HSE and Cyber Security in Remote Work

Lars Bodsberg, Tor Olav Grøtan, and Martin Gilje Jaatun
Software Engineering, Safety and Security
SINTEF Digital
Trondheim, Norway
{lars.bodsberg, torog, martin.g.jaatun} @sintef.no

Irene Wærø
Technip FMC
Trondheim, Norway
irene.waeroe@technipfmc.com

***Abstract*—Digitalization and increased use of remote operations is a growing industrial trend. Work that previously had to be done physically on a facility, can now be conducted from remote locations. However, remote operations may lead to new vulnerabilities and risk. This paper presents results from a study on Health, Safety and Environment (HSE) consequences and cybersecurity in remote operation of oil and gas installations. The paper addresses digital technology that supports, controls and monitors industrial production and safety functions (Operational Technology), and not general (administrative) Information Technology. A main challenge in remote operations pinpointed in the study, is the increased complexity and interactivity for managing crisis situations. Thus, increased collaboration between operator companies and system suppliers should be facilitated, including regular physical meetings. The distinction between work process and work form is important in understanding the necessary reorganizing of work when implementing remote operations. Further development of cyber security practices should draw more heavily on the ideas behind the resilience concept. The study is based on 14 group interviews with representatives from operating companies, drilling companies and system suppliers.**

***Index Terms*—HSE, Cyber Security, Industry 4.0, Reliability and Safety, Cyber-Physical Systems, Oil and Gas industry**

I. Introduction

Operating companies and system suppliers in the petroleum industry have for a long time been able to monitor and maintain industrial control and safety systems (ICS) using remote access [1]. Remote access is therefore nothing new, but the current digitization trends means that new work processes and forms of collaboration between operator companies and system suppliers are established [2]. Once an installation has been commissioned (for example, after one to two years), professionals with in-depth knowledge of ICS (2nd line personnel) can perform remote operations from other locations, often in collaboration with employees at the installation who have some knowledge about the systems (1st line personnel). Planning and execution of remote operations can be done with the support of system suppliers' own specialists in the systems (3rd line personnel) [3].

An ICS is a real-time system that must satisfy stringent requirements for reliability, availability and integrity to maintain operational performance. System failure may cause lost production as well as adverse Health, Safety and Environment (HSE) consequences. Based on technical safety requirements, the ICS has been developed to be independent of other IT systems. IT systems, on the other hand, largely communicate with other systems. Historically, there has been a different philosophy for managing access rights for IT systems and ICS.

Until recently, this strategy has shielded ICS from the exposure to hackers, but that has changed. Piggin [4] warned that hackers are directing their activities toward the technology commonly found in power stations, factories and other infrastructural facilities, and discuss how engineers managing these systems must understand the rising risk, and ensure that safeguards are implemented.

In August 2017, a petrochemical company with a plant in Saudi Arabia was hit by a new kind of cyberattack. Investigators believed that the attack was not designed to simply destroy data or shut down the plant, but meant to sabotage the firm's operations and trigger an explosion [5]. The hackers had deployed malicious software, or malware, that let them take over the plant's safety instrumented systems. These physical controllers and their associated software are the last line of defense against life-threatening disasters [6]. This type of threat must be considered as even more severe during remote operations.

This paper investigates this challenge for oil and gas installations from a sociotechnical and situated practice perspective, thus recognizing that the difference between security and insecurity is decided by "work as done", rather than "work as imagined" [7], in the same manner as for the distinction between safety and accident. The sociotechnical perspective employed is resting on a distinction between work processes and work forms [8], and a digital complexity perspective of re-presentation [9], not explicitly elaborated in this paper.

II. Objective

This paper presents results from a study on HSE and cybersecurity in remote operations in the Norwegian petroleum industry, including offshore and onshore petroleum installations as well as drilling rigs [10]. A main objective was to gather knowledge on the extent of remote work, and explore important factors contributing to common situational awareness and safe work practices.

