2021:00056 - Open

Report

Use of models in drilling

ICT security – Robustness in the petroleum sector 2020

Author(s)
Maria Vatshaug Ottermo, Knut Steinar Bjørkevoll, Tor Onshus

SINTEF Digital
2021-01-28

SINTEF Digital
Postal address:
Postboks 4760 Torgarden
7465 Trondheim
Switchboard: 40005100

info@sintef.no

Register of Business Enterprises:
NO 919 303 808 MVA

Report

Use of models in drilling

ICT security – Robustness in the petroleum sector 2020

KEY WORDS:
Models
Model-controlled operation
Drilling
OT system
IT system
ICT security

VERSION	DATE
1.0	2021-01-28

AUTHOR(S)
Maria Vatshaug Ottermo, Tor Onshus, Knut Steinar Bjørkevoll

CLIENT(S)	CLIENT'S REF.
Petroleumstilsynet	Arne Halvor Embergsrud

PROJECT NO.	NUMBER OF PAGES AND APPENDICES:
102022556	43+ appendices

SUMMARY
The purpose of this report is to discuss challenges and opportunities associated with the use of model-controlled operations, particularly relating to how the models and data from the models can be used securely and how ICT security is safeguarded. The main focus is on drilling operations.

This report is one of six SINTEF reports from the project entitled: “ICT security – Robustness in the petroleum sector 2020”. The project has collated knowledge relating to risks, vulnerabilities and ICT security for industrial ICT systems.

PREPARED BY	SIGNATURE
Maria Vatshaug Ottermo	

CHECKED BY	SIGNATURE
Lars Bodsberg	

APPROVED BY	SIGNATURE
Maria Bartnes	

REPORT NO.	ISBN	CLASSIFICATION	CLASSIFICATION THIS PAGE
2021:00056	978-82-14-06480-3	Open	Open

History

VERSION	DATE	VERSION DESCRIPTION
1.0	29.01.2020	Final report

Image crediting:
Page 1: Equinor (drilling)
Page 23: Wikipedia (Scrum)
Other images: Pixabay

SINTEF

Contents

Summary

Introduction

The purpose of this report is to discuss challenges and opportunities associated with the use of models to control drilling operations, particularly relating to how the models and data from the models can be used securely and how ICT security is safeguarded.

This work was primarily based on a document review, interviews and working meetings. Interviews were conducted with oil companies, drilling companies and drilling vendors.

Opportunities and challenges associated with the use of model-controlled operations

Models are actively used in both the planning and execution of drilling operations, and it is clear that an increase in the use of models and digitalisation will facilitate optimisation and better control of the drilling process. Traditionally, there are many manual processes associated with a drilling operation, both for the purpose of direct control and for the input of values into the system. Experience has shown that these manual processes represent an error source which can be either partially or completely eliminated through the use of digitalisation.

Some of the opportunities and benefits of model-controlled operations that are highlighted may also present challenges. For example, there is a risk that the user's mental model and understanding of the process is impaired, or that the user loses focus because he or she is accustomed to the system handling the situation automatically. Over time, this could cause the user to become unable to intervene in the event of an incident. High-quality data is essential when using models, and it is important to be aware that models can only provide a limited picture of reality. There are often many parties involved in the development and use of models, and good communication both between the systems and between the people who develop, operate and use them is essential to ensure that the operations and models work as intended.

Secure use of data from model-controlled operations

Data constitutes the very foundation of a digital society, and must be both correct and of high quality in order to achieve the desired effects. This also applies to models, where a general rule is that bad data in results in bad data out (“garbage in, garbage out”). Models may be more vulnerable to errors in input data because operators are often capable of handling unexpected situations better than a model.

Model-based solutions have to deal with many different sources of data. It is therefore important that the data sources to be used in a model are clearly defined and delineated. There is still enormous untapped potential in reliable and robust sensor technology, as well as high-frequency communication to and from the lower section of the drill string. Provision must therefore be made to process and compile this data in a sensible manner as soon as it becomes available. It is also important to be aware who has access to process and make changes to the data, regardless of whether those involved have good or bad intentions. Experience has shown that fragmented data storage by different participants has led to challenges relating to data access and quality assurance. Data confidentiality can also make it difficult for developers to test their models satisfactorily.

Suggestions regards improvements relating to the safe use of data for model-controlled operations include the quality assurance of data both in and out of the models, good control over who has access to data, the provision of compatible data formats for easy sharing between applications, and a willingness to share appropriate data to ensure that models can be tested satisfactorily.

Safe use of models for model-controlled operations

No model will ever be able to fully reflect reality. There will always be a trade-off between the complexity of the model on the one hand, and performance requirements on the other. To ensure that a model works as

intended, it must be tested, verified and validated. The most challenging aspect of testing a model will often be anticipating the possible scenarios to which the model may be exposed, especially in the case of dynamic models. During the interviews, no reference was made to special standards or guidelines concerning the development and testing of models, but the use of such aids could lead to better quality. Lack of training was highlighted in interviews as one of the biggest challenges to managing the transition to new systems. For a driller who will perform important monitoring and/or control tasks linked to the models, it will therefore be necessary to ensure that the systems support him or her, rather than create uncertainty, frustration and/or a sense of disempowerment.

There is no common communication standard for drilling equipment, which makes it even more challenging to develop solutions which can communicate with existing equipment and drilling systems.

Suggestions for improvements include establishing a common communication standard for drilling equipment, having well-defined model constraints, following a tried and tested method of software development where all parties involved are represented, ensuring appropriate procedures in connection with updates, and having a carefully considered plan for training and the roll-out of new technology. It should be noted that there is no standard/methodology for developing applications for use in critical processes, and it is recommended that work to establish such a standard/methodology be initiated.

ICT security in connection with the use of model-controlled operations

When sensors, systems and machines are connected together to enable information flow, communication and remote control across geographic locations, it also opens up the possibility of unauthorised persons gaining access to sensitive information or interfering with critical functions from anywhere in the world. Having more participants with access to critical production systems will increase the potential exposure to malware. In order to have a complete view of the potential for both unintentional and targeted attacks on a facility or data centre, it is important to identify all possible information and communication channels, both between and within the various levels of IT and OT. As soon as the potential attack surfaces have been identified, it will be easier to segregate, monitor and protect them. However, this can also bring with it vulnerabilities, because attack surfaces are becoming better known and standardised, which in turn can make it easier to organise targeted attacks.

Suggestions for improvements include a structured approach to threat picture mapping and the identification of vulnerabilities. The available frameworks and methodologies can seem overwhelming and unnecessarily complicated, and developing a more practical approach to ICT vulnerability analysis could be helpful.

Recommendations

A total of 13 proposals for measures have been made for the industry, while six recommendations for action have been made for the Petroleum Safety Authority Norway.

We believe there is a need to learn more about how meaningful human control can be facilitated as models become more complex and more reliant on cognitive technologies, rather than physical models. We also see a need to bring in more knowledge on how to combine domain knowledge and physics-based models with machine learning in order to improve security and reduce costs. It is also apparent that there will be a need for more knowledge relating to the management of ICT incidents in connection with the use of model-controlled operations, as regards the competence of technical personnel and knowledge concerning how to drill and prepare employees and the organisation itself for such incidents. While working on this report, it also became apparent that it would be desirable to establish specific recommendations for a framework which can be used, or a guide which makes it easier to adopt existing standards for development and ICT vulnerability analyses of models.

Executive summary

Introduction

The purpose of this report is to investigate challenges and opportunities related to use of models in drilling operations, with emphasis on how the models and data from the models can be used in a safe way, both in a safety and ICT security perspective.

The work is based on document reviews, interviews and working sessions with the industry. Interviews have been conducted with selected oil- and drilling companies and drilling contractors.

Challenges and opportunities related to use of models in drilling operations

Models are used actively both during planning and execution of drilling operations, and the increasing use of models and digitalization enables new ways of optimizing and controlling the drilling process. Traditionally, drilling operations are associated with many manual operations both for direct control and data input to the system. Based on experience, these manual processes are a frequent source of error, that can be partly or fully eliminated by using digital solutions.

Some of the opportunities and benefits associated with use of model-based control can also result in new challenges. For instance, there is a risk that the user's mental model, situational awareness, focus or understanding of the process is impaired because the system usually handles and controls the situation and demands no input from the user. Over time this can result in a situation where the user is unable to intervene should an incident occur. Models are dependent on good quality data. At the same time, it is important to point out that models can only provide a limited approximation of reality. Several stakeholders are often involved in development and use of models; hence it is important to enable efficient communication and interaction both between systems and between people to ensure that the operations and models are run as intended.

Safe and secure use of data from model-controlled operations

Data is the foundation of a digital society, and it must be accurate and of high quality to obtain the desired benefits. This also applies to models, where a common rule is that garbage in results in garbage out. Models can also be more vulnerable to errors in input data, since a human operator often will be better suited to handle unexpected situations than a model.

Model-based solutions often rely on different data sources; hence it is important that data sources are well defined and delimited. There is still a large unexploited potential in reliable and robust sensor technology as well as high-frequency communication to and from the lower part of the drill string, and preparations should be done to be able to process and compile this data in a sensible way as soon as they become available. It is also important to control who has access to processing and making changes to the data material, regardless of whether those involved have good or bad intentions. Fragmented data storage by various actors has, from experience, led to challenges related to data access and quality assurance of data. Data concealment can also make it difficult for developers to test the models satisfactorily.

Suggestions for improvements related to safe and secure use of data for model-controlled operations include quality checks of data both to and from of the models, access control, ensuring compatible data formats for easy sharing between applications, and willingness to share relevant data to ensure that the models can be thoroughly tested.

Safe use of models for model-controlled operations

A model will never be able to fully reflect reality. There will always be a trade-off between the complexity of the model on the one hand and performance requirements on the other. To ensure that the models work as intended, they must be tested, verified, and validated. The most challenging part of testing the models will

often be to foresee possible scenarios the models may be exposed to, especially for dynamic models. No specific standards or guidelines for development and testing of models were mentioned in the interviews, but the use of such aids can provide better quality. Lack of education and training was highlighted in interviews as one of the biggest challenges in dealing with the transition to new systems. The driller will have an important monitoring and/or control function related to the models, and it is important to ensure that the systems provide support to the driller rather than introducing uncertainty, frustration and/or a feeling of being incapacitated.

There is no common communication standard for drilling equipment, and this makes it more challenging to develop solutions that can communicate with existing equipment and drilling systems.

Suggestions for improvements include establishing a common communication standard for drilling equipment, ensuring well-defined model limitations, following a proven method for software development where all involved parties are represented, ensuring good procedures for updating the models and establishing plans for training, education, and rollout of new technology. Note that no standard/method adapted to design of applications used in critical processes is available, and it is recommended to work towards establishing this.

ICT-security for model-controlled operations

When sensors, systems and machines are connected to enable information flow, communication, and remote control across geographical locations, it makes it easier for unauthorized persons to access sensitive information or target critical functions from anywhere in the world. More stakeholders with access to critical production systems will increase exposure to malware intrusion. To have a full overview of the possibilities for both unintentional and targeted attacks on an installation or a data centre, it is important to identify all possible information and communication channels between the various levels within IT and OT and between IT and OT. Once the possible attack surfaces have been identified, it will be easier to segregate, monitor and protect them. However, standardizing the attack surfaces, will also make them more exposed to targeted attacks.

