Barrier Management Digitalization in the Oil and Gas Industry – Status and Challenges

K. Øien

SINTEF Digital, Trondheim, Norway. E-mail: Knut.Oien@sintef.no

S. Hauge

SINTEF Digital, Trondheim, Norway. E-mail: Stein.Hauge@sintef.no

T.O. Grøtan

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

The background for the study described in this paper is the Norwegian Petroleum Safety Authorities (PSA) emphasis on major accidents and barrier management, where maintenance and maintenance management play important parts. Previous studies and the PSA's own supervision have revealed weaknesses and potential for improvement in both barrier management and maintenance management. The PSA therefore conducted studies in 2018 that compiled information regarding the oil and gas companies' status assessment, maintenance and follow-up of safety-critical functions and equipment, including new trends such as digitalization, Information and Communication Technology (ICT) security and new possibilities for data analysis (machine learning, pattern recognition, big data, etc.), also referred to as maintenance 4.0 or predictive maintenance 4.0. In this follow-up study, six selected oil and gas companies responded to a questionnaire on three main topics: i) how to make information on barrier and risk status available, ii) providing information on condition monitoring of early failure development, and iii) information on the extent of digital vulnerabilities and strategies to deal with them. The companies also participated in individual dialogue meetings with the PSA and SINTEF to present, elaborate and discuss the responses. The results in terms of status and challenges for the three main topics are presented along with ten proposals for further work by authorities, oil and gas companies and research institutes.

Keywords: Barrier management, condition monitoring, digitalization, digital vulnerabilities, maintenance, technical condition.

1. Introduction

The main purpose of the paper is threefold. First, it describes the status in the Norwegian petroleum industry with respect to making information about barrier condition and risk status available for all employees requiring such information. Second, it describes the status on condition monitoring, i.e. early detection of failure development for safety equipment. Third, it describes the industry's concerns with respect to possible vulnerabilities in digital solutions, which may affect safety. The links between these three aims are illustrated in Figure 1.

Frequent updating of barrier status (I) is made possible through automatic detection of failures and other impairments. Condition monitoring of early failure development (II) is one such possibility, which can be utilized when describing the current status of the barriers. It also makes it possible to register and "flag" degradations early, even before failures are captured by the maintenance management system, i.e. before notifications or work orders are prepared. However, both systems for presenting barrier status (I) and systems for condition monitoring (II) are examples of digital solutions with potential digital vulnerabilities (III) affecting safety (Øien et al., 2019).

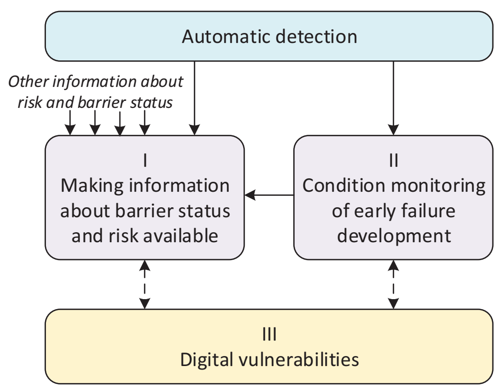

Fig. 1. Links between the three main topics.

Digital solutions are developed to increase safety or production, but it is important to ensure that they do not provide undue or unforeseen vulnerabilities, even if they are made with the best

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

of intentions. Recall that the "Win love in Russia" cyber attack on the safety systems of the gas distribution in Georgia and Turkey in 2008 led to an explosion in a gas pipeline in eastern Turkey (Robertson and Riley, 2014) and that cars have been hacked through the entertainment system (Greenberg, 2015). Thus, attacks can be targeted directly towards the safety systems, or towards utility systems such as entertainment systems or other supporting systems, including systems developed to enhance safety, such as barrier panels.

Another example is the TRISIS malware in 2017 deployed against at least one victim in the Middle East (Dragos, 2017). It targets Schneider Electric's Triconex safety instrumented system (SIS) – thus the name TRISIS – enabling the replacement of logic in final control elements. TRISIS is not a highly scalable attack that could be easily deployed across numerous victims without significant additional work. However, although the attack is not highly scalable, the tradecraft displayed is now available as a blueprint to other adversaries looking to target SIS and represents an escalation in the type of attacks seen to date as it is specifically designed to target the safety function of the process.