When assessing HSE consequences and cyber security in remote operations, we distinguish between:

1) Remote work, where software changes are made to ICS via remote access (”write access” - which is the focus of this paper)

2) Remote support, where ICS is monitored and debugged via remote access (”read access”).

Although the paper is aimed at Operational Technology (OT), and not general (administrative) Information Technology (IT), it is worth mentioning that general IT or office systems are often a target of cyber attacks [11] – partly due to the use of commodity software and extensive connectivity. Once an attacker has gained access to the office systems, this access can be utilized to gather information that can be used in planning and preparing for a cyber attack on the corresponding ICS [12]. For example, people with access to office systems may create new users, collect login information, or scan and map infrastructures.

III. Research Method

The analytical framework for the study and interview guide is largely based on two SINTEF reports by Grøtan and Albrechtsen [13] and Rosness et al. [14].

The latter addresses framework conditions for HSE work in the Norwegian petroleum sector, while the former is a synthesis of 11 hypothetical trends for remote work in the offshore petroleum sector also based on

- An approach to complexity that recognizes that systems are undergoing continuous change, that the dynamics of change are linked to stakeholder relationships as much as local adaptations, and that this is all about continuous balancing of human, technical, and organizational conditions (MTO-balances).
- A description of two different but related forms of MTO-balance: 1) the balance between work process and of work form, and 2) a shift from a focus on value creation in the individual organization to value creation through the interfaces of interaction.
- A perspective on IT as “re-presentation” technology that issues a warning that the flexibility provided by IT primarily facilitates coordination of the work process rather than comprehensive understanding of the work to be done (that is, including the work form).

Simply put, the work process is the idealized description of a sequence of tasks devised necessary to produce an intended outcome, while the work form refers to the additional activities or informal ways of doing the work, in order to produce the result in practice. This distinction is not identical to but resembles the main line of distinction between “work as imagined/prescribed” and “work as done/ disclosed” by Shorrock [15]. Reaching across this distinction is important for enabling discovery of adaptive (resilient) properties of existing cyber security practices.

The empirical material is based on 14 group interviews in autumn 2018 / winter 2019 with representatives from operator companies, drilling companies and system vendors (see TABLE I). Several of the interview subjects had long experience from petroleum activities and extensive knowledge of solutions and procedures for remote operation, not only in their own company, but also in several other companies. All interviews were guided by an interview guide. Questions were elaborated during the interview depending on the topics raised by the informants. In addition to the group interviews, a half-day workshop was conducted with 9 participants from operating companies, system vendors, the Norwegian Maritime Directorate and the Petroleum Safety Authority Norway.

To avoid conflicts with research ethics and privacy regulations, no audio or video recordings were made of the interviews or the workshop. Instead, each interview was performed by at least two investigators, where one had the primary responsibility of asking questions, and the other taking notes.

The empirical material is analysed in two ways; 1) by grouping the findings thematically (”Main findings”) and 2) by investigating to which extent they support the 11 hypothetical trends for remote work (”Detailed results”) (Section V)

Regarding the latter, the empirical material in this report is too narrow to support a hypothetical-deductive investigation ending with strong conclusions. However, we still find it reasonable to interpret the findings in the light of this theoretical framework. If enough support is found in the empirical material, the theoretical framework can be used to recognise key trends, to guide and correct further development, and to inform and guide future research related to the link between HSE consequence and cyber security. Ultimately, it could thus facilitate an improved level of cyber security that is more acquainted with actual work practices. Moreover, by elaborating the key adaptive properties of work forms to the overall equation, we can also envisage a conceptual basis for understanding situated cyber resilience [9] rather than cyber security merely founded on “work as imagined”.

IV. Main Findings from the interviews

The main findings from the interviews are presented below. The term “installation” denotes both onshore and offshore petroleum facilities as well as drilling rigs.

A. *Extent of remote work*

Technical and operational personnel interviewed are largely sceptical to allow changes to ICS via remote access. Some informants experience pressure to increase the extent of remote work on offshore installations and make changes from shore.