Suggestions for improvements include working in a structured way to map the threat picture and identify vulnerabilities. Available frameworks and methodologies can seem overwhelming and unnecessarily complicated and establishing a more practical approach to ICT vulnerability analysis could be useful.

Recommendations

Thirteen suggested measures for the industry have been identified, while 6 recommendations have been suggested to the Petroleum Safety Authority Norway.

We see a need to gain more knowledge about how to enable meaningful human control when models become more complex and to a greater extent are based on cognitive technologies rather than physical models. We also see a need to gather more information about how domain knowledge and physics-based models be combined with machine learning to increase security and reduce costs. There is also a need to identify ways of handling possible ICT incidents related to the use of model-controlled operations, both in terms of competence among professionals and knowledge about how to train and prepare employees and the organization for such incidents. While working on this report, it was identified that there is a need for specific framework recommendations that can be used or a guide that makes it easier to apply existing standards while developing and performing ICT vulnerability analyses of models.

1 Introduction

1.1 Background

The Petroleum Safety Authority Norway has commissioned SINTEF to investigate various aspects of the topic of ICT security — robustness in the petroleum sector. The project has collated knowledge relating to risks, vulnerabilities and ICT security for industrial ICT systems. The aim of the project was to improve the understanding of ICT security in the petroleum industry and thereby increase the industry's resilience against undesirable incidents. SINTEF has also provided input for updating the Petroleum Safety Authority Norway's regulatory framework for monitoring ICT security.

The following is a brief description of the six subprojects:

Data quality

The aim was to examine which data sources and data are used in industrial ICT systems and how data is handled and processed prior to being made available in the office network. Strengths and vulnerabilities relating to data quality and the protection of data are discussed.

Memorandum – ICT security in the petroleum industry

SINTEF has prepared a memorandum to clarify how ICT security in the petroleum industry is regulated by applicable regulations. The memorandum shows the extent of systems which are typically covered by industrial ICT systems and which directly support the operation of facilities and mobile rigs.

Guidelines for ICT security

Guidelines have been prepared for the Norwegian petroleum industry to supplement the core ICT security principles set out by the Norwegian National Security Authority (NSM). The guidelines are tailored to the solutions typically employed in the petroleum sector, while retaining the flexibility to address the key elements of the petroleum industry's ambitions for digitalisation.

Model-controlled operation - *this report*

The report summarises knowledge and recommendations concerning the secure use of model-controlled drilling operations. A special emphasis is given to the quality assurance of models and data therefrom, as well as ICT security and communications between software solutions in drilling operations.

Principles of digitalisation and IT-OT integration

The purpose was to describe and assess how digitalisation and the use of cloud services affect industrial ICT systems, and the security solutions that need to be implemented to ensure secure use of cloud services. The Petroleum Safety Authority Norway's regulations are particularly built on a pillar of segregation and independence as strategies for establishing safety and security.

Communication networks

The aim was to investigate external communications roles that data networks can provide in the event of hazard and accident situations. The report describes challenges involved in the risks and vulnerabilities of data networks and makes specific recommendations for improvements.

This project forms part of a wider ICT security initiative being carried out by the Petroleum Safety Authority Norway (PSA). Key issues for the PSA include:
How does the industry manage change processes relating to the introduction of new technology?

- How will digitalisation impact HSE conditions and risk management?

SINTEF's work on this project is largely a continuation of previous projects carried out by DNV GL and SINTEF within the same thematic area [7])

1.2 Objectives and purpose

The main objective of this delivery is to provide the industry with a greater understanding of the challenges and opportunities associated with using model-controlled operations, particularly as regards how models can be used safely and how ICT security is addressed.

The following objectives are defined:

1. Consider the challenges/opportunities associated with model-based solutions. Specific emphasis is placed on drilling operations.
2. Describe and evaluate how data from model-controlled operations can be used safely.
3. Describe and evaluate the quality assurance of models.
4. Describe and assess ICT security in connection with the use of model-based solutions.
5. Propose measures for the safe use of model-based solutions (for both ICT and HSE).

1.3 Limitations

- Emphasis has been placed on current solutions for model-controlled operation, rather than emerging trends.

- By ‘model-based solutions’, we mean solutions where models and data are included in order to describe all or certain aspects of the equipment and process. They can be used offline for testing equipment and processes, for planning or for training purposes prior to an operation or the next step in an operation. The models can also be used in real-time during an operation with a direct link to the control systems that are controlling the drilling operation.

- Here, models are limited to mathematical process models which calculate (multi-phase) flow, pressure and temperature in the well, as well as forces and elastic effects in the drill string. Well stability may be included, but for model-based control, the input of tables which provide pressure constraints may be sufficient. We have therefore excluded, inter alia, physical models and mathematical models for structural computations.

- Applications may include planning, training, real-time decision support, automation and post-analysis/experience transfer. Variants of the same mathematical models are often included. Computations in all the phases may be of relevance to the extent that they either directly or indirectly help to control the operation.

- In the interests of anonymisation, documents shared by the various companies that were interviewed are not included as references.

1.4 Terms, definitions and abbreviations

1.4.1 Terms and definitions

Term	Definition/description	Reference
Barriers*	Measures intended to prevent a specific sequence of events from occurring or to guide such a course in a specific direction to limit damage and/or loss. The function of such barriers is ensured by technical, operational and organisational elements, both individually and collectively.	PSA 2020 (ptil.no) [8]
Bit	Drill bit	
Driller	Norwegian: borer	
ICT security	Protection of information and communications technology (hardware and software, as well as communication systems).	SINTEF 2018:00572 [9]
Information Technology (IT)	Technology which processes information.	This project
Operational Technology (OT)	Technology which supports, controls and monitors industrial production, control and safety functions.	This project
Operational envelope	Norwegian: Operasjonsområde	
First principles	Model based largely on physical laws and system information, rather than on empiricism or parameter adaptation.	
Patching	Process for fixing a vulnerability or bug in software.	
Risk (1) **	'Risk' means the consequences of the activity and its associated uncertainty.	Guidelines to Section 11 of the Framework Regulations [10]
Risk (2) **	Risk can be expressed as a combination of the probability and consequence of an undesirable incident.	NS 5814:2008 [11]
Risk (3) **	Risk can be expressed as the relationship between the threat to a given asset and this asset's vulnerability to the specified threat.	NS 5832:2014 [12]
Vulnerability (1)	The inability of an analysis object to withstand the effects of an undesirable incident and to restore to its original state or function following an incident.	NS 5814:2008 [11]
Vulnerability (2)	An expression of the problems that a system experiences in operating when exposed to an undesirable incident, and the problems that the system experiences in resuming its activities after the incident has occurred.	NOU2015: 13 [13]

*) The term "barrier" is rarely used in ICT security standards. Instead, terms such as measures, countermeasures, defence mechanisms, protective mechanisms, solutions etc. are used.

**) Risk (1) is an example of a qualitative definition of risk, while risk (2) and risk (3) are examples of definitions for describing risk; see [14].

1.4.2 Abbreviations

Abbreviation	English	Norwegian

1.5 Methodology and implementation

This work was primarily based on a document review, interviews and working meetings. It was carried out by a multidisciplinary project team with expertise in instrumented safety systems, ICT security, drilling and well operations, as well as petroleum regulations and standards within these disciplines.

Interviews were conducted with oil companies, drilling companies and drilling vendors. The names of the companies have not been disclosed to preserve their anonymity.

Seven group interviews were conducted with a total of 20 interviewees.

1.6 Report structure

Chapter 2 describes the role that model-controlled solutions play in drilling operations, with an emphasis on current technology. Examples of the use of model-controlled solutions that are used in both the planning phase and operations are highlighted. Opportunities and challenges associated with the use of model-controlled operations are also discussed.

Chapter 3 deals with the safe use of data from model-controlled operations and what processes are used to secure and protect data used in the models.

Chapter 4 takes a closer look at the quality assurance of models.

Chapter 5 deals with ICT security in connection with the use of model-controlled operations and looks at data flow between systems and software solutions, amongst other things.

Chapter 6 briefly summarises implications for production optimisation.

Chapter 7 summarises SINTEF's recommended measures for the industry and the Petroleum Safety Authority Norway, as well as the need for further work on knowledge acquisition and subsequent work.

In addition to figures and tables, we use fact boxes (green boxes on the left-hand side of the page) and result boxes (blue boxes on the right-hand side of the page). The same colours are used for tables, i.e. result tables are blue.

2 Scope and general use of model-controlled operation

At present, approximately 50% of the cost of field development is linked to drilling and well operations. In addition, drilling always entails risk, and failure can have enormous consequences for equipment, people, the environment and the organisation. There is broad agreement that both costs and risks can be mitigated through the widespread use of digitalisation to optimise the drilling process.

NTNU, 2016 [3]

Godhavn, 2011 [6]

The drilling process is often associated with high costs, fragmented work operations involving many parties and interfaces, and considerable uncertainty relating to underground conditions. At present, approximately 50% of the cost of field development is linked to drilling and well operations [3]. In addition, drilling always entails risk, and failure can have enormous consequences for equipment, people, the environment and the organisation [6]. There is broad agreement that some of these costs and the risk of failure can be reduced through greater automation of drilling operations, using both robotisation and the more widespread use of digitalisation to optimise the drilling process. To achieve this, greater use of models and better use of available data from sensors will be key.

In recent decades, increasingly sophisticated drilling solutions have been introduced, not only for decision support and monitoring, but also for direct control. The models are generally implemented in IT systems which are closely linked to OT systems, and examples of models which have a direct link to the control systems that control the drilling operation have been introduced over time.

2.1 Current status of the use of model-controlled operations

The purpose of this section is to review the status of use of model-controlled operations on the Norwegian shelf, with a particular focus on drilling operations. During the interviews conducted for this study, the companies noted that they use anything from a few to just over 20 models in their drilling operations. Some are offline, while others are in operation, linked either directly or via operators as advisory information.

The use of models varies in the industry. Anything from a few to over 20 are currently in use by the companies that were interviewed, although each company often owns a few of them. This leads to many fragmented models which could potentially impact on the process and it can be difficult to maintain an

Models have a wide variety of applications in drilling operations, but they can roughly be divided into the following main categories:

- Planning phase, including personnel training
- Operating phase.

Some models are also used in both phases. Because drilling operations are complex, it is unrealistic to model and simulate every aspect of the process, but extensive research and development is under way in many areas. In the past, it has been challenging to run such models in real time, but over time methods have been developed to reduce the complexity of the models, while computing power has increased. This has now made it possible to model with a greater degree of detail and accuracy. Drilling a functioning well requires the use of a wide variety of equipment, including a rig, drill pipes, bottomhole assembly (BHA), casings, risers, pumps, hoist system, top drive, pipe racking machinery, valves, degasser, tanks and processing systems for drilling mud and cuttings. In addition to the physical systems, many people are also involved in the process.

