SecureSafety; state-of-the-art and remaining challenges

T.O. Grøtan
SINTEF Digital, Trondheim, Norway. E-mail: Tor.O.Grotan@sintef.no

S. Petersen
SINTEF Digital, Trondheim, Norway. E-mail: stig.petersen@sintef.no

T. Myklebust
SINTEF Digital, Trondheim, Norway. E-mail: thor.myklebust@sintef.no

G.K. Hanssen
SINTEF Digital, Trondheim, Norway. E-mail: Geir.K.Hanssen@sintef.no

The term SecureSafety (SeSa) was launched in a project that was completed in 2006, which left behind a (at the time) new method for securing Safety Instrumented Systems (SIS), which pioneered modern approaches to industrial control and automation systems (ICAS) security in the oil and gas industry. The basic conceptual advance of the SeSa approach, combining security and safety in the manufacturing of ICAS systems, is today prolonged by an ongoing attempt to integrate functional safety standards with emerging security standards aimed at ICAS and SIS, founded on advancing the barrier model that originates from the safety domain. However, arguing that there is a need for additional measures for countering unexpected and surprising events from the complex security threat landscapes, this paper explores how the increasingly popular resilience concept can be the foundation for additional SeSa approaches and measures. The exploration takes into consideration some recent critique towards the resilience concept as it is applied in the discourse on safety management in the Norwegian oil and gas sector, the difficulty of adopting key premises aspects of resilience to an increasingly software-intensive SIS domain, and the potential disruptive impact of new technologies such as 5G, with a sensitivity to technocultural aspects. Arguing that the adaptation of the resilience concept into the SeSa domain should be based on a pronounced sociotechnical perspective and a deliberate contextualization of resilience into a procedural, compliance-oriented scheme that facilitates managerial accountability also when attempts of resilient performance fails, the paper concludes by sketching out a road map for further work on SecureSafety.
.

Keywords: Industrial ICT, operational technology, safety, security, cyber resilience, technoculture, sociotechnical

1. Introduction

Digitalization and SecureSafety (SeSa)

Digitalization of offshore oil and gas industrial processes is an ongoing transformation process driven by introduction of new technologies, a persistent mix of old and new technologies and practices, and not at least an increased dependency of software, and by implication, reliance on frequent software updates. The functional integrity of Safety Instrumented Systems (SIS) remains a highly critical baseline for any step of this transformation process.

Scurity aspects of remote access to SIS entities was the key issue of the SecureSafety (SeSa) project (Grøtan et al. 2007, Jaatun et al., 2009). SeSa left behind a method founded on a zone and barrier approach that is commonplace today, but it also represented a step forward of conceptual thinking pioneering a combined safety and a security perspective in the Norwegian offshore oil and gas industry. Such a combined perspective transcends the mere methodological aspects that were relevant at the time, as we now need new SeSa methods to keep up with the emerging threat and vulnerability landscape. In short, the zone and barrier approaches are necessary, but insufficient.

The number of cyber-attacks and incidents towards industrial installations continue to grow, and recently even SIS is reportedly targeted specifically and deliberately (Dragos, 2017) with the presumed intention of enforcing physical danger. Further down the road, we must expect to be repeatedly surprised in ways that are practically impossible to foresee. The protectors should use their imagination methodologically to reduce the level of surprise and increase their responsiveness (Grøtan and Antonsen 2016).

Scope of SeSa development

The joint safety and security perspective is hardly as pioneering today as it was 2006, but the "SeSa"

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

label is still meaningful for pointing forward to contemporary and future challenges of SIS. E.g., the challenging integration and fusion of generic information technology (IT), and operational IT (OT). As the scope of digitalization and software dependency also in industrial applications grow, new technologies (e.g., Industrial Internet of Things (IIoT), 5G and DevOps) enter the scene, and must be integrated in the overall sociotechnical approach to daily work. DevOps is not a technology but a set of practices that combines software development (Dev) and information-technology operations (Ops) (Debois 2011, Laukkarinen 2018). A prospect arise: can DevOps accommodate key SeSa aspects, helping to manage vulnerabilities caused by increased reliance on frequent software updates?