The current practice is to test any software changes onshore before they are implemented on the offshore installation. However, onshore testing does not verify all functionality of ICS, as full functionality requires on-site personnel offshore to observe actual performance of the physical systems.

There are different strategies for remote work among operating companies. This may be explained by a large variation in company size and installation age. For example, with one company, the strategy is to gather its own personnel for operational support in an onshore operations center so that the engineers can operate multiple installations. At another company, the strategy is to keep engineers offshore to ensure adequate local knowledge of ICS, as these systems are becoming increasingly complex.

TABLE I
PARTICIPANT BREAKDOWN

Organisation	Number of participants	Competence and experience
Offshore operator	23	Managers/ system administrators/ specialists from operations center, automation department, drilling department, plant integrity, ICT security and ICT infrastructure
Onshore operator	9	Managers/ system administrators/ specialists from SAS, telecom, electrical systems, fiscal measurement systems, automation, maintenance and modifications
Drilling companies	5	Managers/ specialists from drilling technical integrity and IT/OT
Vendors/suppliers to onshore or offshore installations	7	Specialists with extensive experience from supply and support to installations on the continental shelf
Vendors/suppliers to drilling companies	6	Managers/ specialists with extensive experience with control systems, drilling systems, safety and operation support

B. Remote work management

All installations have specific work processes and associated technical solutions for user access to ICS. The purpose is to contribute to secure identity and access control so that only personnel with a defined need get the right level of access. Considerations when deciding on user access include the need for user access, what systems one can access, what type of access is needed and the required duration of access.

Increasingly, systems and devices require a personal username / password for remote work. On older systems, there may still be shared usernames, and it is thus technically challenging to restrict different accesses to individual systems. Hence, it is difficult to find measures that can prevent unwanted actions from a user who has only accessed a less critical system.

All installations provide remote access as part of the work permit process, and those who must carry out remote work must be invited by personnel in a dedicated position in the operating company. Work processes for safe operation of an installation are the same for remote work as for work carried out on the installation itself, i.e., secure job analysis and work permit systems are essential both with and without remote access.

C. HSE consequences for those involved in remote work

As ICS becomes more complex, some 1st line personnel experience increased uncertainty and extra need for support from specialists. The informants agree that remote work provides increased access to specialist expertise from 2nd and 3rd line personnel.

Remote work enables better working time arrangements for service personnel and engineers through fewer trips to offshore installations. Some engineers in operator companies experienced better work environment working onshore compared to offshore, mainly due to ease of contact with other specialists. Some onshore workers stated that they experienced increased job satisfaction when they still had the opportunity to take some trips to offshore facilities. According to some system suppliers, the social benefits of offshore work were limited. It is not always easy to get in touch with offshore personnel as a service employee with limited time available at the facility.

The use of dedicated rooms for remote work provides extra opportunities for concentration on work tasks. Incident management service onshore should be organized to ensure that personnel have enough local knowledge of the installations [16]. It may be challenging to deal with specific technological solutions for an installation when service personnel work remotely on several different installations. One suggestion may be to state that personnel should not work on different installations simultaneously. However, a dedicated room with access control has a negative effect on work environment as it limits personnel's contact with other colleagues. This is particularly perceived as a challenge during night shifts.

D. Common situational awareness for safe operation

Situational awareness has both in previous studies [17] and in the current study been pointed out as a potential challenge when working remotely. Important factors that contribute to common situational awareness and safe decisions[1] in remote work are clear guidelines, good communication and local knowledge. Requirements for system and installation specific knowledge is even more crucial for those working remotely. Understanding the consequences of one's actions in the system and the other work operations performed, is often a necessity for safe operation. Good local knowledge is also important because applications will never be fully standardized. Informants particularly pinpointed the importance of physical access to, and hands-on information from, drilling equipment on drilling rigs. It was also pointed out by some, that more digitalization requires increased focus on situational awareness since less personnel will have the total overview of the risks and work conducted.