2.1.1 Use of models during the planning phase

Drilling Modelling and Simulation (DMS) deals with modelling and simulating the behaviour of the drilling system and process, and aims to provide important information about these without actually constructing the well [15]. The aim of using DMS methods is to contribute to improved drilling efficiency, productivity and performance, as well as improve risk management and thus enhance personal safety.

Various drilling simulators have been developed, including for planning and optimisation and the 3D simulation of equipment and the drilling process. These simulators have shown promising results, but many have been inaccurate or incomplete, especially if they have been based exclusively on virtual mathematical models. Simulations based on physical models are often limited to part of a system or scaled down to save costs or space or for safety reasons. It has therefore become more common to use hybrid models, where mathematical models are used for the parts of the process that can be described accurately mathematically, while a full-scale physical model is used where this is not possible [15]. For example, many models are available for analysing the dynamics of the drill string, but there are only a few, inaccurate models of the drill bit and drill rate (ROP). It is therefore natural to simulate the drill string, borehole and drilling rig using virtual models, but to use a physical model for the interaction between the drill bit and the formation [15].

In addition to the fact that the mathematical models discussed above are used individually, more extensive use appears to be being made of digital twins, where several models are integrated, and more data on the physical properties of the process is utilised. A digital twin can be defined as “a digital profile of the historical and

current behaviour of a physical object or process" [16]. Such twins appear to be useful in a number of phases of the process, including planning, training, operation and the retrospective analysis of events.

2.1.2 Use of models during the operational phase

In recent years, considerable progress has been made on the Norwegian shelf in the automation of drilling equipment on the drill floor, partly through the robotisation of top drives, draw works and ties, combined with the automation of pumps and valves. Good experience has been built up of dynamic planning, automated pipe racking and anti-collision. One particular challenge has been to utilise this experience to also automate aspects of the well construction process, for example by using real-time measurements from the borehole to calibrate the mathematical models that are used to predict borehole parameters. Achieving this will require a range of advanced tools and disciplines, including optimised drilling, dynamic monitoring, path planning, and automated control of forces, pressures and vibrations using models and simulators [15].

A number of dynamic real-time models have been developed for drilling operations. These are based on the use of mathematical computations which estimate the expected response, and are compared with real-time measurements from instrumented drill strings or other sensor systems, and used as a basis for real-time decision support and alarm generation. Because the data being entered in the models is incomplete and/or inaccurate, it is important to determine the cause of any discrepancies between the model's computations and physical measurements. If anomalies in the physical system, including sensors and data transmission, can be excluded, the models are calibrated to correct for inaccuracies in input data and computations. Applications include real-time decision support for maximum drilling and tripping speeds, automation of drilling machinery and pumps, automated pressure control during managed pressure drilling (MPD), and the automated processing of drilling mud on the rig.

MPD is an adaptive drilling process which is used when the reservoir pressure is low and the formation strength has been weakened [15]. An important part of an MPD control system is a hydraulic model, which is often the part of the system that limits the accuracy that is achieved. There are therefore many complex and good hydraulic models, but the drawback of them is that they require specialist expertise for both setup and calibration. In practice, it is apparent that much of the complexity does not contribute very much to greater accuracy, because the condition of the well is changing and insufficient measurements are available to calibrate the model parameters during the process. It has been demonstrated that, using a simplified model, it is possible to estimate the dominant characteristics of an MPD system and that, using online parameter estimation for automatic calibration, a level of accuracy can be achieved which is as good as that achieved with more advanced models, provided sensors and data transmission are intact [17].

Parallel to this, work is under way on smarter models which are more robust and less dependent on specialist expertise in operation than existing advanced models. These can improve the capacity to interpret data and thus detect and manage sensor errors and non-conformant status in the well. They can also handle uncertainty in a systematic and consistent manner.

In one example of autonomous drilling which is in use on the Norwegian shelf, real-time updates from the rig and BHA are sent to a digital twin of the borehole. The set-points for optimal drilling and tripping speeds are continuously calculated in the model and updated automatically. The driller is kept updated on these changes, and given the opportunity to make adjustments or intervene if necessary. In addition, the operational envelope for all controllers is updated automatically based on their position in the operation.

The visualisation and interpretation of data is important in order to integrate measurements from the well with other processes. Advanced technologies, such as electromagnetic transmission and telemetry systems, have created the possibility of extracting large quantities of data in real time. With further development, it is

anticipated that real-time optimisation and automation can be done at the drill bit. This will offer opportunities for better design, monitoring and optimisation of the drilling process, as well as a higher degree of autonomy.

2.2 Overview of specific models and applications

This overview briefly describes a number of commonly used models. Most of these are used in planning and some are also used in real time, with the direct input of data from the drilling system. In such cases, specific real-time versions of the models are normally used which have been developed to work optimally and reliably with the direct input of sensor data.

2.2.1 Thermohydraulic models

Models which calculate the flow of drilling mud and other liquids during drilling and completion are pivotal to, amongst other things, the safe and optimal control of the pressure in the well, to ensure good hole cleaning, and to plan the safe management of adverse events, such as reservoir fluid inflow or loss to the formation. Such models are therefore always used during the planning process to ensure that the pressure in the open hole is kept within the constraints imposed by pore pressure, collapse pressure and fracture pressure with a satisfactory safety margin. The pressure is the sum of hydrostatic pressure, frictional pressure losses, local pressure losses and back pressure from surface valves, minus the lifting assistance from any pumps in the annulus or in the sea outside the riser. Each of these links in the chain is dependent on the temperature profile of the well, which is therefore included either as input from an external source or by using an integrated model for calculating the temperature along the well. Dynamic variations in the temperature profile are also of importance and are therefore included in advanced temperature models.

Thermohydraulic models are also used in real time for decision support and for the automation of sub-operations, such as calculating the maximum safe velocity at which the drill string can be withdrawn from the hole or re-entered in order to continue drilling and giving the result as a frequently updated set-point to the drilling control system.

2.2.2 Mechanical models for the drill string

Advanced mechanical models are used in planning to ensure that the string is sufficiently strong to withstand torque and axial forces during relevant phases of the operation. There are also vibration models which can provide a picture of how axial, rotational and lateral vibrations are affected by drilling parameters and fluid properties. Although the accurate determination of vibrations requires the input of sensor data during an operation, the models can provide a useful qualitative understanding of how vibrations can be attenuated by adjusting operational parameters. This can help both to avoid unnecessary wear and damage to the drill string and downhole equipment, and optimise drilling speed (ROP)

In real time, mechanical models can be used in conjunction with sensor data for decision support and automation to further minimise damage and wear, and to indicate that forces are approaching the tolerance limits for the string. Measuring mechanical forces in different directions is also an important indicator of impending problems as a result of poor hole cleaning, and the use of models can help to provide an understanding as to whether changes in measurements are normal or non-conformant.

2.2.3 Cementing models

Models similar to those described in Chapter 2.2.1 are also pivotal to the planning of cementing operations. In this case, the models have to deal with a succession of different fluids with very different characteristics, causing major changes of pressure and temperature during pumping and the injection of cement. Both pressure and temperature are important in achieving a safe and satisfactory outcome. In addition to this are computations relating to the rest of the process, i.e. issues like release of the drill string, the circulation of extra cement outside the drill string, the hydration of cement, and pressure testing.

Automatic control during the pumping and injection of cement is possible and has been done, but this is less common than automation during drilling.

2.2.4 Drilling mud handling

Efforts are being made relating to automated monitoring and management of the drilling mud process. The aim of this is to achieve greater accuracy in controlling the properties of the drilling mud, and reduce the manual handling of drilling muds and additives. The latter has the potential to help reduce HSE-related risk, costs and climate footprint through increased remote monitoring and management. Part of the solution will consist of mathematical models of drilling mud properties and circulation in offshore handling systems. Few rigs are ready for automated drilling mud handling system with all the sensors and actuators that are required, but this is expected to become more commonplace going forward.

2.2.5 Top drive, draw works, pumps and valves

Top drives are automated to varying degrees based on computations using the models described above, amongst other things. For example, models calculate how pump rate, rotational speed and axial string velocity affect fluid pressure and forces in the string, helping to keep these variables within safe margins from given or assumed limit values. The computations can be performed offline before the operation is commenced, or in some cases in real time with direct input from the drilling process. Equipment which is controlled based on such input includes:

- Top drive which rotates the drill string from the top
- Draw works which lift and lower the string
- Ties which hold the string firmly in position when the top drive is disconnected in order to remove or add pipes or other drill string components
- Drilling fluid pumps which circulate liquid down the inside of the drill string, through the drill bit and back up the outside

In many cases, these functions are implemented in specialist modules intended for specific tasks for which they have been thoroughly tested and validated to ensure safe and reliable operation. Examples of this which have been mentioned by the industry include:

- Systems which optimise the drill bit
- Systems which optimise raising and/or lowering of the drill string.

Complex systems for computations in real time are based on developments over decades in various research environments. The results of this development work have now been commercialised by the companies eDralling and Sekal, amongst others, and are used by many oil companies both on the Norwegian shelf and internationally. Both systems calculate dynamic flow, temperature and forces in real time, and compare the results with measurements both for control purposes and to provide decision support during operations. For more details, visit www.edrilling.no and www.sekal.com .

A number of subsystems have also been implemented by various vendors and service companies. One example is a new kick detection algorithm developed by the R&D department of an oil company and integrated into a vendor's software to provide earlier and more reliable information on possible well control events. Another example is software for reducing stick-slip movements, which can cause severe damage. There are several such stick-slip-reducing control algorithms, and they are continually being improved.

2.2.6 Well siting

The optimal siting of wells in oil and gas reservoirs is a challenge when drilling. It involves mapping the subsurface as accurately as possible before drilling, adjusting the map and accurately controlling directional drilling during the drilling process. This requires good models during the planning phase and accurate control and updating during drilling operations.

2.2.7 Link to overarching systems

Operator-controlled systems with elements of automated sequences are widely used in the North Sea, but active work is under way on the digitalisation and integration of different systems, including model computations, in order to avoid duplication and errors in manual input, and to rapidly update plans automatically when the situation changes during the process. When this works well, it is for example possible to achieve automatic updating of the action plan/time planner for operations.

2.3 Other relevant examples of the use of models

Models are also in widespread use in applications other than drilling, and the methods used largely coincide with those which are or can be used in drilling operations:

- An example is Model Predictive Control (MPC), which is currently used for a number of challenging regulatory tasks, such as slug control.
- Dynamic models are also extensively used for analysis in conjunction with construction and optimisation, as well as in training simulators.
- Dynamic models which are synchronised with the process at all times can be used, e.g. to see the effects of certain actions without affecting the physical installation.
- Online models can also be used to obtain insight/measurements which are not available through the measurements that are available for the installation based on computations and available measurements ("virtual sensors").
- The modelling of information in semantic models and the use of information models can also make the linking and use of information easier and more secure.