The original SeSa conceptual challenge anno 2007/2009 is thus today not only accentuated, but also maintains its relevance in a more complex organizational and sociotechnical landscape. Furthering this demands theoretical insight as well as practicable solutions.

The SeSa concept will still rest on some persistently fundamental cornerstones. Functional Safety standardization for SIS is based on the IEC 61508/61511 standards, which are well grounded in practice over many years in the industry. The upcoming IEC 62443 standard is now gaining influence and extends the functional safety approaches with a cyber security perspective. The two standards share much common ground, and thus invites coordinated implementation. This is rational from an industrial and organizational perspective, reusing organizational structures, or sharing or complementing objectives as well as procedures and performance standards. However, there is a persistent fundamental difference between the safety and security challenges, and there are residual contemporary, as well as emerging challenges that needs to be addressed.

This paper discusses these remaining challenges from a mainly theoretical perspective, encompassing cultural, organizational, sociotechnical as well as technical aspects.

The resilience leap

A key prospect for potential advances is to actively adopt new concepts and approaches from the resilience domain, e.g. from resilience engineering. Resilience engineering is "*a paradigm for safety management that focuses on how to help people cope with complexity under pressure to achieve success*" (Hollnagel et al., 2007:6). Among the hallmarks of this approach is the emphasis on complexity as a source of small and large surprises, and the corresponding capabilities to make situational adaptations as a response to these surprises.

Broadly speaking, the resilience approach searches for new answers by asking "why does it work" rather than "why does it fail", the latter representing more traditional safety approaches. The distinction between Safety-I and Safety-II (Hollnagel 2014) in many ways epitomizes this leap from the "old" way to the new way. Another way is to describe this as a leap from the more widely used concept of robustness, to the resilience concept. While both concepts share the objective of resisting stress, shock, disturbance or disruption, the resilience concept is more dedicated to doing this in a manner of being "prepared to be surprised" rather than "preparing for not becoming surprised".

Resilience is thus about resisting, enduring, absorbing and withstanding surprise in a manner that include the capacity to bounce back, bounce forward, of recovery and restoration of a system, while learning from the experience. Hence, resilience is ultimately a matter of being active rather than passive, processual rather than structural, dynamic rather than static, creative rather than predisposed, situated rather than generic, and idiosyncratic rather than replicable and repetitive. All of which should be framed by a sociotechnical, interactive perspective.

Regardless of how we describe the leap from traditional safety thinking into resilience thinking, none of the key differences appears to be reflected in the forthcoming IEC 62443 which addresses the security of functional safety, within the scope of Safety-I. Hence, grasping the implications of this leap remains a key issue for SeSa to explore beyond the scope of standardization.

Emerging technologies like IoT, 5G and DevOps radically influence the way future SIS will be designed, developed and operated, and will carry new vulnerabilities that challenge existing design principles. This includes, not at least, changes in sociotechnical practices to maintain the operational integrity of old and new technologies in combination and mastering the accommodation of the limitations and demands inscribed in the new technologies from the outset.

Aim of this paper

The paper summarizes the state-of-the-art of SeSa as well as remaining and emerging challenges in terms of organizational accommodation of the resilience (Safety-II) component, technocultural challenges related to the IT/OT fusion, and the potential influence of a "telecom culture" (of 5G) that is expectedly rather insensitive to the oil and gas industrial context. IIoT and 5G issues also amplifies the software dimension of the overall challenge, thus the application and feasibility of DevOps is included in the discussion.

The broad notion of technoculture is borrowed from Penley and Ross (1991) and is here used to

refer to a set of technologies with a corresponding group of professionals with their language and practices involved in developing and maintaining the integrity of technologies. The integration of IT, OT as well as "telecom" (5G) thus also involves the meeting between professional communities, with different methods, background, professional jargon, and with different knowledge of the operational domain where IT/OT solutions are being implemented and deployed. Ultimately, it is also relevant to be aware of the distinctiveness of a "software culture" where *development* to a much larger extent is seen as a continuous process as compared to a "hardware culture". Software displays different properties than hardware (such as electronical components) as it relatively easy can be changed and (re)deployed.