Barrier management is a regulatory requirement (PSA, 2019), the PSA has issued a memo on barrier management (PSA, 2017), barrier management was for many years one of four main yearly topics of the PSA, and it is still focused by the authorities. However, the PSA does not require development of barrier panels, although this may be a practical way to fulfil sub-section five of the Management Regulations § 5 on Barriers (Hauge and Øien, 2016). Thus, most companies have developed barrier panels for frequent follow-up of the barrier status.

Early failure detection provided through condition monitoring is rarely included in barrier panels, but exceptions exist (e.g. Edwin et al., 2019). Another exception is the inclusion of the status of operational and organizational barrier elements in the barrier panels (Kilskar et al., 2016), which is still challenging.

The results from this study show that most of the companies have barrier panels that are updated daily. Information on the status of the barriers is made available by these panels, which all employees have access to, or via separate visualization tools. Status is also reviewed in various forums, including daily meetings, such as work permit meetings.

The main users are typically the platform management and operating organization offshore and onshore, and the status information is used for work permit approvals, risk assessments, assessment of compensating measures and prioritization of maintenance. Experience gained is generally positive in that the panel gives a good overview, is useful in daily operations and planning, and provides better understanding of barriers.

All companies provide examples of safety-critical equipment for which condition monitoring data is collected. However, the responses show that there is still limited use of condition monitoring for surveillance of barriers, and that lots of data are not being utilized.

All companies have considered the possibility of digital vulnerabilities, and most believe that there may be digital vulnerabilities when introducing new digital solutions. However, this does not necessarily apply to the barrier panel or the condition monitoring systems currently in use.

Ten issues identified for further follow-up by the PSA were also part of the results from the study. Two of these issues are elaborated in some detail in the discussions.

One of the main conclusions is that the petroleum industry has increasingly made information on the technical condition of safety-critical functions and equipment - barriers - available through the visualization of impairments of these barriers in barrier panels with associated visualization tools. There are however still some companies that have not implemented tools for daily updating of barrier status. Frequent (daily) updating of the status of the barriers is mainly based on maintenance data such as outstanding corrective maintenance (CM) and overdue preventive maintenance (PM) retrieved from the maintenance system. Only exceptionally other types of information about impairments are included in some companies' barrier panels.

Frequent updates of the status of the barrier condition requires automatic harvesting of data, and if possible, the data should also be based on automatic detection of the impairments. Condition monitoring of early failure development is also largely based on automatic detection, and both the barrier panel and the condition monitoring system represent digital solutions that can provide possibilities for digital vulnerabilities affecting safety.

2. Methods

Document review, questionnaire, dialogue meetings, and qualitative analysis have been the main methods used. The study consisted of the following four main activities:

1. Document review and identification of relevant issues
2. Preparation of questionnaire, collection and review of answers
3. Dialogue meetings with selected companies

4. Analysis of status with respect to the main problems being addressed

The following three main topics were highlighted:

I. Making information about barrier condition and risk available
II. Condition monitoring of early failure development
III. Vulnerabilities in the digital solutions affecting safety

2.1 Document review

Relevant issues, within the three main topics, are identified based on a systematic review of the selected background material (DNV GL, 2018; Gressgård et al., 2018; NSOAF, 2018; Øien et al., 2017; Øien and Hauge, 2014; Øien et al., 2018[a]) as well as discussions with the PSA.

2.2 Preparation of questionnaire

The questions were based on findings, recommendations and challenges described in the reference documents listed above. The questionnaire was structured according to the three main topics, with two or three sub-themes for each. The structure with the associated number of questions in brackets (in total 70) was as follows:

I. Making information about barrier condition and risk available
    1. Barrier status/barrier panel (34)
    2. Risk status/risk picture (5)
    3. Overall technical condition and aggregate risk (4)
II. Condition monitoring (CM) of early failure development
    1. CM – utilization (6)
    2. CM – opportunities (4)
III. Vulnerabilities in the digital solutions affecting safety
    1. Vulnerabilities in general (8)
    2. Barrier panel vulnerabilities (5)
    3. Condition monitoring system vulnerabilities (4)

2.3 Dialogue meetings

Dialogue meetings were held as half-day meetings hosted by the PSA, with the six selected companies (June 19, September 4 and September 5, 2019). Both SINTEF and PSA staff participated in the meetings. The companies were asked to present what they considered as the most important from the questionnaire, answer follow-up questions and participate in the discussion of relevant issues.

2.4 Analysis of status

The answers were analyzed mainly qualitatively (and partly quantitatively) and discussed in working meetings with the PSA. Selected responses (providing most learning and insight into the problems) have been reproduced for three of the companies and all responses are summarized (Øien et al., 2019). Based on a summary of the answers, relevant issues for the PSA's further work were identified.