E. Cyber security in remote work

Remote update of software in ICS imposes the need for additional countermeasures to protect against cyber attacks. Interviewees expect today's solutions for remote work to be continued with even greater emphasis on:

[1] A safe decision is a decision that does not lead to adverse effects for HSE

- Dedicated rooms for remote work, including restrictive access control.
- “Clean” PCs that are used only for remote work on ICS.
- Security requirements in contracts.
- Online monitoring and analysis of networks and connected systems.
- Compliance with established security guidelines and work processes.

V. Trend picture supported by interviews

In the following we detail the trends identified in remote operations, supported by comments from informants.

- Trend: Need to focus not only on work process, but also on underlying working method (= work forms)
  - Remote work enables faster support to operators and drilling companies, and system suppliers may be better prepared for the work.
  - System supplier can offer troubleshooting 24/7 from “anywhere in the world”.
  - Increased complexity in ICS can lead to increased competence requirements. Perceived uncertainty among field personnel may demand extra need to support specialists from onshore.
  - Increased collaboration between operator and system supplier in project development provides improved overview for system supplier and contributes to more comprehensive solutions.
  - Important systems in drilling operations will still be operated on site. Several companies are presently involved in a drilling operation and the operations will continue to be fragmented. However, introduction of new technology may facilitate automation of some tasks.
  - There may be more ad hoc work onshore to solve immediate problems offshore. This can result in more Irregular work hours onshore.
  - Personnel onshore may miss important feedback from the offshore production process (challenge to situational awareness).
  - It may be easier to use the person who is available onshore, rather than postponing work and use someone who has adequate local knowledge of the installation.
  - Some operators do an extra check of personnel expertise before personnel who have not been to the installation before, can work remotely.
  - Technical personnel have pronounced scepticism to allow software changes on safety instrumented systems through remote work. Local knowledge about the individual installation, physical proximity to the installation (i.e., conditions outside the formal work process) is emphasized as essential.
  - Emphasizing strict access control (in time, space and activity) for cybersecurity provides even more focus on the formal work process (e.g. procedures), and less room for developing new working methods.
  - Someone uses chat as communication channel during remote work (Can be interpreted as need to maintain informal work practices).
  - Increased awareness of insider risk. (This can be interpreted as follows: the personal knowledge and relationships created through presence in the same physical location, may be seen as a flexible work form. New work processes, e.g., formal clarification meetings and monitoring of service personnel during work, emerge to compensate for personal acquaintance in a small community of practice, leaving behind a perceived new risk factor.
  - According to system suppliers of drilling control systems, participation in online preparedness teams is perceived as recognition of competence and is therefore attractive for personnel to join. This may be interpreted as an appreciation of work forms as an informal competence
  - Some system suppliers perceive any monitoring of the execution of their remote work processes/operations by operating companies, as negative.
  - Dedicated room for remote work contributes to better concentration.
- Trend: Expanding focus from completing work to planning work
  - Better response time and access to expertise on land. Specific expertise is better utilized for several operators and drilling companies.
  - Increased collaboration between operators/drilling companies and system suppliers during design
  - Personnel from different organizations are physically gathered in the same premises and in joint teams.
  - Better opportunities for planning and knowledge transfer between “junior” on site and “senior” in remote location.
- Trend: Continuous change processes leading to experimentation, continuous adjustments and focus on responsibilities.
  - Major differences in collaboration strategies between operators and system suppliers: 1) Operators have ICS engineers onshore to operate multiple facilities vs. retaining engineers offshore to secure local knowledge. 2) Operators develop own specialist knowledge of ICS to be independent of system supplier vs. give system supplier responsibility for daily operations.
- Trend: New decision-making processes are based on the assumptions of easy access to large amounts of real-time data and unrestricted access to varied expertise. Access to expertise will be scarcer than access to data
  - Advanced data analysis is expected to replace the current analysis work done by the system suppliers and reduce the need for periodic maintenance.