2.4 Opportunities in connection with the use of model-controlled operations

In 2017, the International Research Institute of Stavanger AS (IRIS, now NORCE) carried out an assignment on behalf of the PSA to summarise and analyse knowledge concerning the positive and negative effects of digitalisation for health, environment and safety in the petroleum industry [18]. The report summarises the findings of a literature search and interviews with industry actors, and one of four digitalisation initiatives in the petroleum industry to be highlighted was the automation of drilling operations. During the interviews, emphasis was placed on the fact that digital models of wells will open up new possibilities linked to the simulation of drilling operations, which can provide useful information regarding the robustness of a drilling operation plan, and offer better opportunities for learning and experience transfer between teams and projects, such as between the driller offshore and experts on land.

One of the main points highlighted during the interviews was the opportunities that models and digitalisation present to optimise and control the drilling process. With the aid of good planning tools and real-time measurements, there is a more scope to optimise operating parameters during the drilling operation itself, and to make necessary adjustments during the process. It is also apparent that the overall control of the operation is improved, as drilling is forced to remain within a given framework. Recent years have seen a trend towards increasing automation of individual functions, such as pipe racking and drilling mud systems. However, it is anticipated that more integrated systems which automate more complex functions will make a greater contribution to greater efficiency and safety. This assumes user-friendly solutions which are not reliant on complex configuration or experts in order to use them. Another important point that was mentioned was the ability to link different systems together in a common user interface (HMI), which will provide a better overall

view. This assumes that the user interfaces are specifically adapted to both operation and user, so that only relevant information is available at any one time.

Traditionally, many manual processes are associated with drilling operations, both for the direct control of downhole equipment and for the inputting of values into the system. In both cases, there is also a risk of operations being based on erroneous underlying data, as a result of a failure to obtain the latest version of the data, for example. By adopting models which do not require manual input, but where data input and version control can be carried out automatically, these possible error sources can be reduced or even eliminated altogether.

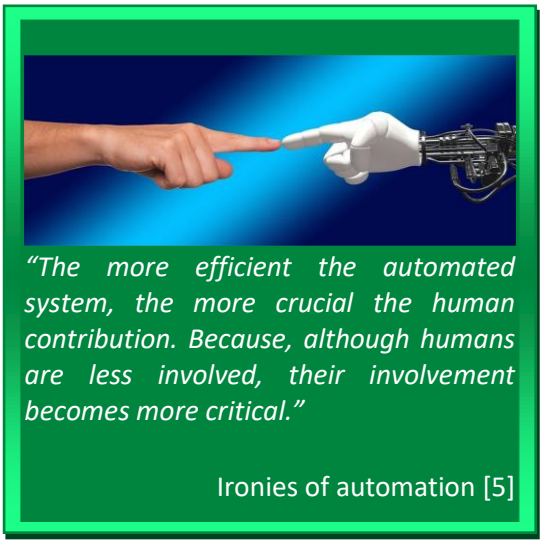
With an increase in the use of models and access to more and better sensors, there are ample opportunities to leverage redundancy to create a safer and better system.

With an increase in the use of models and access to more and better sensors, there are ample opportunities to leverage redundancy to create a safer and better system. For example, the fact that models are able to monitor each other could be exploited, so that an alarm is triggered if one model receives invalid input from another model. On the sensor side, it would also be possible to use a number of different sensors to take the same measurement or measurements which are connected together in order to create redundancy in the measurement and enable erroneous measurements to be detected. The models also present opportunities for estimating values where it is neither possible nor appropriate to take direct measurements using sensors, such as in exposed environments. It is nevertheless important to be aware that having more data sources can be a challenge. This issue is discussed further in Chapter 3.1.

2.5 Challenges associated with the use of model-controlled operations

Some of the opportunities and benefits of model-controlled operations that have been highlighted may also present challenges. For example, there is a risk that, although users of model-based and autonomous systems will initially monitor and make empirical assessments relating to the process in the same way as before, the situation will change over time as the systems become engrained and trust in the system doing things correctly builds up, leading to greater vulnerability in the future. This could represent a risk, because over time it could cause the user to lose the mental model of the process, and thus lose their understanding of the system and render them unable to intervene in the event of an incident. Another danger could be loss of focus caused by users growing accustomed to the system handling the situation, and thus no longer devoting sufficient attention to the process. Hardly any other function has a greater impact on safety functions than the driller, and this can therefore be critical. A third challenge may be that the systems are utilised in a way which enables intended barriers to be removed. An example is the use of what is known as a “floor saver”. This is a back-up system which is normally installed to prevent equipment from hitting the drill floor, but which instead is often used in normal operations and thus removes the human barrier in the system.

Another challenge is the fact that the new models and systems can become so complex that it becomes difficult to keep track of what the systems do and how they are linked together. This applies during both development and operation. During the development process, it can be difficult to see the entirety because, by optimising functions or systems in one place, one can inadvertently affect other aspects of the processes. In addition, during operations, it can be difficult to see and understand the entirety if there are many fragmented and complex models to deal with. Even with a holistic user interface, it can be challenging to sift out only the most important information.



The introduction of more complex systems and models can rapidly lead to the paradox of automation, namely that the more efficient the automated system, the more crucial the human contribution [5]. Because, although humans are less involved in processes, their involvement becomes more critical. Thus, it is apparent that new technology requires specialist expertise and a more holistic approach to MTO, cultural change, user-centred design, meaningful human control, and thorough training programmes. See also [19] for more details.

Good data is essential when using models, and it is important to be aware that models always have limitations and will never be able to provide a complete picture of reality. Even for accurate models with good parameter adaptation, changes in operating conditions and the actual conditions prevailing during the drilling process itself will lead to inaccuracies in the model. Such adaptations are often not adequately taken into account when a model is used.

Figure 1 shows a non-exhaustive record of participants involved in model-controlled operations, from design and development to testing and management. As the figure shows, many parties are involved and have to talk to each other to ensure that the operation proceeds in a satisfactory and safe manner. In addition, there may be uncertainties linked to contractual relationships and ownership of the model which impact on whether or not such a project becomes a success, partly because it has implications as regards the (lack of) sharing of data. This represents an important challenge, not only for model-controlled operations, but also in connection with the introduction of all new technologies and work processes. The actual work processes relating to the systems will be the responsibility of the rig owner and operator. During the development process, all the parties involved should be brought together to exchange information and think collectively. One challenge that was highlighted during the interviews is that vendors compete against each other, and this can reduce the amount of interest they have in sharing challenges with each other. In the worst case scenario, this could delay the dissemination of best practice and impair the ability to manage non-conformities. Working with a single responsible vendor can also be an essential prerequisite for success in project work; see [19] for more discussion of this topic.

Overall, it is evident that the introduction of new technologies can also lead to the introduction of new vulnerabilities. However, it is necessary to also be aware that drilling operations using conventional solutions, where systems are operated right up to the tolerance limit, can often be more dangerous. This is because the new technology adds new barriers or improves existing ones, and can therefore help to improve safety.

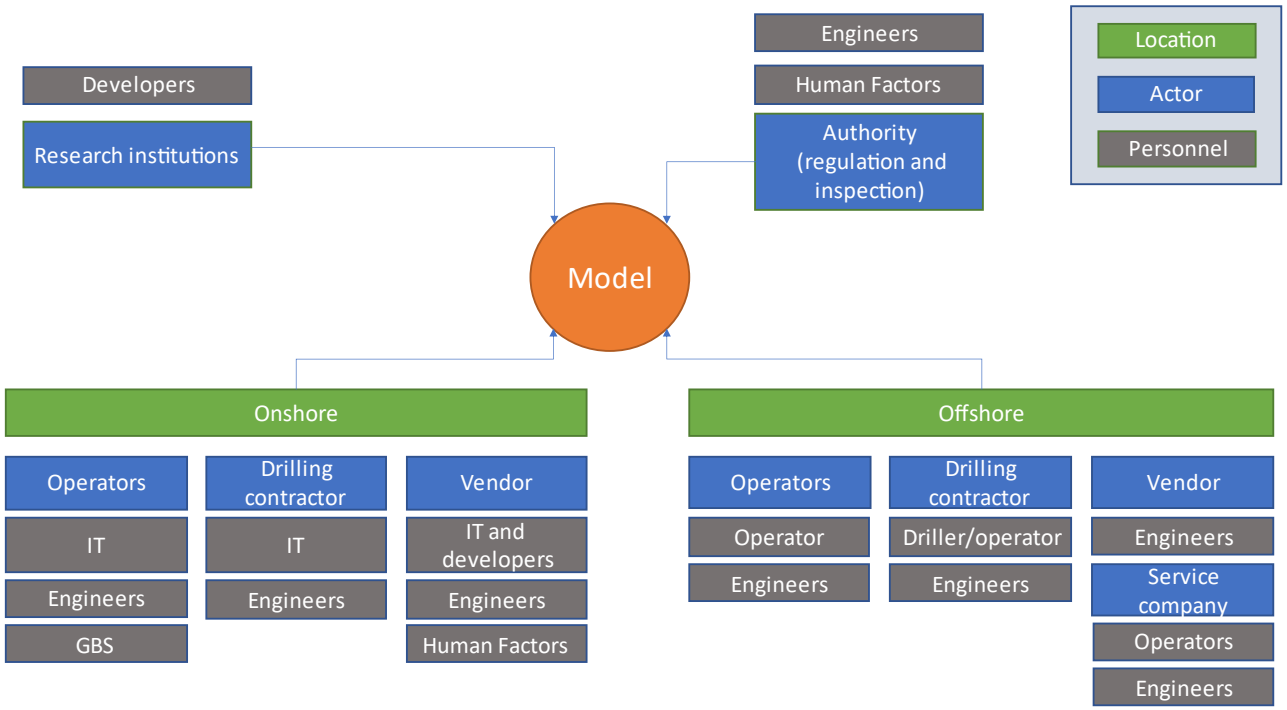


Figure 1 Possible participants involved in model-controlled operations

3 Secure use of data from model-controlled operations

A key challenge for digitalisation is data quality. Data constitutes the very foundation of a digital society, and must be both accurate and of high quality in order to achieve the desired effects of digital solutions. Poor data quality can result in higher operational costs, lower confidence and an increased risk of adverse events. This is also very relevant to models, where a general rule is that bad data in results in bad data out ("garbage in, garbage out"). While one may believe that it is possible to develop models which are to some extent robust in relation to poor quality data, a combination of poor quality data and an inaccurate model could, in the worst case scenario, result in erroneous information and, ultimately, poor or even fatal decisions.

The impression gained from the interviews is that models can be considerably more vulnerable to errors in input data than human operators. On the one hand, models add accuracy and reliability, provided that data and external circumstances lie within the range for which the model has been designed and tested. On the other hand, an operator will often be able to handle surprises much better than a model. Efforts are being made to improve software in relation to this, partly through the introduction of learning algorithms, but such methods are considered to be at an early stage as regards drilling operations. Accordingly, the quality of data from model-controlled operations is closely linked to the quality of the input data.

During the interviews, an emphasis was placed on the testing of models, to some extent combined with the training of users. First offline against a series of test cases, then in a realistic simulator, followed by onshore test facilities, and later with a gradual phased introduction offshore, with the models being run parallel to operations, without the results being actively used.

In many cases, there is some overlap between models from different companies, and different models can be compared in order to verify calculations during the process.