Finally, a roadmap for advancing the field of SecureSafety is sketched out.

2. The power of barriers – and the remaining problem

The starting point for our analysis is the general need to secure systems providing functional safety in the context of Industrial Control and Automation Systems (ICAS). Hence, the problem addressed may affect systems labelled as SAS (Safety and Automation), SCADA (Supervisory Control and Data Acquisition, SIS (Safety Instrumented Systems), etc.

For short, and for emphasising the proximity to, as well as the criticality of, ICAS for operation and control of physical industrial process, we will also use the term Operational Technology (OT) as a synonym for systems affected by the SeSa challenge. OT systems are cyber-physical by nature, as they often contribute to the operational control of physical processes, and their specific contribution is often of a safety-critical nature.

A lack of security in ICAS/OT, and specifically in SIS, may therefore affect or jeopardize the integrity of the assumed protection from a safety function, with possible (safety) implications in the physical world. From a narrower safety perspective, there exist approaches that formalize those aspects through "SIL" (Safety Integrity Level) concepts of IEC 61508. A "SIL" approach is conceivable for security properties, but will not be pursued here.

Generic Information Technology (IT) and OT share many technological parts and components, but their ways of being designed, described, assembled and built into operational systems, operated and maintained, and, not at least their link to the physical world, is a major difference with significant implications.

However, generic IT systems are often surrounding the OT systems in an intendedly "read-only" manner, but the solutions for ensuring such constraints are often vulnerable and sometimes even fragile. Hence, compromised surrounding IT systems are often a key part of the attack vector towards OT systems, and such attacks will exploit the vulnerability of OT systems that expose too much trust in their surrounding IT environment. Hence, the very aspect of integrating IT and OT not only as technologies, but also as sociotechnical practices with cultural underpinnings, represents an opaquer, but persistent challenge with no easy solution in sight.

The functional safety issue of industrial control systems (OT) per se is predominantly framed by the IEC 61508/61511 standards. Recently, the IEC 62443 standard has been offered to address the security issues of such functional safety implementations.

In addition, the IEC TR 63069 is aimed at guiding the application of IEC 61508 and IEC 62443 holistically at the same time to a manufacturing system. The overall aim is to maintain the technical integrity of such a system. Hence a technical bias remains with respect to scope and objective, while the sensitivity to the sociotechnical fit between technical integrity as a goal, and the social practice of ensuring this, is less emphasized. The nature of standardization is to seek the least common denominator and leave the rest for local adaptation. Hence, we do not claim that these standards deliberately turn a blind eye to human factors, but by implication, they do not employ a pronounced sociotechnical, situated interactive perspective on human practice related to their implementation. It must however be kept in mind that the aim of standardization is not to falsify Shorrock's (2017) claim on behalf of the sociotechnical perspective that "*this kind of human factors .... tends to be neglected in favour of simplistic approaches to 'human factors'*".

From an ICAS/OT, SeSa management point of view, it is expectedly regarded as beneficial that the implementation of IEC 61508/61511 and IEC 62443 standards can be addressed jointly, through the very same organizational resources and governance constructs. Having used a lot of resources and organizational energy to deal with the IEC 61508 requirements and issues in a consolidated manner over many years, it is very understandable that the appetite for setting up a "parallel track" for dealing with IEC 62443 issues for the very same (ICAS) systems, is rather low. Integration is however not straightforward (Skoglund, Warg and Sangchoolie, 2018).

These practical considerations and limitations embedded in the standardization process invites a continued attention to and reliance on the renowned (safety) barrier model (e.g., PSA 2017, Hauge and Øien 2016) also for security. However,

despite that such a barrier orientation doubtlessly will spark significant achievements, there are inherent shortcomings left behind that calls for another strategy as well.