  - System suppliers should ensure that personnel working remotely, have adequate local knowledge of the installation and do not work on two installations simultaneously. There is a significant possibility that someone will be “thrown” into tasks on unknown installations during unplanned work outside normal working hours.
  - A dedicated group for 24/7 services should be organized for event management.
  - Drilling operations are automated by implementing drilling plans directly in the drilling control system without the involvement of drillers. This will place greater demands on the quality assurance of the drilling plan.
  - System suppliers for drilling equipment offer tailored courses to improve competence for operator personnel who remain on the drilling rig. There is a high demand and limited number of personnel with cutting-edge expertise in digitalization.
  - Increased access to specialist expertise for offshore personnel is positive, but service personnel must know the peculiarities of the installation.
  - Personnel involved in the project and start-up phase will have better local knowledge in the operational phase.
  - Rotating personnel between various work positions contributes positively.
  - Currently, changes to ICS are planned and controlled by both onshore specialists and operating personnel at the installation. System suppliers can simulate the effect of proposed changes before implemented on an installation.
- Trend: Greater access to a broad repertoire of knowledge, resources and expertise through the interfaces between different actors. This consequence applies to the operator, system suppliers and subcontractors in day-to-day operational tasks and decisions, as well as in crisis situations.
  - System suppliers have their own courses for employees who performs remote work.
  - System suppliers provide 24/7 services for drilling equipment.
  - During incident management, it is easier to trust someone sitting in the neighbouring chair than one located offsite.
- Trend: Facilitation for close collaboration in multidisciplinary teams that are independent of the individual’s organizational and geographical location.
  - New collaborative models where system supplier and operator work physically together are mentioned as an opportunity.
  - Remote work requires extra attention and preparedness in the event of unexpected events.
- Trend: Increased complexity and interactivity make it more difficult to manage crisis situations
  - Some installations have a display that shows “remote work in progress”.
  - Digitization may increase competence through increased utilization of data and better reports.
- Trend: Increased focus on the development and availability of information and knowledge. New competence / understanding is not created by sharing data alone
  - Digital twin may lead to increased knowledge and understanding of equipment in operation, and force (efforts to) increase understanding.
  - Remote work does not necessarily create complexity. Collaboration across companies may seem more complex, but collaboration also helps one learn more from each other.
- Trend: Personal / organizational quality relationships are important to deal with perceived inter-organizational complexity. However, there is a need for the industry to make a clearer distinction between what is complicated and complex. A concept such as “quality relationships” is positively charged but should be clarified through examples.
  - To a certain extent, security can be improved by closer cooperation between operator and system supplier during both design and operation phase.
  - Engineers find it more sociable to be located together with specialists onshore compared to offshore.
- Trend: Digital nomads - is that a problem?
  - Job content for onshore engineers is enriched by (periodic) offshore stays.
  - The social benefits of working offshore are limited, it is not always easy for service employees to get in good contact with offshore personnel and get support in the work situation.
  - Since control rooms are increasingly moved offsite, personnel working remotely has lost the opportunity to visit the control room to get tacit knowledge which is difficult to transfer to another person by means of writing it down or verbalizing it.
- Trend: Challenges in establishing and maintaining common situational awareness across geographical distances and disciplines
  - Unmanned installations with less safety systems need more electronics / instrumentation to compensate for the presence of people. This affects SAS and communication systems.
  - Local knowledge is important. Demanding to sit in the operating room when operating different generations of equipment.
  - Greater competence requirements for personnel working remotely than for those who are physically at the installation.
  - Sound can be an important source for situational awareness, e.g. in drilling operations.
  - (Differences in) Language and terminology present challenges.

VI. Discussion

In section V, some key elements pointed out by the informants are mapped with more detailed assumptions embedded in the overall trends derived from the theoretical framework.