Input into models and model computations performed during an operation, either to provide a set-point for control systems or to provide decision support to operators, is monitored partly using algorithms and partly by dedicated operators ensuring that everything is functioning as intended, depending on the complexity and vulnerability of the computations concerned. Several interviewees described algorithms which can, for example:

- Remove data points which are obviously erroneous, e.g. because the value jumps beyond what is physically possible without any operational reason.
- Correct for jumps if the cause is operational in nature, such as when drill bit depth jumps because the driller corrects the length of the drill string, or when active volume jumps because a tank is added to or removed from the active volume.
- Check whether calculated values fall within a predefined range of values. As a general rule, this method does not work for parameters which vary during the process, such as bottomhole pressure, which rises as the borehole gets deeper, or surface pressure, which is a function of pumping rate in managed pressure drilling (MPD) and well control operations. It is possible to envisage methods which take such effects into account through a simple and robust algorithm monitoring a more advanced model, but we did not see any examples of this in the interviews.

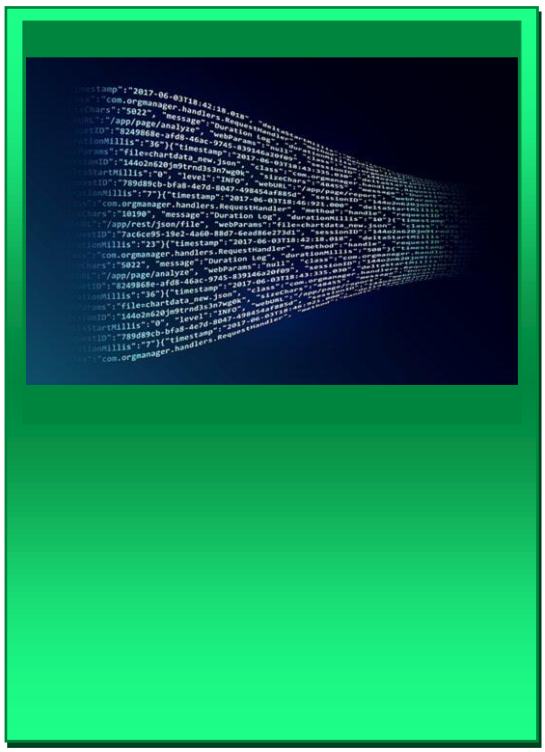
Otherwise, the impression that operators and/or model specialists still have a pivotal role to play in model-controlled operations is confirmed through the fact that they monitor operations to ensure that the systems are functioning satisfactorily and either control the operation using input from model computations, or intervene if the automatic systems fail.

3.1 Data sources and quality assurance

According to [18], the industry is currently facing challenges associated with insufficient sensor data and inadequate data quality for drilling operations. This is causing a lot of time to be spent configuring, checking and maintaining the information that automated drilling systems need, and as a result, more people are needed, rather than fewer. A lot of data from sensors is rarely used today, and no checks are therefore performed to determine whether or not the quality of the data is sufficient.

The use of poor quality data masks the existence of various problems, and signs of poor quality data must therefore be given the same priority as signs of drilling problems. It is sometimes impossible to correct poor data. Computer systems should therefore be developed to give immediate feedback to the user if poor data is detected (i.e. a system which monitors data quality), especially if the error could impact on decisions. Users of real-time drilling data must also have the ability to provide instant feedback on data quality, which is easier if there is a clearly defined relationship between different interest groups.

Model-based solutions have to deal with many different data sources, not only because there are so many different systems and data sources in use on a facility, but also because the same model can be used by several participants. It is therefore important that the data sources used in a model are clearly defined and delimited, and if changes are made which affect these sources, this should preferably be detected automatically by the model by means of alarm limits or similar, or notified to the relevant participants. However, it can be challenging to obtain an overview of the consequences that various changes will have. For example, interviewees pointed out that a change as small as the resolution of a data point could have major undesirable consequences elsewhere in the data chain. It is therefore important to limit both possible data sources and input values, so that changes are more likely to be identified. At the same time, redundancy between sensors (and models) provides more scope for consistency checks and the detection of sensors which are producing erroneous values. In this way, multiple sources of data can be an advantage, and this is a careful balance which must be struck in each case. Another important point is that the amount of duplicated data input into different models should be reduced, as this can mean that the same value has to be updated in several places, which experience suggests is a potential source of error [20]. In cases where erroneous data has been entered in systems, it has often been easy to blame human error, while many recent reviews and reports suggest that underlying technical causes are more important, which perhaps indicates that technology should provide humans with better support [19].



As described above, multiple data sources can represent a challenge if different data sources do not produce the same results or measurements. A solution is also needed which will work when or more of the data sources have been disconnected or fail. In theory, estimators can produce better results, but for all computations which are based on multiple data sources, it will be difficult to make them sufficiently robust in the event of errors or disconnections.

Data quality from a security perspective is discussed in more detail in [21]. However, it is important to point out that data quality in itself is not enough to ensure the safe use of data from models. Safe use will also require provision for repeatable real-time measurements with little time delay, sufficient resolution and high accuracy.

3.2 Access control and reliable communication

As mentioned previously, models will often be complex, and changes to both model and data input will require thorough testing before they can be put into operation. Even small changes made to a model's input signals can have a major impact on the output, and it will therefore be important to maintain control over who has access to make changes, whether intentional or unintentional. In addition, a log should be kept of all changes that are made, and who made them and when. Such a history will make it easier to correct any errors or unfortunate changes.

Another important point that was highlighted during the interviews was to ensure reliable communication, such as knowing that data is being generated with the right time-stamp (see [21] for more details on this topic). There was also a lot of discussion concerning the availability of data, with particular reference being made to the importance of having priority access to communication channels with respect to land. If a communication

channel is overloaded, there is a risk that data that is essential for a drilling operation will not arrive in the correct manner.

3.3 Utilisation and availability of data

As regards the utilisation of data, this is largely limited by available sensor, communication and data processing technology. For example, there is still a strong need for reliable, high-frequency, inexpensive and good communication between the lower part of the drill string and the drill floor, as well as better sensors and processing solutions. This will help to improve the availability of accurate and reliable information which can be used directly in models and decision-making processes, and will in turn contribute to safer and more efficient drilling operations. Although solutions which offer faster communication rates are available, they have often not been adopted due to the absence of an industry standard, tight budgets, poor reliability and/or high maintenance costs.

Sensors are supplied by different vendors, and the data from these sensors must undergo quality assurance and be compiled in an appropriate manner so that trust in the data can be built up. According to [15], one that the most challenging aspects of using models and simulators in automated drilling operations are delays in time and space with tools in the well. Insufficient bandwidth makes it difficult to use models in real time. We are now seeing a trends towards the introduction and commercialisation of 'wired pipe' with built-in communications. This will enable some of the challenges associated with time lag and low bandwidth to be overcome.

As mentioned previously, the availability of data can also be improved by using redundant and preferably independent sensors. These can either be of the same type or use different measurement principles, but the most important point is that they provide a quality check on data by comparing measurement values and ensure that data will be available even if one of the sensors fails. Nevertheless, it is necessary to be aware of how this information is handled, with the result that, instead of having systems which quality-assure each other or ensure back-up in the event of an error, one ends up with twice as many input values with perhaps neither set of values being correct.

During the interviews, it was also noted that models must be compatible with known (and preferably standardised) data formats, so that data can be readily shared between applications

3.4 Data sharing and ownership

Data is often stored by parties which offer a range of services, such as directional drilling, drilling mud handling, grouting, downhole tool handling and sometimes other services such as MPD and circulation systems. This presents challenges regarding joint access to, and the quality assurance of, data, which has also led operators to set up initiatives to address the problems using integrated platforms. However, it was mentioned during several of the interviews that data confidentiality can represent a challenge because the companies believe that it can give them a competitive advantage. This makes it more difficult for developers to test their models with sufficient thoroughness using suitable data sets.

During the interviews, the importance of data ownership was noted. It was regularly noted that it is the operators which own the data. However, it can be a challenge that so much data is spread across so many different applications that it is difficult to obtain a complete overview.

Nevertheless, the introduction of new ways of utilising data and information should not be delayed until data quality and communication is improved. Implementing work procedures and using data is the best way to test

that data is being stored and transmitted correctly within complex organisations and computer systems, and that poor data is detected. This will enable weaknesses to be identified which can be made more robust with regard to poor data.

4 Safe use of models for model-controlled operations

As noted previously, one challenge associated with the use of models is that they are just that, models. A model will never be able to fully reflect reality, and it is difficult to ensure that all parameters are taken into account during the development of a model. Even for accurate and complex models with good parameter adaptation, changes in operating conditions and the actual conditions prevailing during the drilling process itself will lead to inaccuracies in the model. Such adaptations are often not adequately taken into account when a model is used. There will also always be a trade-off between the complexity of the model on the one hand, and the requirements regarding performance and uptime on the other. It is therefore important to involve experts with a detailed knowledge of the processes that are to be modelled throughout the development process, and ensure that models are subjected to systematic testing before they are taken into use. Vendors and end users should also review and agree on procedures and standards for the development and documentation of software and models. One challenge associated with this may be the division of responsibilities, as a result of the fact that each company has its own areas of expertise, so that the decision as to who takes overall responsibility must largely be based on trust in the specialists employed by the vendors.

4.1 Development of models

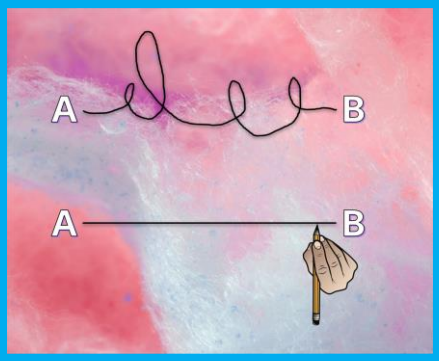
During the interviews, information on the standards, guidelines and specific methodologies that were applied during the development of systems was requested. No reference was made to any particular standards or guidelines. However, one of the interviewees mentioned the use of Technology Readiness Level (TRL) level, where each individual step of the TRL provides information on the requirements that a new technology must fulfil. This suggests that development is largely technology-driven, while development and design with specific consideration for human factors have less focus; see also the report on “Automation and Autonomous Systems, Human-Centred Design” [19] for more information on this.

There are currently no suitable or applicable standards to ensure good quality during the development of models. However, there are aspects of several possible methods and guidelines which could be useful. For example, the requirements of IEC 61508-3 [22] and ISO/IEC/IEEE 12207 [23] which define software development requirements will be of relevance. The same applies to DNV GL's best practice “Framework for assurance of data-driven algorithms and models” [24]. However, it should be noted that this was not developed with regard to applications for use in critical processes (e.g. where there are high security, environmental or economic risks).