3. Results

3.1 Part I: Making information about barrier condition and risk status available

3.1.1 *Barrier status/barrier panel*

Four of the six selected companies have barrier panels where the status of the barriers is updated daily. Information on the status of the barriers is made available by the barrier panel, which everyone has access to, or via separate visualization tools. Status is also reviewed in various forums, including daily meetings, such as Work Permit (WP) meetings.

The main users are typically the platform management and operating organization offshore and onshore, and the status information is used for work permit approvals, risk assessments, assessment of compensating measures and prioritization of maintenance. Experience gained is positive in that the panel gives a good overview, is useful in daily operations and planning, and provides better understanding of barriers.

Information on failures and impairments that are typically included in the barrier panel is outstanding CM and overdue PM, as well as information on deviations. Data is obtained from the maintenance system and the deviation management system. Only exceptionally, information on overrides is included, and none of the selected companies have included safety alarms from Safety and Automation Systems (SAS) or condition monitoring alarms in their barrier panel. The number of technical

[a] Including about 80 references from this report, which mainly consist of PSA accident investigation reports and safety audit reports.

components/tags that are included as barriers are somewhat different between the companies, but two of the companies estimate that between 4-6% of the total number of components/tags on their facilities are barrier tags.

Three of the companies have included impairments of selected operational and organizational barrier elements in the barrier panel. Information that is typically included is lack of specialized courses, lack of emergency preparedness training, and deviations during emergency preparedness exercises.

3.1.2 *Risk status/risk picture*

The status of the barriers (information via the barrier panel) forms part of the risk status/risk picture, along with other information, e.g. various Key Performance Indictors (KPIs) and information from other systems. The risk picture is communicated through various tools and screens, as well as being discussed in meetings. The main users are typically offshore platform management or operational management, and operations/maintenance, Health, Safety and Environment (HSE) and technical department onshore. The information is used for planning and prioritizing work/ maintenance/activities, WP meetings, as well as deviation treatment, assessment of compensating measures and need for additional resources.

3.1.3 *Overall technical condition and aggregate risk*

All the selected companies respond that they have information about technical condition and risk in different computer systems. When asked about compiled (holistic) information on technical condition and risk, the answers range from reference to the barrier panel or a separate risk tool, or to a manual review in order to obtain a comprehensive overview.

3.1.4 *Example question and selected answers*

Question 4: How do you ensure that the barrier status is made known to the organization offshore?

Three selected answers:

- The barrier status is easily accessible through the barrier panel as well as through other visualization tools. In addition, the barrier status is discussed in various forums, for example in the WP meetings. Courses have also been run for operators and personnel who perform functional testing / maintenance of barrier systems.
- The barrier panel is open to the entire organization. It is used in WP meetings, in welcome meetings for newly arrived shifts and when needed in HSE meetings. The digital WP system panel is continuously displayed on its own screen in the central control room.
- The barrier panel is available to everyone and is actively used in meetings: morning meetings, planning meetings, WP meetings (with tools for overview of WPs and impairments) and evening meetings.

3.2 Part II: Condition monitoring of early failure development

3.2.1 *Condition monitoring - utilization*

All companies have examples of safety-critical equipment for which condition monitoring data is collected. Analyzes performed are deviations from historical trend, comparison of operating profile with baseline, thermography, vibration analysis and analysis of oil samples. However, the responses show that there is still limited use of condition monitoring for surveillance of barriers, and that lots of data are not being utilized.

3.2.2 *Condition monitoring - opportunities*

Two companies have established a center for condition monitoring, and one company is in the process of establishing a center for "Smart Maintenance". Companies with few facilities either have a dedicated position for condition monitoring or the associated discipline (e.g. mechanical, rotating equipment, instrument/ automation, etc.) is made responsible. Most companies have philosophies or plans to utilize automatic condition monitoring to the greatest extent possible, i.e. as much condition-based maintenance as possible. All companies also have plans for predictive maintenance, but few of the companies have implemented this type of maintenance. The plans cover both production equipment and barriers.

3.2.3 *Example question and selected answers*

Question 47: What are the experiences with automatic condition monitoring of barriers?

Three selected answers:

- Good experience where we have good data to analyze failure modes, or where we get additional condition information as well as information from calendar-based mainten-ance.