Although the informants' key points are not exclusively relevant for the assumptions they are mapped to here, in sum they strongly hint in support of the hypothesises. A main takeaway is that the distinction between work process and work form makes sense in understanding the necessary reorganizing of work, not at least in the sense that lost work forms cannot be directly replaced by new (formal) work processes, and that even new work processes may need support from a (new) work form that cannot be prescribed in advance. Furthermore, the shift of focus towards planning, the presumption of sustained rearrangement of work encompassing experimentation, the rise of expectations to new decision processes based on easy access to data and sharing of knowledge and expertise, and expectations of facilitation for close collaboration in multidisciplinary teams that are independent of the individual's organizational and geographical location, are all supported to the extent that they should be considered in processes of organizational diagnosis, development and relevant research activity.

However, the findings also support the presumption that increased complexity and interactivity make it more difficult to manage crisis situations. Informants are also aware that new competence and understanding is not created by sharing data alone, and that personal and inter- organizational quality relationships are important to deal with inter-organizational complexity [18].

A concept such as "quality relationships" is positively charged, but we lack good examples to illustrate the substance of the term. Similarly, we (still) expect that the term "digital nomad" should be helpful, but the prime examples are missing. On the other side, the challenges in establishing and maintaining common situational awareness across geographical distances and disciplines, seems to be highly recognized, and is probably an issue of high concern.

Although the informants' expressions and views do not explicitly reflect, from a strictly academic point of view, the crucial distinction between what is complicated and what is complex, an appreciation of the underlying complexity is present. All in all, the findings indicate that the oil and gas sector is sufficiently primed to advance on a path towards a more ambitious type of cyber security that is more acquainted with actual work practices, and to recognize and include the key adaptive properties of work forms to the overall cyber security equation. In short, the situation demands, and the circumstances allow, a further reinforcement of IT/OT cyber security practices that can draw more heavily on the ideas behind the resilience concept.

VII. Recommendations

Our main recommendations to the industry are:

- Continued focus on access control and user-friendly administration procedures for authorized personnel.
- Facilitate increased collaboration between operator companies and system suppliers, including regular physical meetings.
- More focus on requirements for suitable locations for remote work, including working environment, shift schemes, access control, and measures to improve situational awareness for safe decisions.
- More use of hardware devices (data diodes [19]) as a cybersecurity solution to make sure that information can travel in one direction only. This provides easier access to those who only need "read access".

VIII. Further work

Our main recommendations for further studies of remote work are:

- How to combine safety and security management of ICS; also addressing the cultural differences between IT and OT disciplines?
- How to balance cyber security requirements, work processes and operational safety? This can form the basis for a guide that sets limits for technical complexity and digital vulnerability.
- How to manage unexpected situations during incident management, including knowledge of why things go well? Should avoid rigid rules for cyber security limiting the scope for handling unforeseen events.

Acknowledgment

This study was funded by the Norwegian Petroleum Safety Authority (PSA) in 2018/2019. Thanks to the participating companies and PSA employees who have provided important input to the study. At the time this research was performed, Irene Wærø was employed by SINTEF Digital.

References

[1] M. G. Jaatun, M. B. Line, and T. O. Grøtan, "Secure remote access to autonomous safety systems: A good practice approach," *International Journal of Autonomous and Adaptive Communications Systems*, vol. 2, no. 3, pp. 297–312, 2009.

[2] C. K. Tveiten, "Conditions for resilient operations of complex systems undergoing technological alterations," Ph.D. dissertation, Norwegian University of Science and Technology (NTNU), 2014.

[3] Y. Qian, Y. Fang, M. G. Jaatun, S. O. Johnsen, and J. J. Gonzalez, "Managing emerging information security risks during transitions to integrated operations," in *2010 43rd Hawaii International Conference on System Sciences*, 2010, pp. 1–11.

[4] R. Piggin, "Industrial systems: cyber-security's new battlefront [information technology operational technology]," *Engineering & Technology*, vol. 9, no. 8, pp. 70–74, 2014.

[5] N. Perlroth and C. Krauss, "A cyberattack in Saudi Arabia had a deadly goal. experts fear another try," *New York Times*, vol. 15, 2018.

