Agile Approaches in Critical Infrastructures

Geir Kjetil Hanssen[1][0000−0003−2718−6637] and Martin Gilje Jaatun[1][0000−0001−7127−6694]

SINTEF, Trondheim, Norway

Abstract. This paper explores the emergence of agile-inspired approaches in the critical infrastructure sector, with a focus on the current digital transformation of the Norwegian Oil & Gas industry. It addresses how traditional plan-driven development and strict architectural principles are challenged by the need to exploit the growing volume of operational data, in search for better, faster, and safer operations. We emphasize the increasing reliance on data for optimizing operations and the inherent risks and culture clashes between Information Technology (IT) and Operational Technology (OT). We furthermore discuss the role of cybersecurity in this transition, illustrating how increased connectivity and agile-like approaches can both mitigate and exacerbate security vulnerabilities.

Keywords: Agile Development · Critical infrastructures · Digital Transformation · Security · Safety.

1 Introduction

All aspects of our society are being digitalized, where increasing amounts of data are gathered, shared, analyzed, and used to improve almost every conceivable aspect of our lives. Well-known examples are streaming services, where we consume media in totally different ways than before, where data about how we consume media is used to tailor content and increase consumption. Another example is banking services that only can be accessed via self-managed solutions. Following this development, we also see a very clear trend of digitalization also within critical infrastructures, such as energy production and distribution systems. This is however an industry that is "invisible" to the everyday consumer. It's based on traditional and trusted technologies and a conservative and change-resistant culture where the pace of change is moderated by strict regulations, where change must be restricted and controlled to minimize unintentional mistakes, which – in worst case scenarios – can lead to catastrophic events, and ultimately loss of lives [3].

In this paper, we look into the Norwegian Oil and Gas sector which is currently undergoing a massive digital transformation [3]. In short, operational technology (OT) systems, e.g., drilling systems on off-shore installations, are being instrumented (e.g., via edge devices) and used as data sources to gather vast amounts of detailed data that are used to optimize drilling. Another example is data that are harvested from production equipment used to monitor wear and tear to enable predictive maintenance, where there are great cost savings in replacing expensive equipment only when needed, instead of at fixed service intervals. The main driver for such digitalization efforts is the search for faster and more efficient operations [9]. In the case of oil and gas production, it is about producing more energy resources, within shorter time, at lower cost, while also ensuring high operational availability and maintaining very strict safety requirements.

In Norway, oil and natural gas is produced at very large off-shore installations that rise hundreds of meters above the sea bed, and where resources are extracted through drilling holes reaching kilometres below the sea-bed. These are complex installations consisting of complex sub-systems, ranging from highly specialized operational technologies (OT) where the production happens (the so-called “sharp end”), to traditional IT-systems that are used by administrative personnel. In between, we find control systems, historians (time-series databases), functional safety systems (e.g. fire- and gas detection), etc. As a mean to enable overview and control, systems are logically arranged in layers, from layer 0 where we find the most critical operational technologies, to level 4 where we find traditional IT and office support systems. This layering of the system is often referred to as the Purdue model [13], illustrated in Fig. 1. Level 0 is the production level, where the consequences of failures are the highest and respectively, the need for protection is the highest. Level 1 is the control-level (controlling level 0), level 2 controls several sub-areas (e.g. drilling), level 3 controls the operation of a site (e.g. a well). Levels 0 to 3 is often known as the manufacturing zone. Over the past years, a level 3.5 has been introduced as a demilitarized zone, separating Level 4 and 5 which is called the enterprise zone (low-criticality) from Level 3-0 (high criticality). Level 4 and above are referred to as the IT-levels, while levels 0-3 are referred to as the OT-levels.

The rationale for organizing such complex systems in layered zones is that each layer can have varying levels of criticality, and that control and communication between layers are easier to manage, and that the flow between two layers have to pass through those in between.

This way of organising the system is however being challenged as a consequence of the digitalization of this industry. For example, we can now define a new (IT) level 6 - which is the cloud level that is connected via the Internet above the enterprise zone, and that even can be outside the organization itself in cases where one of the major cloud providers manage data at external infrastructures. Adding to this, new system providers enter the market to offer value-enhancing services (a.k.a. "AI magic") where large amounts of data (gathered from the operational level) are used to provide services that can increase efficiency. For example, data about production can be used to deliver operator support systems, where people, e.g., at the drilling deck, get better insight and decision support via handheld devices. This, however, means that the flow of data and control no longer always passes through the layers (and the protection that these offer) [3]. Furthermore, providers of such solutions may also want to gather data directly from lower levels to fully control the quality of data.

In sum, we see clear trends that the traditional control of *how* data flows between layers are challenged as a consequence of the digitalization of this industry with increasing amounts of data and - hence - increasing reliance on software-based systems.