Due to the complexity of modern drilling systems, it is necessary to ensure that the models undergo thorough design testing and verification and validation (V&V). This will enable design flaws in a model to be identified, e.g. integer overflow, dead logic and erroneous table lookups. Design verification must be in addition to the development activities. Formal tools and methods for development are becoming increasingly important for accurate and reliable verification. Many interviewees stressed that, in most cases, models are used which have been tested and developed over a number of years. This harmonises well with the recommendation of the participant who uses the most models amongst those interviewed to start with a basis which has been thoroughly tested and can be developed further. However, even when starting from a solid foundation, models can quickly become very complex. This causes them to require considerable processing capacity which can be at the expense of speed and real-time updating. In addition, the complexity will mean that specialist expertise is needed to set up and calibrate the models. It appears to be a challenge to determine when a model is “good enough” versus “too computationally intensive”. It may therefore be appropriate to simplify the models as

much as possible. Key assumptions for the model must also be visible and clear. This could for example be achieved through well-defined model constraints, so that each model only solves a single problem, rather than a set of challenges. This will also make it easier to facilitate transparent computations and technologies. However, as mentioned earlier, it is necessary to be aware of the uncertainty in both the model and the parameters associated with the model, and to see the entirety when combining models.

To date, it has been more common to develop physical models based on "first principles". This normally makes it easier to create a transparent model, where it is relatively easy to understand the underlying processes. Models developed according to physical principles often become very computationally intensive, and it is tempting to perform table lookups instead. However, table lookups can rapidly become challenging when multiple parameters vary simultaneously. As more data becomes available, development will probably increasingly be based on curve adaptation and machine learning, which could challenge the fundamental understanding of the system.



It appears to be a challenge to determine when a model is "good enough" versus "too computationally intensive".

Another challenge is that models are only correct within the range for which they have been adapted and experience has already been gained. Unforeseen events can therefore lead to major errors.

During the development process, it is also important to remember that the model should contribute to the best technical solution, and that the introduction of new technologies is not an end in itself. Consideration should also be given right from the start to the type of human-model interaction that will be required, and that this interface should make a positive contribution to the existing solution (where applicable). In addition, it is important to facilitate for the widespread use of auxiliary functions and the simple collection of documentation.

In addition to the need for the model to contribute to the best technical solution, it is important to point out that the model must be reliable. If the user cannot be confident that the systems will work when needed, the result could be frustration or, in the worst case scenario, even dangerous situations.

4.1.1 Working methods associated with the development of models

It is recommended that the parties involved, including the model developer, end users and vendors involved, discuss working methods to ensure high-quality deliverables, upgrades and troubleshooting. This is especially important when models are complex and developed by many people or over an extended period of time.

The following discussion is intended not as a complete overview of good working methods, but as examples to illuminate key areas. It is recommended that the parties involved agree on a document which outlines specific procedures and methods which are to be used in each project.

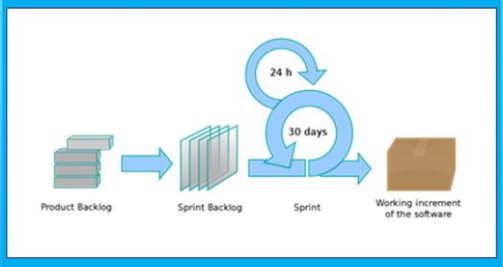
First, *documentation* is a pivotal and often relatively neglected area. The process starts with an overall specification of how a system and involved models are expected to work, including a description of what constitutes the input and output, what effects should be included in the model, and how accurate the results will be. The specification of accuracy must be adapted to the relevant needs. For example, the needs will be different when reliable measurements are available and can be used to calibrate a model which will interpret the measurements or predict the immediate future, compared with a situation where the model is used to calculate a long and complex sequence of events without supporting data.

Plenty of experience has been gained of the development of documentation in some detail down to the individual algorithms that must be created before the actual coding begins. Such documentation is often created as separate inhouse documents. However, during code development, it is advantageous to integrate the documentation with the code, either in the form of comments or by using specific tools for this process. Similarly, it can be useful to obtain good documentation for software libraries that are to be used.

A major challenge is to keep your documentation up to date when the algorithms change during the process. It is recommended that ways of following this up be identified, both because updating documentation improves the quality of the work, and because it makes it much easier to pick up the code for further upgrading after an extended period of time has passed, especially if new employees have taken over responsibility.

It is also recommended that consideration be given to some form of *test-driven development*, ideally fully automated where practicable, for the project. This often requires some modularisation of the model, where the anticipated limits of the response to each module can be described. For example, when describing the density of a water-based drilling mud, it is possible to check that density, compressibility and thermal expansion values lie within what is practicable. A test can then be integrated into the compiler so that it is conducted automatically each time a change is made to the code.

It has become standard to use tools for the *version control* of source code, with associated documentation. This is recommended as a mandatory minimum requirement. In addition, it is recommended to have a conscious approach to the way in which such a tool should be used, particularly as regards how development versions and versions that are undergoing the final test phase prior to dispatch are combined. More details fall outside the scope of this report, and reference is made to the many books and publications on the subject; see for example [25].



There is some variation in the way in which operators fulfil their “see-to-it duty” and ensure that all parties in the supply chain have an overview of and follow up HSE consequences, both during the design phase and in the event of changes.

Good cooperation during both the development process and subsequent upgrades and bug fixes is considered to be very valuable. In this regard, extensive

There can also be some variation in the way in which operators fulfil their “see-to-it duty” (the Framework Regulations: Section 18 “Qualification and follow-up of other participants” and Section 7 “Responsibilities pursuant to these regulations” [10]) and ensure that all parties in the supply chain have a record of and follow up on HSE consequences, both during the design phase and in the event of changes.

Good *cooperation* during both the development process and subsequent upgrades and bug fixes is considered to be very valuable. In this regard, extensive use is made of agile work processes with user involvement, and it is recommended that consideration be given to this. One such method is Scrum, where the entire project team communicates on a daily basis, the direction can be continually adjusted based on the experiences and wishes of the end users, and the work is divided into “sprints” (short periods of time) of two to four weeks, where some functionality is completed, demonstrated and assessed at the end of every “sprint” [26].

The *testing and validation* of software is pivotal, both during the process and in connection with the handover of deliveries. It is recommended that this be emphasised with strong end user involvement during certain

aspects of the testing process. It also became apparent during the interviews that end users also placed great emphasis on this point and allocated resources to it; see also section 4.2.

4.1.2 The development of models which are robust in relation to poor data

As explained earlier, it is still necessary to take account of the fact that both measured values and their associated time-stamps could be inaccurate or erroneous, even through considerable effort has been made to improve sensor technology. This is a challenge that has accompanied the development of real-time models for decision support and automation over many decades, and a lot of resources have been spent on creating algorithms which check consistency both between different sensors and between computations and sensors. In many cases, a model can correct or disregard erroneous data, and thus continue without any problems of significance, while in other, less clear cases, a model can issue warnings or alarms, and then either switch to a predefined "safe mode" or prompt human operators to intervene, or both. However, there will always be a risk of unexpected errors which the model does not detect. This can be handled through gradual implementation, with thorough and realistic testing during the process, until a level is reached where the use of models in a holistic perspective offers safety benefits which outweigh the risks and consequences associated with the introduction of models.

One possible pitfall is allowing human operators to monitor systems which use model calculations. Over time, operators will gain so much confidence in the models that they start focussing too much on other challenges and become too slow in detecting problems caused by data errors which one of the models fails to handle. This is why we believe it is important that the monitoring of models is also automated and tested thoroughly, preferably supported by redundancy and consistency checks.

4.2 Testing of models

"The responsible party shall ensure that analyses are carried out that provide the necessary basis for making decisions to safeguard health, safety and the environment. Recognised and suitable models, methods and data shall be used when conducting and updating the analyses."

Section 16 of the Management

According to the Section 16 of the Management Regulations [4]: "The responsible party shall ensure that analyses are carried out that provide the necessary basis for making decisions to safeguard health, safety and the environment. Recognised and suitable models, methods and data shall be used when conducting and updating the analyses".

But when is a model good enough, and when can it be trusted to provide the right information for a decision to be made, both in relation to the safeguarding of health, safety and the environment, and in relation to optimising a given process?

To ensure that a model works as intended, it must be tested, verified and validated. According to the interviewees, this is done using simulations based on real process data. In this way, it is possible to build up a good understanding of how a model works with real data, as well as how it works when poor quality data or incomplete data sets are fed into it. In addition, a factory acceptance test (FAT), site acceptance test (SAT) and minor pilots are conducted before a complete rollout is carried out.

The most challenging aspect of testing a model will often be anticipating all the possible scenarios to which the model could be exposed, especially in the case of dynamic models. Using different data sets, it is possible

to test a wide range of realistic situations, and by manipulating the data sets, it is also possible to build up a good understanding of how robust a model will be with respect to poor quality data. However, it is not possible to test for events that have not yet occurred, and it is often in such cases that the most dangerous situations will occur, especially if the models have been in use for a long time and users have begun to blindly rely on them to work at all times. In such cases, it becomes important that consideration is given to possible back-up solutions, and that these are readily available and well-known to the operators involved.

4.3 Communication between models and with the operating system

During the interviews from [18], it became apparent that there is no common communication standard for drilling equipment, and that there are so many uncoordinated initiatives aimed at establishing such a standard that they are leading to greater complexity. The fact that there is no standard also makes it more challenging to develop solutions which will communicate with existing equipment, such as sensors. This can also be a challenge where many different models developed by different participants have to talk to each other and exchange data. In such cases, the various participants involved should agree on how data exchange should take place and which formats should be used. The use of good frameworks and protocols which safeguard this exchange will avoid unnecessary errors relating to the exchange and sharing of data. For example, Open Platform Communication Unified Architecture) (OPC UA was highlighted during several of the interviews as an example of a framework that is becoming increasingly widely used. OPC UA is a standard for industrial communication and information modelling which was first published in 2008 [27] and has been increasingly adopted in recent years. As the name implies, OPC UA is an open standard, which is intended to ensure the secure and platform-independent exchange of data at field equipment level and between OT and IT. More information about OPC UA and data exchange can be found in the report entitled “Data quality in digitalisation processes in the petroleum sector” [21].

Over time, some actors have begun offering a common base platform for automation, consisting of models for controlling, monitoring, planning and optimising drilling operations. On top of this, it is possible to create custom applications which are adapted to the needs of the individual company or user using the Application Programming Interface (API), often based on the provider's example code and associated documentation and technical information. This provides excellent opportunities for tailoring solutions to include only what is relevant to each user or company, and could therefore potentially contribute both to cost savings and better HSE, because it is possible to eliminate functionality which is both unnecessary and makes the systems more complex than is necessary. At the same time, it opens up the possibility of more people having access to connect to external software, which in turn could introduce potential vulnerabilities. This not only makes it easier to introduce potential malware, it also increases the risk of introducing bugs. It is therefore important for vendors to have a good overview of the opportunities that APIs offers, who is connected to them and what rights they have, e.g. in relation to the reading and/or writing of data. It is also recommended that the same regime be used for the development, testing and validation of models as discussed in Chapters 4.1 and 4.2, along with good procedures for change and access control, as discussed further in Chapter 4.4.