[6] M. Giles, "Triton is the world's most murderous malware, and it's spreading," *MIT Technology Review*, 2019.

[7] E. Hollnagel, *Safety-I and safety-II: the past and future of safety management*. CRC press, 2018.

[8] V. Hepsø, "Intelligent energy in e&p: When are we going to address organizational robustness and collaboration as something else than a residual factor?" in *Intelligent Energy Conference and Exhibition*. Society of Petroleum Engineers, 2006.

[9] T. O. Grøtan, "Understanding HSE implications of remote work through a digital complexity perspective," in *e-proceedings of the 30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference (ESREL2020 PSAM15)*, P. Baraldi, F. D. Maio, and E. Zio, Eds., 2020. [Online]. Available: https://www.rpsonline.com.sg/proceedings/esrel2020/pdf/4627.pdf

[10] L. Bodsberg, T. O. Grøtan, M. G. Jaatun, T. Onshus, and I. Wærø, "IKT-Sikkerhet – Fjernarbeid og HMS (In Norwegian) (Cyber security and HSE in remote operations)," SINTEF, Trondheim, Norway, Tech. Rep. SINTEF report 2019:00361, 2019. [Online]. Available: https://www.ptil.no/globalassets/fagstoff/prosjektrapporter/ikt-sikkerhet/sluttrapport-ptil-ikt-sikkerhet---fjernarbeid-og-hms-med-underskrift-og-vedlegg.pdf

[11] M. G. Jaatun, E. Albrechtsen, M. B. Line, I. A. Tøndel, and O. H. Longva, "A framework for incident response management in the petroleum industry," *Int. J. Crit. Infrastructure Prot.*, vol. 2, no. 1-2, pp. 26–37, 2009. [Online]. Available: https://doi.org/10.1016/j.ijcip.2009.02.004

[12] C. Stoll, "Stalking the wily hacker," *Communications of the ACM*, vol. 31, no. 5, pp. 484–497, 1988.

[13] T. O. Grøtan and E. Albrechtsen, "Risikokartlegging og analyse av Integrerte Operasjoner (IO) med fokus på å synliggjøre kritiske MTO aspekter (In Norwegian) (Risk analyses of Integrated Operations)," SINTEF, Trondheim, Norway, Tech. Rep. SINTEF report A7085, 2008.

[14] R. Rosness, U. Forseth, and I. Wærø, "Rammebetingelsers betydning for HMS-arbeid (In Norwegian) (Framework conditions for HSE work)," SINTEF, Trondheim, Norway, Tech. Rep. SINTEF report A16926, 2010.

[15] S. Shorrock, "The varieties of human work," 2016. [Online]. Available: https://humanisticsystems.com/2016/12/05/the-varieties-of-human-work/

[16] I. A. Tøndel, M. B. Line, and M. G. Jaatun, "Information security incident management: Current practice as reported in the literature," *Computers & Security*, vol. 45, pp. 42 – 57, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404814000819

[17] A. Sneddon, K. Mearns, R. Flin, and R. Bryden, "Safety and situation awareness in offshore crews," in *Proceedings of the SPE International Conference on Health, Safety, and Environment in Oil and Gas Exploration and Production*, 2004, sPE-86592-MS.

[18] V. Milch and K. Laumann, "Sustaining safety across organizational boundaries: a qualitative study exploring how interorganizational complexity is managed on a petroleum-producing installation," *Cognition, Technology & Work*, vol. 20, no. 2, p. 179–204, 2018. [Online]. Available: https://doi.org/10.1007/s10111-018-0460-8

[19] M. W. Stevens, "An implementation of an optical data diode," DSTO Electronics and Surveillance Research Laboratory, Tech. Rep. DSTO-TR-0785, 1999. [Online]. Available: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.83.8650&rep=rep1&type=pdf

Appendix

INTERVIEW GUIDE GROUP INTERVIEW

A. Background information about participants in group interview

1. Briefly describe the current position and experience from the petroleum industry.
2. What role do you have in the company related to remote operations?
3. What processes are you involved in when it comes to remote operations?