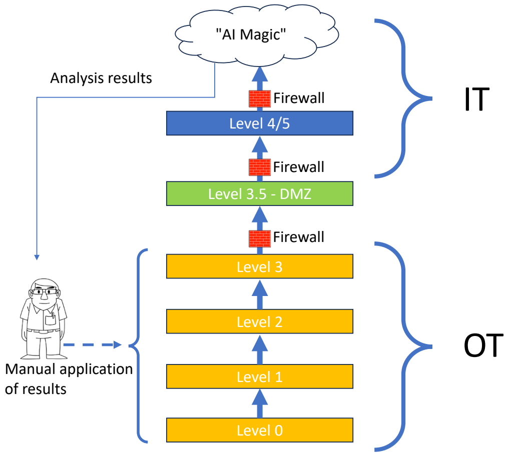

Fig. 1. To the cloud – and back again

2 The Challenge

2.1 Culture Shock

There are enduring culture differences between IT and OT. Traditionally, the speed of change can be perceived as lightning vs. glacial in IT and OT, respectively. Hence, we see that agile approaches are very relevant to the development of IT-systems, while development of OT systems are subject to plan-driven approaches. This is related to the need to enforce very strict control of change in OT-systems through certification procedures that ensure that changes are done according to very detailed international standards and regulations, which again requires high precision in traceability from requirements to implementation. The petroleum industry is a conservative domain, that now needs to deal with an increasing speed of change at the IT-levels and an expanding attack surface, exposing the OT levels.

Traditionally, there has been a hard separation of IT and OT, also because when bad things happen in the latter, really bad consequences tend to follow.

This schism also manifests itself in the dichotomy between security and safety [8] – IT usually only needs to worry about the former, whereas OT is predominately concerned with the latter. This is thus a very mature sector when it comes to safety; how can we capitalize on this in the area of security?

With new IT and software vendors are entering the critical infrastructure domain, culture is a major hurdle. Many of the players in the big data analytics space come from the IT side, and see no problems with siphoning sensor data from the lowest level, working their magic on the data in the cloud (Fig. 1), and using the results to optimize processes in the sharp end. Many of these new players are also relatively small, and do not have the rigid bureaucratic processes common in large enterprises, like suppliers of classical process control systems. It is therefore not surprising that a large number of these smaller, new IT vendors operate under agile principles that have become the norm for non-critical applications.

In a recent report by Vedere Labs [12] it is stated that OT vendors lack a fundamental understanding of security by design, and that existing security control designs are often broken.

Another consequence of this is that vendors often release low-quality patches. This situation is exacerbated by the fact that many industrial control systems still offer no appreciable security once the "hard crunchy shell" of perimeter security has been breached [1].

2.2 A need for agility?

In search of a way to respond to the described development and challenges we see that the mindset from agile software development practices may be relevant. Firstly, requirements tend to change more frequently from the dynamic thereat picture that follows the growing connectivity as well as the increasing amount of data-savvy services that are being offered from new actors. Such new actors may not have the safety-mindset that the established providers of traditional control systems have. Hence, frequent evaluation of the threat situation, and following, faster feedback-loops and reaction to threats (e.g. patches or other security measures) can be a good strategy for having a closer control with rapid change [5]. Secondly, an agile mindset may also offer better (and faster) innovation capabilities. where access to richer data (and new technologies) can be used to create, test, and evaluate ideas faster. Thirdly, an agile approach can also offer a better strategy for following up new actors more closely to ensure that they adhere to the needed safety standards of this domain. Again, frequent evaluation and feedback (and corrections) is the key.

3 How to tackle challenges/way forward?

There is a lot of technology in OT, but unlike in IT, uptime and accessibility are extremely important and can only be sacrificed in situations where the safety of people or the environment is at risk. There is a need to handle the span between control and agility – where the conventional wisdom in OT goes beyond "if it's not broken, don't fix it" to the point where even in cases where there are known vulnerabilities in an OT system, the default stance is that change should be avoided, as it might break a safety certification, and thus lead to a halt in operation, which can be extremely costly. However, this stance is being challenged by the new players. The digitalization of OT, with more edge devices and sensors, and lots of data transferred to, and processed in the cloud, implies an agile transformation. The data is used for optimization of processes, but that means that the results need to be fed back into lower parts of the Purdue stack.

So, within this landscape of digitalization of previously isolated and strictly controlled — and thus, secure — systems, which principles could we turn to, in search of a more agile, but still secure (and safe) approach?

3.1 Safe&Secure Agile Development

With more data and more software in safety-critical systems, it becomes more attractive to work in an agile manner to increase responsiveness and efficiency when changes are needed. The challenge though is of course the need to maintain security and to not introduce new vulnerabilities. One viable approach could be to apply existing approaches for agile development of safety-critical systems, such as R-Scrum [2] or SafeScrum [4], but where cybersecurity considerations are managed in tandem with safety considerations. SafeScrum for example, is an agile development approach that is well aligned with the generic IEC 61508 [6] standard for functional safety. However, we believe that such approaches could be extended to consider safety and security, jointly. In fact, such an approach would be highly relevant in cases where cybersecurity directly relates to safety. Furthermore, it could also be relevant to extend such agile processes to adhere to both safety and security standards, like IEC 61508 and the IEC 62443 [7] standard series, which rapidly is becoming the go-to standard for cybersecurity for operational technology in automation and control systems (amongst others).

