.L., 2021. Progress toward resilient infrastructures: are we falling behind the pace of events and changing threats? J. Crit. Infrastruct. Pol. 2 (2), 5–18. https://doi.org/10.18278/jcip.2.2.2.

Woods, D.D., Hollnagel, E., 2006. Resilience Engineering Concepts. In E. Hollnagel, D. D. Woods, & N. Leveson (Eds.), Resilience engineering : concepts and precepts (pp. 1-6). Ashgate.

Woods, D.D. (2019). Chapter 4: Essentials of resilience, revisited. In M. Ruth & S. Goessling-Reisemann (Eds.), Handbook on Resilience of Socio-Technical Systems (pp. 52–65). 10.4337/9781786439376.00009.