B. Remote work, remote support and remote control mapping

Company level

4. To what extent do current facilities/rigs have remote operations?
5. What typical tasks are performed and on what systems? How often?
6. What technologies and communication channels are used for remote operations? Redundancy?
7. What types of companies have the possibility of remote operations?
8. What new form of organisation/cooperation has been introduced as a consequence of remote operations? Contractual relationship?
9. What are the remote operation drivers? (Limitations, opportunities, mode of operation, expertise, etc.)
10. In a 3 year perspective, what will be the most important changes related to remote operation? (Technology, work processes, forms of collaboration)
11. For rigs: In a 3 year perspective, what will be the most important changes related to automation of work processes?

Selected facilities, rigs and onshore facilities

12. Describe card selected facility/rig/onshore facility
13. Which actors/roles have access to real-time information from the selected facility/rig/plant?
14. To what extent has chosen facility/rig/plant remote operation? What tasks, work processes, systems?
15. What technologies and communication channels are used for remote operation? Redundancy?
16. Which companies have the possibility of remote operation?
17. What new form of organisation/cooperation has been introduced as a consequence of remote operation? Contractual relationship?
18. In a 3 year perspective, what will be the most important changes in relation to remote operation? To what extent are automated/unmanned solutions planned?
19. For rigs: In a 3 year perspective, what will be the most important changes in relation to automation of work processes?

Selected work processes

20. Select and briefly describe relevant work processes that deal with remote operation for different systems (i.e., login to different control systems)
21. Which companies are involved and how does the cooperation between the companies take place in these processes?
22. Can you give examples of new practices as a result of the introduction of remote operation?

C. Assessment of consequences of remote work, remote support and remote control

Working conditions, organisational safety and ICT security

1. What are the main challenges related to working conditions in remote operation based on today's experiences? E.g.,
a. working hours schemes (unpredictable work, long and unsocial work, night work),
b. Job control
c. social support (social and physical isolation, degree of support for problem solving at work),
d. training and exercises,
e. job requirements (unilateral work, fragmented work, uncertainty over job contract, high labour pressures, continuously subjected to deadlines),
f. culture
g. language.
2. What are the main challenges related to organisational

security in remote surgery based on today's experiences?
3. What are the main challenges related to ICT security (OT) in remote operation based on today's experiences?
4. In what way are any security challenges investigated and documented?
5. What new vulnerabilities have been introduced by remote operation?
6. What steps have been taken to address these vulnerabilities?
7. In what way does it ensure that unauthorized persons do not have remote access to systems to prevent intentional actions that could damage the facility/drilling rig/onshore plant?

Changed framework conditions

8. How do you ensure that contracts with suppliers ensure safety in the event of remote operation?
9. Is remote operation a driver for higher pace of change in the industry? If so, in what way?

ICT-supported interaction

10. To what extent has remote operation resulted in organizational changes or new forms of cooperation with implications for security?
11. To what extent has remote operation resulted in change processes, new work content and new ways of working with implications for safety?
12. To what extent has remote operations provided greater access to a broad repertoire of knowledge, resources and expertise through the interfaces between different actors (with operators, suppliers and subcontractors) in daily operational tasks and decisions, as well as in emergency situations?
13. How do you get an overview of all actors and systems that will contribute to safe operation in the event of remote operation?
14. In what way is it clear who has the decision-making authority in remote operation?
15. What are the most important factors for achieving a common situational awareness in remote surgery?
16. How time-consuming is the development of new forms of collaboration?
17. How have altered forms of communication/channels and new group compositions affected security?
18. To what extent has remote operation given an increased focus on the development and disclosure of information and knowledge?
19. To what extent has remote operation given increased complexity in the organization and how does this affect security?

D. Closing

20. Are there topics we have not addressed in this interview that we should have addressed in terms of remote work and HSE consequences?