- Automatic condition monitoring works well, among other things, on transmitters and run time on valves. We create events continuously when the engineer detects, for example, a transmitter that has drifted from process measurement. Then a job is created to calibrate the transmitter.
- Good experience with rotating equipment, identifying early failure development. High regularity (> 90%).

3.3 Part III: Digital vulnerabilities

3.3.1 *Vulnerabilities in general*

All companies have considered the possibility of digital vulnerabilities, and most believe that vulnerabilities will arise when introducing new digital solutions. However, this does not necessarily apply to the barrier panel or the condition monitoring systems currently in use. They point to different solutions for dealing with new digital vulnerabilities, some of which are mentioned below.

Most companies have strengthened, or will strengthen, internal expertise in this area, and the vast majority also reply that they will use external expertise. When it comes to penetration testing, most companies do this on the office network, but not on safety-critical systems during operation.

In order to safeguard ICT security, companies refer to cyber security expertise and cooperation with the Information and Technology (IT) department, the use of security standards based on international frameworks, own performance standards for cyber security, vulnerability assessments, and requirements and work processes that are integrated into access control systems and firewalls.

3.3.2 *Barrier panel vulnerabilities*

Two of the companies respond that data transfer to and from the barrier panel may pose a possible vulnerability, while a third company replies that there is no data flow *from* the barrier panel, but that there may be vulnerabilities due to data flow errors *to* the barrier panel. The other three companies have not identified any particular vulnerabilities to safety-critical systems because the barrier panels only retrieve data from the office network assuming no effect on the safety systems.

3.3.3 *Vulnerabilities of condition monitoring systems*

Most companies respond that they have a continuous focus on vulnerabilities in data quality, data security, and data and network infrastructure in terms of condition monitoring and predictive maintenance.

Four of the companies use external sub-contractors for condition monitoring systems, where access is controlled through remote access connected to the work permit system, or by providing access offshore only (without allowing for remote access).

3.3.4 *Example question and selected answers*

Question 56: Do you / would you like to strengthen internal expertise in handling new digital vulnerabilities?

Three selected answers:

- Yes. This is a continuous task for our technical departments which is also further strengthened.
- Through extensive cooperation between Operations and IT (both at local and corporate level), we will claim that we have internal expertise to handle digital vulnerabilities. The solutions in the market around this are currently relatively immature, but we are constantly evaluating this.
- The company is constantly working to look for new digital vulnerabilities by means of internal and external resources and by participating in professional forums etc. where we can acquire new expertise in this area. The IT department has just hired a new person with cyber security as the main focus.

3.4 The safety delegate service

The main impression is that the companies' elected safety delegates have been well acquainted with the work on barrier panels, and that the personnel have received adequate training. At the same time, the barrier panels are perceived by many as complicated, and one representative for the safety delegate service was particularly critical of the lack of use of Norwegian (i.e. local) language in the barrier panel. One other representative expressed little or no user involvement in the development of the barrier panel.

Concern was also expressed about the introduction of many new digital systems within a short period of time, including changes from existing well-known maintenance systems to new systems.

3.5 Relevant follow-up issues for the PSA

The following 10 issues for further follow-up by the PSA were identified:

1. Active use of information on barrier status among operational personnel, including necessary training, understanding, time, access, recognition and usefulness
2. Specific positive and negative experiences with the barrier panels. What has worked well and what has not worked well (or is still not working well)?
3. How barrier impairments are handled step by step from detection to correction, how this is made visible in the barrier panel (e.g. by traffic lights that change color/status when introducing compensating measures), how the status of the handling itself (not the impairment) is followed up (e.g. KPIs that measure the number of work orders that have not yet been risk assessed), and how this may be displayed in the barrier panel
4. The choice of, and reasons for, the selection of equipment included (and not included) in the barrier panels could have been examined and compared between the companies for transfer of experience
5. Amount and type of information needed to describe the risk picture/risk status at any given time (including information on barrier status)
6. Active use of risk picture/risk status information among operational personnel, including necessary training, understanding, time, access, recognition and usefulness (including information on barrier status)
7. Assessment of overall technical condition versus overall risk picture/risk status and the link between the two related dimensions
8. Main reasons for limited use of automatic condition monitoring and low utilization of existing data, and how this can be improved
9. Main reasons for limited use of predictive maintenance and how this can be improved
10. Digital vulnerabilities in introducing new digital solutions in general, including IT/OT (Operational IT) integration and possible future vulnerabilities of external data representation by new actors with new business models based on big data and machine learning

4. Discussion and Conclusions

Five selected issues that are considered particularly interesting for further follow-up are:

i. Differences in time span between a failure is identified until it is recorded and displayed in the barrier panel
ii. What type of information about barrier impairments should be included in the barrier panel?
iii. Daily automatic status update versus infrequent, but more thorough, manual status reviews
iv. Challenges and opportunities associated with the use of condition monitoring data
v. Digital vulnerabilities in the control and safety systems of the facilities, with emphasis on integration of existing IT and OT, as well as new enabling technologies such as 5G, Internet of Things (IoT) and big data

In this paper, we focus on the first and the last of these issues.