4.4 Change and access control

As the models are taken into use, it is likely that both minor and major updates will be necessary. For example, this could be due to changes in the process, other external influences or the discovery of errors in the model. In the case of minor changes in parameters, for example, it may be enough to ensure that the model continues to operate within given limits. These limits will then typically be set during the development of the model. What is important about such an update is that it is ensured that those who make the changes understand how the changes will impact on both the output of the model and the rest of the process in which it operates. This can typically be done by limiting those who have access to make changes and ensuring that any such changes undergo quality assurance before implementation. There should also be a limit on the scope of the changes

that can be made in order to mitigate the possible consequences of errors. For example, it could be physically possible to make major changes in the input to a model, but where this is not necessary, it should be limited so that humans and other systems can more readily verify the change and intervene in time if necessary.

In addition, a log should be kept of all the changes that are made to the models, and who made them and when. Such a history will make it easier to correct and identify both intentional and unintentional errors.

Another point that has been highlighted, but which may not be considered a direct change, is that it must be ensured that the models are calibrated and updated at all times. For example, it was mentioned during an interview with one of the companies that if a process simulator is used for testing and verification, changes to the actual process will not be approved with final effect and put into operation until the simulator has also been updated. This approach ensures that the simulator does not become outdated.

One challenge associated with the use of models, which is also relevant to both parameter changes and calibration, becomes apparent if the model does not work optimally for certain sections of the well or a certain type of operation. This could then force the operators to override the model, and if this happens repeatedly, it could become both annoying and disruptive. It will then be important that there is a good system to capture this type of non-conformity, so that the model can be better adapted. There are several ways of doing this, e.g. through manual updates to the model, but it is also possible to use online parameter estimation for automatic calibration [17].

In the case of major changes, such as changes in functionality, the interviews showed that quality assurance will be required through management of change (MOC), verification and validation (V&V) and functional safety assessment (FSA) [28].

4.5 Training

Inadequate training was highlighted as one of the biggest challenges to managing the transition to new systems [29]. This issue was also discussed extensively during the interviews. Although the companies believe that they have good training programmes in place, it is difficult to train users to handle every possible situation. Not only can it be a problem that the models and systems are so complex that it is difficult to understand what to do in the event of a failure if the systems produce erroneous data, it can also be a challenge that users come to rely on the systems so much that no one possesses the necessary mental models of what goes on down the well. With regard to this, a number of the interviewees referred to the importance of running the new systems in parallel with the “old”. In this way, it is possible to both verify and improve our understanding of the new system without taking away the underlying understanding. This will also increase the verifiability for the operator.

Regardless of the scope of training and testing, it will never be possible to predict every possible situation, and it is important to be aware of this limitation in any training programme.

Regardless of the scope of training, it will never be possible to predict every possible situation, and it is important to be aware of this limitation in any training programme. Thus, for a driller who is an important safety barrier on a facility, it is necessary to ensure that systems are created which support him or her, rather than create uncertainty, frustration and/or a sense of disempowerment. This approach will enable the driller to

spend more time specialising in and focussing on the aspects of the process which offer increased safety and optimised drilling, and thus remain a driller, rather than simply becoming a computer expert.

5 ICT security in connection with the use of model-controlled operations

When sensors, systems and machines are connected together to enable information flow, communication and remote control across geographic locations, it also opens up the possibility of unauthorised persons gaining access to sensitive information or interfering with critical functions from anywhere in the world [18]. Increasingly advanced ICT systems also place greater demands on relevant ICT expertise, both internally within the industry and amongst regulatory authorities. This makes it even more important that professionals and managers possess such expertise [18]. In order to detect abnormal circumstances in data from drilling operations, the right person must look at the right data at the right time, and at the same time interpret the data correctly. This therefore entails a balancing act between operational security and ICT security, as the information flow which is necessitated by secure automated and/or remotely controlled operations supported by models must be balanced against greater vulnerability and the need for confidentiality between vendors.

The most effective strategy for improving ICT security for industrial applications is to ensure that development is an iterative process, both because threats are constantly evolving and because it takes time to develop the experience that is needed to manage ICT security well.

According to DNV GL's 2015 report to the Lysne Committee, the "top ten" digital vulnerabilities in the oil and gas sector were [29]:

Table 5.1 "Top ten" digital vulnerabilities in the petroleum industry

Scenario no.	Vulnerability
1	Insufficient attention and training amongst employees
2	Remote working
3	Use of standard products with known vulnerabilities in production environment
4	Inadequate safety culture amongst subcontractors
5	Insufficient separation of data networks
6	Mobile storage devices (including smartphones)
7	Data networks between onshore installations and oil fields
8	Failure to physically secure computer rooms, switchgear cabinets, etc.
9	Vulnerable software
10	Outdated control systems on installations

Most of these are relevant to drilling, and some are discussed in more detail below.

5.1 Training (scenarios 1 and 6)

Humans can be both the greatest asset and the greatest threat to a company, because it is easy to make mistakes and take injudicious decisions, such as using an unsecured USB flash drive. Humans are the common denominator in every link in the safety chain, and it is important to train staff to cover every area and to deal with every conceivable situation.

In DNV GL's report entitled “Training and drills” [30] , a number of measures aimed at ICT security incidents are defined, such as that requirements regarding training should not be established at system level, but be included in the company's overarching systems. A holistic system with an overview of completed planned training is desirable, and a plan for skills development within the field of ICT security should be established. It is also recommended that objectives be defined for training and drills, and that anyone who could involved in a real incident be included; see also [30] for more details.

Training and drills can be particularly challenging as regards drilling operations because, as mentioned in Chapter 2.5, many participants are involved in such operations. In turn, it then becomes essential to have a good overview of the parties involved and the delegation of responsibilities.

5.2 Remote control from onshore (scenarios 2 and 7)

As the world is digitalised and made “smarter,” it also means that the attack surface gets bigger. While this contributes to the streamlining of both operations and ICT infrastructure, it also creates greater complexity, which opens up the possibility of new ICT security challenges. It is also apparent that the threat landscape is expanding due to the fact that more and more actors are becoming increasingly sophisticated in their attacks.

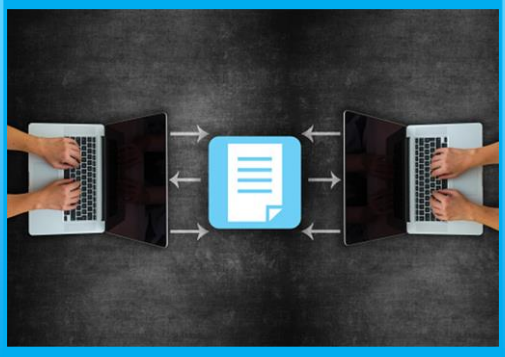
In connection with the use of remote control, there are a number of questions that should be borne in mind:

- Who has access and why?
- When do they have access?
- How long do they have access for?
- Which areas do they have access to?

Firewalls and encryption can assist in monitoring and restricting access to information and different parts of the system. Using various integrity mechanisms, such as digital signatures, it is also possible to detect whether data has been altered or tampered with. A system to manage access is needed, and during the interviews, it became apparent that secure remote connection solutions were often used to gain access to control operations from land. Once access has been granted, it is important that the networks are segmented so that access is only given to the necessary parts of the system. This helps to provide protection against both intentional and unintentional errors and incidents.

In the case of drilling operations, it is currently possible to make only limited changes from land with regard to the models. Where this is done, secure remote connection solutions are used which require authentication in order to obtain approval from the facility prior to connection. However, this will become an increasingly topical issue, and the systems required to deal with it will then have to be put in place.

As regards the drilling process, it has become more commonplace to send configuration files or procedures from the land, which the driller is then responsible for initiating. These files have an advisory function, and direct control from land in real time has not been necessary. Nevertheless, there is a risk that such an approach could inflict damage on the



For the drilling process, it has become more commonplace to send configuration files or procedures, which the driller is then responsible for initiating, rather than controlling the system directly from land. These files have an advisory function, but they can still lead to incidents, e.g. if the configuration files are based on poor quality data or someone with an overlay has deliberately made potentially

system, for example as a result of someone deliberately making a change in the configuration file before it is sent. In this case, the driller will be the barrier that must be sufficiently familiar with the systems to be able to identify the error. In such cases, it will therefore be important that the driller has the right aids at his or her disposal. For example, good user interfaces which provide a complete overall picture, as well as real-time sensor data, can be good sources for identifying errors, although it can still be difficult to trace the cause directly to the configuration file. Another possibility using models and simulators highlighted in the report entitled "Remote Work and HSE" [31] is to use these in an attempt to replicate any interference or incident. In this way, simulators can be an important measure in relation to ICT security.

5.3 Logical and physical division of networks (scenario 5)

Having more participants with access to critical production systems will increase the potential exposure to malware. An inadequate security culture amongst subcontractors relating to digital vulnerabilities is also a risk that DNV GL highlighted in its report on Digital vulnerabilities in oil and gas [29].

"Direct hacking via the IT domain is a risk that is mitigated with zones and tunnels. For example, the use of DMZ (demilitarized zones) provides a segregation between IT and OT."

DNV GL 2020 [2]

Direct hacking via the IT domain is a risk that is mitigated through zones and tunnels [2], but the impression is that this is not a widely used approach in drilling operations. For example, the use of DMZ (demilitarized zones) provides a segregation between IT and OT, and the need and scope for communication between them is also often limited in terms of both quantity and time, so that the DMZ can be configured to allow only small transfers of data during limited periods of time as and when appropriate. However, such segregation of networks could represent a challenge for older installations where industrial ICT systems were developed without regard to the extensive sharing of data. There are in any case numerous ways of getting malware into OT systems, e.g. in connection with the delivery of a system, through maintenance or through an unauthorised connection to an OT system (mobile phone, laptop, etc.). This path is often the most difficult to establish barriers against, because it is person-dependent [2].

In order to have a complete view of the potential for both unintentional and targeted attacks on a facility or data centre, it is important to identify all possible information and communication channels between the various levels within IT and OT. As soon as the potential attack surfaces have been identified, it will be easier to segregate, monitor and protect them. However, this can also bring with it vulnerabilities, because attack surfaces are becoming better known and standardised, which in turn can make it easier to organise targeted attacks. The typical vulnerabilities that have been identified are access points to OT and IT and include both physical and remote access. Other attack surfaces include applications which are shared between OT and IT, and internally on an installation. Although the boundaries between IT and OT are being challenged, it is important to bring about a good collaboration between the two levels. This is because, even if the OT department is responsible for the OT side, it is possible to draw on expertise from the IT side, e.g. concerning the operation and securing of networks. A prerequisite then is that the IT side also possesses the necessary expertise relating to OT.

A model can be implemented at most levels (see Figure 2), but it is often the case that the more complicated and complex a model is, the further away from the drilling operation itself it is located. Some examples of models and where they are implemented are presented below:

- Dynamic floor saver, which is implemented in the control system for the draw works in order to take account of mass and velocity to reduce the speed to prevent a collision with the drill floor.

- Mathematical models implemented in the control systems of robots which describe dynamics and motion in order to prevent collisions and control collaborating robots and machines.
- Dynamic models implemented on a PC outside the control system to calculate assumed future behaviour and, based on the results, determine set-points for regulating loops in the control system (Model Predictive Control - MPC).
- A digital twin with one or more built-in dynamic models is implemented on a PC outside the operating system to simulate the operation in real time. The results are then compared against measurements to provide alerts and decision support.
- In cloud solutions, parameters and limit values transferred to the driller are calculated as part of the plan to drill a specific well.