The most striking shortcoming is the ability to effectively deal with hidden, dynamic and emergent threats and vulnerabilities that fall outside expectations behind established preparedness, e.g. when surplus operational data creates a vulnerability (Grøtan, 2018). Andy Bochman (2018) of Idaho National Labs (INL) in the US points out the extreme end of this for energy systems, by claiming that the brutal truth is that "*it doesn't matter how much your organization spends on the latest cybersecurity hardware, software, training, and staff or whether it has segregated its most essential systems from the rest. If your mission-critical systems are digital and connected in some form or fashion to the Internet, they can never be fully safe. Period*." In other words, even the perfect implementation of recognized "cyber hygiene" practices cannot stop the dedicated hacker.

Interestingly, Bochman (2018) argues that "*disconnecting as much as possible, installing old-fashioned mechanical devices, inserting humans in automated functions might sound like a regressive business function…..but should be reframed as a proactive risk-management decision*". Although we do not necessarily address worst-case scenarios of, e.g., state-sponsored hybrid warfare attacks in this paper, we share the view of Bochman (2018) on the importance of keeping the human-in-the-loop. Our interest will however be directed towards how the human-in-the-loop, embedded in sociotechnical interaction, can make a significant difference.

Adding to Bochman's (2018) argument, we also argue that the vulnerability of the OT targets per se, partly stems from an underappreciation of the importance of sociotechnical practice as a resource for adaptive performance of the system as a whole. Moreover, there is also a possible failure lurking in terms of not recognizing the technocultural impact when the already demanding IT/OT integration is "disrupted" by the entry of the telecom technoculture through the arrival of 5G/IIoT, and the unique horizon of software development technologies. The sociotechnical fit must always be renewed and cautiously maintained, but in this new situation it may have to be reconstructed, on new and potentially strange grounds.

The point of departure for the further discussion in this paper will hence be that the consolidated effort of combining IEC 61508 and IEC 62443, guided through IEC TR 63069 or otherwise, may be insufficient to keep up with the full spectrum of the security challenge. The main reason for this is that the security threat landscape evolves and continuously presents surprising events and combinations embedding hostile motivations for utilizing existing and new attack vectors and exploiting IT/OT vulnerabilities.

3. Is "resilience" the answer?

The resilience concept has gained immense attraction and prominence at many arenas over the last decade. It is therefore reasonable to consider the resilience concept, or "Safety-II" (Hollnagel 2014) as a platform for building a response capability to the residual risk rendered by the combined application of IEC 61508 and 62443, not exclusively for, but also for the SeSa target.

In employing the resilience concept, we do not here restrict ourselves to the post-event recovery performance, but also pay attention to the potential value of anticipating, discovering, addressing and compensating disturbances before they develop into an event or incident.

3.1 A critique of resilience as a "hegemonic" theory in safety management

Somewhat surprising from the SeSa perspective, Du Plessis and Vandeskog (2020) finds that the resilience engineering concept has gained prominence with respect to safety management in the Norwegian oil and gas sector, to the extent that they portray it as a "hegemonic" theory. From that position, they scrutinize the resilience approach from the perspective of Critical Management Studies (CMS). We cannot address the whole critique formed by applying three theoretical perspectives, and creating three different stories from combining them. We restrict ourselves to addressing six claims drawn from Du Plessis and Vandeskog (2020):

1. The concept of resilience is significantly more ambiguous than what it is made out to be.
2. The dominant conception of resilience is functionalist and prescriptive and chiefly derived from a single scientific position, namely resilience engineering.
3. It is a "catch-all" concept, while it is hard to pin down its exact meaning
4. Resilience can however also be seen as a vacuous, albeit fashionable, "bullshit"-term, a notion that stems from Frankfurt (1973/2005). As such a term, resilience is utilized, e.g. by safety managers to gain legitimacy. It can also be linked to the kind of "strategic ambiguity" that is associated with tools for achieving visionary strategies that "hinges on the ability of managers to instill confidence".

5. Resilience can also be related to the rise of neoliberalism and the depoliticizing of danger for off-shore workers, also forwarding, under the ubiquitous presumption of unmanagable complexity, the (dangerous/questionable) assumption that they - as resilient subjects – will thrive from exposure to danger.
6. In effect, resilience "might have become a popular principle because it potentially allows for more risk-taking, while still retaining some general or abstract degree of safety".