4.1 Differences in time span between a failure is identified until it is recorded and displayed in the barrier panel

A particularly interesting question, based on the answers to the questionnaires and the dialogue meetings with the selected companies are: How quickly after the barrier impairment is identified, is it recorded in the barrier panel?

Section 5 of the Management Regulations on Barriers (PSA, 2019) states, among other things, that "It must be known which barriers and barrier elements are not functioning or are impaired." This can be interpreted as knowing the condition of the barriers at all times. Thus, a detected barrier failure (or malfunction) should be made visible in the barrier panel immediately or "as soon as possible".

The companies' barrier panels primarily collect information from the maintenance system in the form of corrective notifications/work orders and overdue preventive work orders for barrier tags. The questionnaires and discussions with the six companies clearly show varying practices for when the barrier impairments are registered in the panel. Some companies collect registered notifications (with specified codes) for barrier tags immediately upon registration, some pending until the notification has been given a certain status (e.g. approved), while others wait until the deadline for the execution of the corrective job has expired, i.e. the CM is overdue.

With reference to Section 5 of the Management Regulations (PSA, 2019), it is reasonable to question the latter practice. This practice implies that a barrier tag that is impaired does not enter the barrier panel until a certain number of days (typically three to five) after the fault is discovered. The argument for such a practice may be that new impairments will nevertheless be captured in the maintenance system and will be addressed in daily work permit meetings. However, it can be questioned whether this status is "known to everyone" as the companies themselves claim. Furthermore, one may argue that the panel will provide an incomplete picture of all barrier failures if corrective work is only shown as impairments in the barrier panel when the corrective work is overdue (have exceeded the deadline).

4.2 Digital vulnerabilities in the control and safety systems of the facilities

During the dialogue meetings, several people expressed great concern about new digital vulnerabilities in general, and to a greater extent than the answers in the questionnaires might indicate. The latter was probably due to the specific link to the barrier panel and the condition monitoring system in the questionnaire, which most companies were less concerned about with respect to digital vulnerabilities. Further work should therefore look more closely at digital vulnerabilities associated with all new (and existing) digital solutions, not specifically limited to barrier panel and condition monitoring system.

A related example is the control and safety systems on the facilities, as well as the systems that will ensure good technical condition. In general, this can also cover the positive aspects of digitalization, i.e. how digitalization improves technical condition and safety. In order to limit the scope of the discussion, the following relevant issues have been identified: Digital vulnerabilities in the control and safety systems of the facilities, with emphasis on integrating existing IT and OT, as well as new enabling technologies such as 5G, IoT and big data.

IT/OT integration is about technological inequalities and different concepts, but also about languages, cultural assumptions and priorities. Within the IT world, a recognition has emerged that preventing all intrusions is unrealistic, that unknown extraneous elements are likely to be present, and that effective incident management and rapid updating must therefore be emphasized to a greater extent, in addition to implementing barriers against intrusion. Within the OT domain where concepts such as plant integrity are emphasized, both technological and organizational objections can be raised against a similar consequence-reducing focus. For example, unplanned complete shutdowns for rapid updating motivated by a cyber event or vulnerability may not be practically possible or desirable for continuous process control or to ensure the safety function of the process. It may e.g. be advisable with a gradual controlled shutdown. A relatively radical but less flexible solution for securing process control systems against intrusion can be so-called information diodes.

In the past one had to explain thoroughly the meaning of terms such as "Secure Safety" (Grøtan et al., 2007), whereas today it is self-explanatory that safety systems with external communication over Internet Protocol (IP) networks represent serious challenges. The industry should actively engage in standardization activities that unite the various domains, but also help to highlight good practices that utilize and promote human and organizational resilience in terms of management of surprises and disruptions.