3.2 Zero Trust

Zero-trust [11] is currently a popular buzzword in OT, and for the particular case at hand it may be vital. Optimization decisions made in the cloud need to provide an audit trail and provenance, ensuring that no party have had the opportunity to tamper with the information on the way to or from the cloud. On the simplest level, it implies that any results need to be provided with a digital signature that can be verified before these results are being used to modify OT processes. Furthermore, if system engineering becomes more agile, security needs to follow, and security must be automated whenever possible.

3.3 Cybersecurity Barriers

The petroleum industry has a long tradition in implementing safety barriers, e.g. safety valves in connection with Emergency Shutdown Systems. Introduction of agile principles also highlights the need for additional *cybersecurity barriers*.

Preliminary studies and ongoing work indicate that cybersecurity barriers may intergrate well with traditional safety barrier management, focusing on identifying and managing existing cybersecurity measures rather than solely deploying new ones. This integration is essential for maintaining the security and integrity of operations against new and evolving digital threats [10].

4 Conclusion

Critical infrastructures, exemplified here by the Oil & Gas-industry, are undergoing an inevitable digital transformation that leads to an increased flow of data and potential new cybersecurity vulnerabilities. Well-established principles for protection are being challenged and operational technologies are exposed to an increasingly more dynamic threat landscape. We argue that some of the key principles in agile development should be considered in search for better ways to ensure cybersecurity and system safety, and that there is a need for improved feedback loops to ensure better responsiveness to emerging threats.

We have identified three challenges: (1) The need for an integrated culture between IT and OT, (2) Newcyber-security challenges, and (3) The need for technological responsiveness. Further work will explore how these should be addressed.

Acknowledgements

This work has been funded by the Research Council of Norway as part of the Cybersecurity Barrier Management project, grant number 326717.

References

1. Dragos: PIPEDREAM: CHERNOVITE's emerging malware targeting industrial control systems. Whitepaper, `https://hub.dragos.com/whitepaper/chernovite-pipedream`
2. Fitzgerald, B., Stol, K.J., O'Sullivan, R., O'Brien, D.: Scaling agile methods to regulated environments: An industry case study. In: 2013 35th International Conference on Software Engineering (ICSE). pp. 863–872. IEEE (2013)
3. Hanssen, G.K., Onshus, T., Jaatun, M.G., Myklebust, T., Ottermo, M., Lundteigen, M.A.: Principles of digitalisation and IT-OT integration. Tech. rep., SINTEF Digital (2021), `https://www.havtil.no/globalassets/fagstoff/prosjektrapporter/ikt-sikkerhet/sintef---report---principles-of-digitalisation-and-it-ot-integration.pdf`
4. Hanssen, G.K., Myklebust, T., Stålhane, T.: SafeScrum® – Agile Development of Safety-Critical Software. Springer International Publishing, Switzerland (2018)
5. Hanssen, G.K., Thieme, C.A., Bjarkø, A.V., Lundteigen, M.A., Bernsmed, K.E., Jaatun, M.G.: A continuous OT cybersecurity risk analysis and mitigation process. In: Proceedings of the The 33rd European Safety and Reliability Conference (ESREL 2023). Research Publishing Services (2023). https://doi.org/10.3850/978-981-18-8071-1_P413-cd, `https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/3103209`

6. IEC: IEC 61508-1:2010 functional safety of lectrical/electronic/programmable electronic safety-related systems
7. IEC: IEC/TS 62443-1-1:2009 Security for industrial automation and control systems - Part 1-1: Terminology, concepts and models (2009)
8. Line, M.B., Nordland, O., Røstad, L., Tøndel, I.A.: Safety vs security? In: PSAM Conference, New Orleans, USA (2006)
9. Lu, H., Guo, L., Azimi, M., Huang, K.: Oil and gas 4.0 era: A systematic review and outlook. Computers in Industry **111**, 68–90 (2019)
10. Øien, K., Hauge, S., Jaatun, M.G., Flå, L., Bodsberg, L.: A survey on cybersecurity barrier management in process control environments. In: 2022 IEEE International Conference on Cloud Computing Technology and Science (CloudCom). pp. 113–120. IEEE (2022). https://doi.org/10.1109/CloudCom55334.2022.00026, https://ieeexplore.ieee.org/document/10005352/
11. Sanders, G., Morrow, T., Richmond, N., Woody, C.: Integrating zero trust and DevSecOps. Carnegie Mellon University Software Engineering Institute White Paper (2021), https://apps.dtic.mil/sti/trecms/pdf/AD1145432.pdf
12. Vedere Labs: OT:ICEFALL - The legacy of "insecure by design" and its implications for certifications and risk management. Tech. rep., Vedere Labs (2022), https://www.forescout.com/resources/ot-icefall-report/
13. Williams, T.J.: The Purdue enterprise reference architecture. Computers in Industry **24**(2), 141–158 (1994). https://doi.org/https://doi.org/10.1016/0166-3615(94)90017-5, https://www.sciencedirect.com/science/article/pii/0166361594900175