Du Plessis and Vandeskog (2020) claim that their juxtaposed "stories" offers a more nuanced understanding of what is actually implied by resilience. Here, we will briefly explore to which extent the three stories shed light on the introduction of resilience in the SeSa context.

23.2 Stories of Resilience in the SeSa context

Even while there is a huge difference in scientific approach between the CMS approach that Du Plessis and Vandeskog (2020) apply in their paper, and the more practical research related to implementation of safety and security standards, their critique may be accounted for in our attempt of devising a path of SeSa development that incorporates "resilience" as a main inspiration.

Plessis and Vandeskog (2020) however also argue that "*research on resilience may have performative effects on its object that is quite different from those intended*". Combined with their claim that resilience engineering enjoys a "hegemonic" position in the Norwegian oil and gas safety management community, there is also the possibility that this "hegemony" would reach the SeSa discourse, and create a prerogative for resilience that could divert our attention from the traditional key issues of SeSa. We have no empirical data systemized in a manner comparable with Du Plessis and Vandeskog (2020). However, our assessment based on enduring observation and participation is that the standardization and development processes are not visibly influenced by the resilience perspective. Quite the contrary, the main focus seems to be on a "Safety-I" perspective that is sought transferred to the security domain without much problematization on its validity. However, the DevOps perspective accommodates perspectives that resembles resilience principles in terms of flexibility, "lean", "agile" and so on, and particularly embedded in the SCRUM approach (Hanssen et al. 2018, Myklebust et al. 2019). However, these preferences have only indirect influences on the SeSa main line of thinking, mainly as a consequence of the growing acknowledgement of software reliance.

Regarding the critique of Du Plessis and Vandeskog (2020) on the ambiguity of the resilience concept, its functionalist and prescriptive nature, as well as its "catch-all" appearance, we argue that the key cure against these is to define a proper context that defines the purpose – "resilient to what" – and the presumed operational conditions for resilient performance.

A key part of this is that resilience requires a sociotechnical balance that ensures association and correspondence with real/actual practice at some level. According to this premise, resilience is never purely technical, there must be a human activity involved that can generate novelty.

Another key part is that resilience should never be considered as the only working principle for achieving safety or security, it should always be contextualized into another principle or frame that can contain or confine the possible shortcomings of resilience. Here, it is possible to draw on the Training for Operational Resilience Capabilities (TORC) approach (Grøtan 2017) which is founded on the principle that the resilience logic should be framed by its' sheer opposite, namely the principle of compliance. Broadly speaking, this corresponds to the mixed presence of both Safety-I and Safety-II principles in Hollnagel's (2014) terms, constituting a *complementary*, *dialectical* as well as a (mutually) *shaping* relation between the two principles (Grøtan, 2015). An important aspect of the complementary relation is that "compliance" (Safety-I) by default dominates "resilience" (Safety-II).

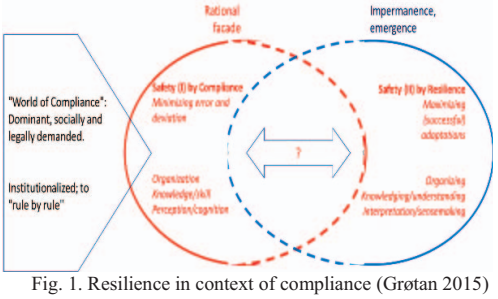

Fig. 1. Resilience in context of compliance (Grøtan 2015)

For SeSa, the TORC scheme of Fig.1 could be paraphrased as resilience operating in the context of the barrier approach epitomized through IEC 61508/61511, IEC 62443 and the IEC TR 63069.

Regarding the claim that resilience *might* serve as a "bullshitting" instrument for management to obscure or obfuscate the very purpose of SIS or other safety functionality, our experience does not indicate any of the kind. Quite the contrary, the managerial support for integrity of safety functions sustains. It cannot be precluded that the

efforts of (us as) researchers and others to extend the SeSa concept based on inspiration from resilience is received by practitioners as "bull*", but that is a story of another kind.