However, the challenges include more than preventing intrusions and other unwanted interventions with the computer systems themselves. It must be expected that technologies that have been developed and actors using them to map, describe and influence individuals and groups in a targeted manner, through big data and machine learning in the business-to-consumer (B2C) domain, will also spur corresponding mapping and optimization initiatives in an industrial context. This may also affect the petroleum industry.

Hence, while condition monitoring, optimization and predictive maintenance can be the positive outlook and objectives that entail external knowledge of operational conditions and (safety-relevant) vulnerabilities, the very same knowledge can be abused and even weaponized. The industry should develop an appropriate understanding and preparedness for such future challenges in terms of emerging vulnerabilities related to integration of e.g. 5G and IoT technologies, and proper security measures.

4.3 Conclusions

In the study presented in this paper, six selected oil and gas companies responded to a questionnaire on providing information on barrier condition and risk, condition monitoring of early failure development and digital vulnerabilities, as well as participating in half-day dialogue meetings to present, elaborate and discuss the responses.

The petroleum industry has increasingly made information on the technical condition of safety-critical functions and equipment - barriers - available through the visualization of impairments of these barriers in a barrier panel with associated visualization tools. This frequent (daily) updating of the status of the barriers is mainly based on maintenance data such as outstanding CM and overdue PM retrieved from the maintenance management system. Only exceptionally, other types of information about impairments are included in some companies' barrier panels. Barrier status along with other information (events, activities, etc.) are also used to provide risk status information.

Due to the need for frequent updates of the status of the barrier condition, it is desirable to automatically obtain data, and whenever possible, the data should be based on automatic detection of the impairments. Condition monitoring of early failure development is also largely based on automatic detection, and both the barrier panel and the condition monitoring system represent digital solutions that can provide possibilities for digital vulnerabilities affecting safety.

Acknowledgement

The contribution is based on the agreement no. 06618 – 01-2019 – 992704 supporting the work on the maintenance, technical condition and digital solutions project provided by the Petroleum Safety Authority (PSA) Norway. This support is gratefully acknowledged. The contribution from Per Schjølberg, NTNU, is also greatly appreciated.

References

DNV GL (2019). Digitization in maintenance management and application in analysis. DNV GL, 2018-1250. In Norwegian.

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

Edwin, N.J., L. Fornes, and K. Øien (2019). Improved safety in the Arctic through digitalization. The European Safety and Reliability Conference (ESREL 2019), 22-26 September 2019, Hannover, Germany. ISBN: 978-981-11-2724-3.

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).

Gressgård, L.J., K. Melberg, M. Risdal, J. Tømmerås Selvik, and R. Østgaard Skotnes (2018). Digitization in the petroleum industry: Development trends, knowledge and proposed measures. IRIS report - 2018/001. In Norwegian.

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).

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

Kilskar, S.S., K. Øien, S. Hauge, Å.S. Hoem, and L. Bodsberg (2016). Monitoring of operational and organizational safety barriers. The European Safety and Reliability Conference (ESREL 2016), 25-29 September 2016, Glasgow, Scotland.

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

PSA (2019). The Management Regulations; Regulations Relating to Management and the Duty to Provide Information in the Petroleum Activities and at Certain Onshore Facilities, https://www.ptil.no/en/regulations/all-acts/, April 26, 2019.

NSOAF (2018). NSOAF Summary Report Multinational Report - "Maintaining Safe Operations". https://www.ptil.no/contentassets/19d854a23c3741959d4b761ad3ed2d6e/nsoaf-summary-report-multinational-audit-wo-national-reports-for-publishing---final-0021.pdf

Robertson, J. and M. Riley (2014). Mysterious '08 Turkey pipeline blast opened new cyberwar. Bloomberg. https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar (accessed on January 1, 2020).

Øien, K. and S. Hauge (2014). Maintenance within barrier management. SINTEF A26001 (ISBN 978-82-14-05676-1). In Norwegian.

Øien, K., S. Hauge, T.O. Grøtan, and P. Schjølberg (2019). Follow-up of key safety functions and associated digital vulnerabilities. SINTEF 2019:00966 (ISBN 978-82-14-06368-4). In Norwegian.

Øien, K., S. Hauge, P. Schjølberg, and Å. Snilstveit Hoem (2017). Maintenance management – status and improvements, SINTEF A27980 (ISBN 978-82-14-06188-8). In Norwegian.

Øien, K., S. Sklet, S. Hauge, and P. Schjølberg (2018). Actors' condition assessment, maintenance and follow-up of safety-critical functions and equipment. SINTEF 2018:01086 (ISBN 978-82-14-06859-7). In Norwegian.