Regarding the claim that resilience may be used to depoliticize danger, fool workers to believe that they will thrive from danger and trick them into more risk taking under the disguise of some general or abstract degree of safety, it must be acknowledged that this actually may happen. Not just under the auspices of resilience as a vague or general concept, but also as a possible consequence of an underappreciation of the differences between the overall safety and (cyber) security challenge, as epitomized by SeSa. The SeSa "resilience story" is as follows:

1. The sociotechnical imperative ensures that the principles of resilience are contextualized into a more common frame (procedures) whenever possible, and may be linked to actual practice "somewhere" in the organization
2. The characterization of "resilience" in contrast to "compliance" prevents a mere relabelling of existing practices that are actually void of resilient properties.
3. Standards, e.g. IEC 61508, 61511, or 64223 can be clearly positioned as "templates" for procedural action ("Security-I"), and thus be supplemented by other actions, possibly of a more resilient nature, with a purpose of practical implementation.
4. Future attempts of "bullshitting" by means of resilience will effectively be prohibited from the SeSa discourse due to the above principles
5. Using the TORC approach (Grøtan 2015, 2017) as a prototype or template, it will in principle be possible for management to develop a mandate for resilient behaviour ("Security-II") at the operational (but managed) level.
6. Through such a mandate, management also assumes and absorbs *accountability for the potential failure* of *attempted* resilient action within the given mandate. This enables an open dialogue on the actual content of the mandate, rooted in actual practice and experience rather than some general or abstract degree of safety.
7. This way, depoliticizing of danger may be actively counteracted, employees will not have to assume that they should be obliged to more "risk-tasking" to satisfy a tacit expectation of being a "resilient subject".

It is important to note that this arrangement provides an *opportunity*, but not a guarantee for countering the shortcomings pointed out by Du Plessis and Vandeskog (2020). An actual implementation will never be straightforward.

These new ways of addressing and drawing insight and value from "normal" and successful operation by asking "why does it work" rather than "why does it fail?" however requires a sustained attention to sociotechnical practice, and not at least a sustained willingness to investigate the gap between "work as imagined" and ""work as done" with open minds (Shorrock , 2016).

2.3. Transparency as a scarcity

Returning to the combined safety and security agenda of SeSa, the "resilience story" depicted above however turns a bit more challenging. This because the whole concept of "Safety-II" rests on the assumption of transparency, proximity and skilled knowledgeable participants. The resilient subjects are presumably informed about what is going on, they are close to the dangers, they can influence the key mechanisms, their sociotechnical interaction is rooted in experience, skills, knowledge and competence, and the organizational context allows and supports this to unfold. Without this in place, "Safety-II" is just thin theoretical air.

Will it actually be possible to conceive a "Security-II", founded on similar premises to deal with cyber security issues and challenges? A number of factors points in the wrong direction; First, while the cyber-physical implications may be tangible and conceivable for a "reliability professional" (Roe and Sculmann, 2008), the internal constructs of the vulnerable IT/OT system, especially concerning the software part, may not. The IT and OT specialists may not communicate well, especially in stressing situations. When a problem occurs in a system with, e.g., a lot of legacies and/or lack of updated documentation, any reluctance to probe "innovative" solutions or practices will be highly understandable. This can be put even stronger: it may be more likely that operators prefer to stick to predefined procedures, defined by other (accountable) actors, in situations that actually call for resilient performance.

2.4 DevOps as a facilitator for transparency

Especially for the software-intensive parts of a SeSa system, the DevOps concept represents maybe the best opportunity to facilitate increased

transparency and updated information as an enabler of resilient performance.

DevOps is a set of practices that combines software development (Dev) and information-technology operations (Ops) (Debois 2011, Laukkarinen 2018), and its main features are depicted in Fig 2 which indicates development activities (aligned with the SCRUM process), and operational activities. Regarding safety, the figure indicates that development activities provide proof-of-compliance with safety (and security) standards by updating a *safety case*. Regarding the operations-part, the figure indicates that operation has to be supported by monitoring as a key input to the development process – this includes both monitoring of the system as is, as well as dedicated information security (attacks or threats) monitoring.

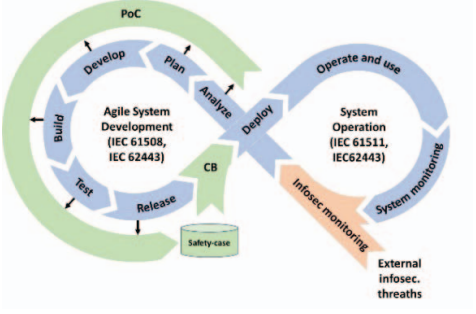

Fig. 2. DevOps principles

DevOps is basically nothing more than a framework for merging development and use/operation of a system. The rationale of the idea is that a system, especially a software-intensive system, is never done – it is under constant development. However, to encompass resilience such a framework also needs to be extended in such a way that the continuous development (or refinement) of a system also includes development and improvement of guidelines for the organization that uses the system. This may be guidelines (cultural, organizational or procedural) that inform people on how to e.g. countermeasure failures or incidents, on how to keep an eye on potential threats to information security, and how to feedback requirements or needs to development.

2.5 Disruptive technocultures

We have already indicated that the IT/OT technocultural integration is a persistent challenge that manifest at the level of sociotechnical practice, e.g., when it is perfectly rational from an IT point view to install an update to fix an imminent security threat, while the OT counterpart hesitates due to the lack of proof that the update will not influence the safety function.

With the arrival of 5G and Industrial IoT, the challenge amplifies. Opportunities arise for the factories, plant owners or automation companies to be a 5G operator, but also for telecom operators to be providers of industrial 5G. Which scenarios will prevail is impossible to know, but a lot of technocultural adaptations and disruptions will presumably take place.

But we may already conclude that the entry of the 5G and IIoT technologies, together with the already existing imperative of DevOps, will demand a major shift for the ISAC/OT vendors, and their users, that seems to be well rooted in the traditional, more linear "waterfall model" of software development.

The overall picture will be that the rules of the sociotechnical interactions change, new players enter the scene, and the overall "fit" has to be renegotiated, probed and experimented.

3. A draft Roadmap for SeSa

No attempt of supplementing the "security barrier" approach with a resilience approach will be straightforward. Our best advice at the moment is that the industry moves along a "roadmap" for safe and secure digitalization. In short, the roadmap contains the following directions:

Hardware/firmware vulnerability is an underattended area. With more off-the-shelf equipment related to e.g. 5G and IIoT, the security supply chain and the potential vulnerabilities must receive more attention. Too many components may be too easily reverse engineered, and rendered open for attack

Hyper connectivity. With 5G, IIoT, the attack surface will increase dramatically, while the appetite for increased scope of control expectedly will rise. SeSa stakeholders must develop a trade-off on this.

Agile SW Engineering. The potential for employing DevOps in a balanced way must be further explored. Two pitfalls may be conceived: 1) the possibility to end up as "update junkies" that uncritically relies on other people's judgements, 2) rejecting opportunities based on biased interest in "own" areas only. Both violate the sociotechnical ideal raised in this paper.

The **DevOps** approach must be elaborated with increased transparency as a goal in order to support "Security-II"

The **SeSa resilience story** must be anchored among all stakeholders and all along a conceived "resilience value chain".

Based on the SeSa resilience story, each organization must develop a notion of their **limits of achievable resilience,** in order to avoid overconfidence and thus, increased risk.

Technocultures. The differences and similarities between IT, OT, and telecom cultures must be more thoroughly addressed, the disruptive

potential of 5G must be better understood, and the influence of the "software culture" investigated.

Conclusion

We have described the SeSa challenge, the prospect of using the resilience concept as a reinforcement to deal also with the security challenge, and sketched out a scientific roadmap to advance on a path that in the end could reinforce the SeSa concept with a trustworthy *cyber resilience* component.

The real decision is however up to the OT owners and stakeholders. If they do not want to end up in the same position as in the more generic IT case, that is, more or less surrendering to a reactive incident management strategy because the appetite for new technology is larger than the risk aversion towards the unknown dangers, OT owners need to apply a more proactive stance towards the emerging threats and vulnerabilities. The alternative would be to prepare to encounter Bochman's (2018) prediction in its full might.

Acknowledgement

The paper is financed by SINTEF Digital through the SeSa project, and adapted to a broader project of theoretical advances on cyber resilience (TECNOCRACI), funded by the Norwegian Research Council, under contract no 303489.

References

Bochman, A. 2018. The End of Cybersecurity. Harvard Business Review. The Big Idea. May 2018

Dragos (2017). TRISIS Malware: Analysis of Safety System Targeted Malware. https://dragos.com/wp-content/uploads/TRISIS-01.pdf

Debois, P. (2011). DevOps: a software revolution in the making, J. Inf. Technol. Manage. 24 (8) (2011) 3–39.

Du Plessis, E.M and B. Vandeskog (2020). Other stories of resilient safety management in the Norwegian offshore sector: Resilience Engineering, bullshit and the de-politicization of danger. Scandinavian Journal of Management 36

Greenberg, A. (2015). Hackers remotely kill a Jeep on the highway – with me in it. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (accessed on January 1, 2020).

Grøtan, T.O., M.G. Jaatun, K. Øien, and T. Onshus (2007). The SeSa Method for Assessing Secure Remote Access to Safety Instrumented Systems. SINTEF A1626 (ISBN 978-82-14-04217-7).

Grøtan, T.O. 2015. Organizing, thinking and acting resiliently under the imperative of compliance. On the potential impact of resilience thinking on safety management and risk consideration. Doctoral theses, NTNU, 2015:86

Grøtan, T.O., 2017. Training for Operational Resilience Capabilities (TORC): Summary of concept and experiences. SINTEF Report A28099:2017

Grøtan, T.O., S. Antonsen. 2016. Take it to the limits! Exploring the hidden, dynamic and emergent vulnerabilities of society. In Walls, Revie & Bedford (eds): Risk, Reliability and Safety. Innovating Theory and Practice. 2016. CRC Press. Taylor & Francis Group

Hanssen, G.K, Stålhane, T. & T. Myklebust. 2018. SafeScrum® – Agile Development of Safety-Critical Software. Springer

IEC 61508. Functional Safety. International Electrotechnical Commission (IEC)

IEC 61511. Functional safety - Safety instrumented systems for the process industry sector. IEC

IEC TS 62443. Industrial communication networks - Network and system security. IEC

IEC TR 63069. Industrial-process measurement, control and automation - Framework for functional safety and security Commission. IEC

Skoglund, M., Warg, F. and B. Sangchoolie. In Search of Synergies in a Multi-concern Development Lifecycle: Safety and Cybersecurity. SafeComp 2018 Västerås.

Hauge, S. and K. Øien (2016). Guidance for barrier management in the petroleum industry, SINTEF A27623 (ISBN 978-82-14-06031-7).

Hollnagel, E., Woods, D. D., & Leveson, N. (2007). Resilience engineering: Concepts and precepts. Ashgate Publishing, Ltd.

Hollnagel, E. 2014. Safety-I and Safety-II. The Past and Future of Safety Management. CRC Press

Jaatun, M. G,, M. B. Line, and T.O. Grøtan (2009), Secure Remote Access to Autonomous Safety Systems: A Good Practice Approach", International Journal of Autonomous and Adaptive Communications Systems 2.3 (2009): 297-312.

Laukkarinen, T., Kuusinen, K., and Mikkonen, T. (2018). Regulated software meets DevOps. Elsevier: Information and Software Technology, 2018. 97: p. 176-178

Myklebust, T., Stålhane, T., and Hanssen, G.K. 2019. Safety Case and DevOps Approach for Autonomous Cars and Ships. in First International Workshop on Autonomous Systems Safety.

Penley, C. & Ross. A (1991). Technoculture. University of Minnesota Press

PSA (2017). Principles for barrier management in the petroleum industry. March 15, 2017.

Roe. E. and P. Schulmann. 2008. High Reliability Management. Operating on the Edge. Stanford University Press.

Shorrock, S. (2016). The varieties of human work. https://humanisticsystems.com/2016/12/05/the-varieties-of-human-work/