See also Chapter 2.3 for more examples.

The figure below describes how the information is transported from the technical systems in connection with drilling (green #1 in the figure) and back to the driller (yellow #4) or down into the technical systems (green #2). For a more detailed discussion concerning this figure, see the report entitled “Principles of Digitalisation” [32].

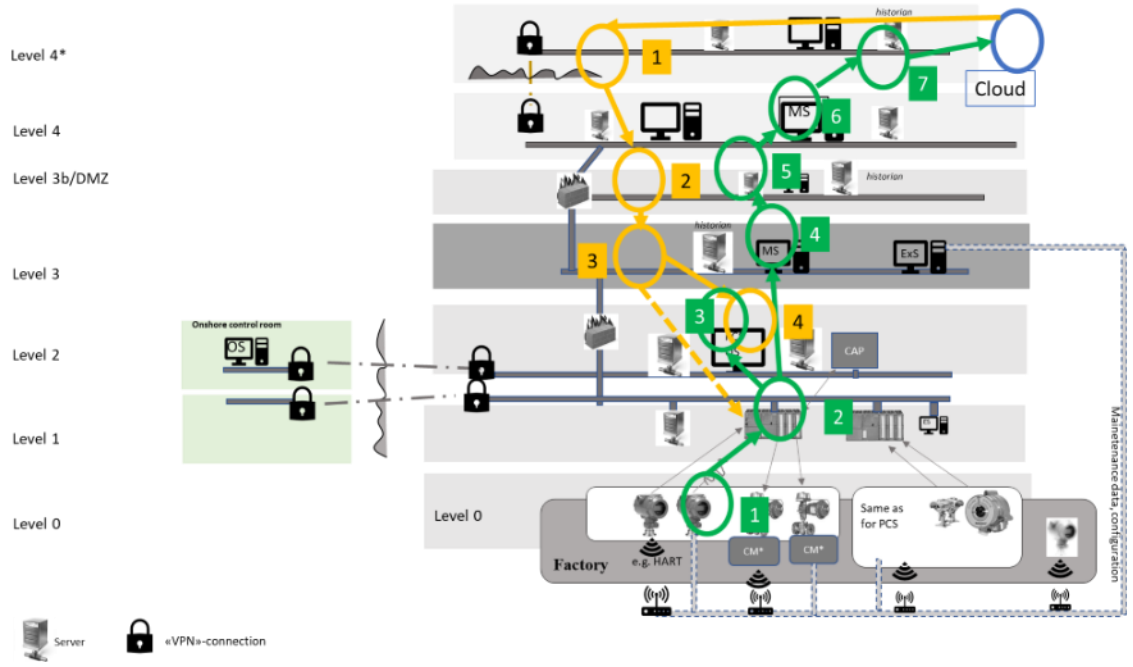


Figure 2 Possible transfer of information to the cloud and back again

By producing the data flow in this way, it immediately becomes clear how important it is to ensure both the green transfer to the systems in cloud solutions, and the yellow data flow back to OT. It is not just the path back that is important; transmitting erroneous values up to the cloud can lead to erroneous decisions and incorrect instructions to the driller and systems.

It is also apparent from Figure 2 that the systems that should be protected are those at the lowest possible level in the model, because they will then be better secured through firewalls and DMZ, while access is easier further

up, e.g. to cloud solutions. Cloud solutions can summarise information from different systems, as well as multiple installations, and will therefore also be more susceptible to both unintentional and intentional errors.

5.4 Physical access to installation and data centres (scenario 8)

Physical access to both facilities and data centres is relatively easy to assess and manage. There are a number of possibilities at both locations. For example, video surveillance, the stationing of security guards, ID cards, key cards, access control and keys are all possible ways of dealing with this. In the case of offshore, in addition to this is the limited scope for access to the facility, as a helicopter (or a boat) will be needed to get to and from the facility. In addition, it is commonplace for all jobs that are to be performed to be managed through work orders, making it easy to log and review what has been done and by whom should an event occur. Securing of the environment is normally expected at a data centre, but this is not always the case on a facility. It will nevertheless be relevant where there is a requirement for models to control all or part of a process, because such security could be essential in ensuring that the models are able to run without interruption. For example, room temperature could be a challenge. Alarms indicating open doors and power outages are other examples, as is the installation of secure cable bushings to provide protection against water leakage and fire. Last, but not least, back-up and recovery plans are important elements to have in place [33].

5.5 Model development and updating from an ICT security perspective (scenarios 9 and 10)

Chapter 4.1 discussed how it is possible to develop robust and good models which, with proper use and training, can both optimise and improve the drilling process. In this section, the focus is placed on model development and updating from an ICT security perspective. Working on ICT security requires the structured mapping of the entire threat picture and the identification and prioritisation of associated working methods. In this way, it will be advantageous to rely on available frameworks and methodologies, such as the NIST Cybersecurity Framework ([34] and Figure 3), ISO/IEC 27001 [35] and IEC 62443 [36]. See also the reports entitled “Regulation of ICT security in the petroleum sector” [37] and “Basic principles for ICT security in the ICT industry” [38].

Drilling applications and models often have proprietary files which can only be read by the applications which created them or which were created in order to read/access them. Specific software will therefore be required in order for it to make sense to read the files. While this may initially provide an additional layer of protection against hacking, it will also present challenges when data is to be shared between models and it is necessary to provide for the use of a common exchange format which facilitates holistic solutions. It is therefore necessary to decide in advance what type of files to transfer and how they should be protected.

During the interviews, no reference was made to any specific standards which are used during the development of the models, although some of the companies had a good knowledge of NIST [34] and IEC 62443 [36]. However, the standards are often considered to be both difficult to read and complicated to apply, and it would therefore simplify the everyday life of the individual participant if there were more practical guidelines for the performance of ICT vulnerability analyses, which also include model-based solutions.

Figure 3 NIST CyberSecurity Framework (from [34])

Regular patching to update the systems on which the models run is important for ICT security [33]. However, this can represent a challenge, especially if the models are in an OT system, both because it is challenging to set requirements regarding expertise, and because it often assumes that dedicated time is set aside, e.g. during a turnaround. Many people also do not know what vulnerabilities exist in their system. This often leads to patching being deferred or, in the worst case scenario, not being carried out at all. It is therefore extremely important that all models and systems are tested thoroughly before they are taken into operation, to avoid them having to be updated more often than is necessary.

6 Implications for production optimisation

By combining better sensors with models and simulators, it is possible to make it easier for users to manage and understand complex operating situations. New production optimisation tools, which utilise real-time data analytics, will lead to better utilisation of data and equipment to boost production, improve energy-efficiency, optimise maintenance and improve recovery [3]. By gaining experience of drilling operations where models and digitalisation are gradually taken into use in a wide variety of applications, as described in Chapter 2.2, it is possible to make it easier both to develop new solutions and to utilise infrastructure, data and technology which is already available for use in production optimisation. Increased instrumentation presents new opportunities for extracting information, but often the necessary systems are not in place to fully exploit this data. For example, there is considerable potential for combining domain knowledge, real-time data and physics-based models with machine learning to provide decision support in day-to-day operations. However, in the same way as with drilling, it is important not to make the systems too complex, because this can cause users to lose their mental model of the process and their overall understanding of the system. Possible application areas for models and digitalisation are logistics, maintenance planning and environmental monitoring [3]. In much the same way as with drilling operations, many small models and digitalisation initiatives can rapidly lead to unfortunate overlapping or adverse effects on each other if a holistic approach is not adopted when introducing new solutions.

In order to exploit the potential of digital solutions and the use of models in production optimisation, it is important to consider a range of issues, including:

- Avoid over-complicating the problem.
- Make use of existing infrastructure and sensor data wherever possible.
- Involve end users as early as possible in the development phase.
- Ensure that solutions are easy to maintain and scale.
- Be aware that new technologies introduce vulnerabilities.

- Work iteratively with ICT security throughout the development process.
- Ensure a holistic approach when introducing new applications.

7 Challenges and proposals for measures and improvements

This chapter summarises SINTEF's proposals for the industry and the Petroleum Safety Authority Norway, as well as the need for further work relating to knowledge acquisition.

7.1 Industry

Recommended measures for the industry are presented in Table 7.1.

Table 7.1 Summary of recommended measures for the industry

No.	Challenge	Recommendation
1	Ensure that models are of high quality.	No procedures or standards are currently available for developing models for use in critical processes. Nevertheless, vendors and end users should review and agree on the use of elements from relevant procedures and standards for the development and documentation of software (e.g. IEC 61508-3 or ISO/IEC 12207). This includes reciprocal involvement through the work. Section 16 of the Management Regulations is also relevant to both testing and operational purposes.
2	Determine when a model is good enough to be put into operation.	Models should be tested, verified and validated. Pilots are recommended prior to full roll-out.
3	Models are only correct within the range for which they have been adapted and experience is available.	Key assumptions for the model should be visible/clear. It should be an aim to test as many scenarios as possible, although it will never be possible to test for every unforeseen eventuality.
4	Inadequate maintenance and updating of models.	Clear ownership of model and data should be defined. The model should be tested sufficiently before it is put into operation to avoid unnecessary maintenance and updating. Plan updates well before the turnaround if it is not possible to update the model while it is in operation.
5	Inadequate understanding of model and system.	The models should not be made overly complicated, but they must still clearly reflect the key variables, objectives and constraints. It should also be ensured that the solutions are easy to maintain and scale.
6	Poor data quality and obsolete data format.	Both input and output data should undergo quality assurance, and compatible data formats should be used to facilitate simple sharing between applications. If appropriate, custom exchange formats into which proprietary formats can be translated can be used.
7	Many small models which solve individual problems and the associated lack of overview of applications and possibly overlapping applications.	A holistic approach should be adopted in connection with the introduction of new applications in order to reduce the number of (overlapping) applications and data sources, e.g. by ensuring that all new applications and digitalisation initiatives are reviewed and discussed by a multdisciplinary team of experts.

No.	Challenge	Recommendation
8	Segregation between IT and OT and inadequate understanding of challenges in the two different “camps”.	Expertise from IT into OT and vice versa should be utilised to build up a good understanding of the possibilities and limitations of both layers, while at the same time ensuring that the boundary between the two is clearly defined.
9	Inadequate system understanding and, in the long term, inadequate understanding of the underlying drilling process.	Thorough training should be provided, and it should be ensured that users have an understanding of both the models and the underlying process. Avoid relying blindly on the models and ensure that operators know what measures are required when the models do not function as intended.
10	Lack of ICT expertise concerning the introduction of models.	Thorough training should be provided, and it is important that both professionals and managers possess ICT expertise. It should also be ensured that this is not one-off training, but training that facilitates continuous skills enhancement in line with developments in digitalisation
11	Static management of ICT security.	ICT security for an industrial control system should be an iterative process, both because threats are constantly evolving and new solutions and remote control via the cloud can introduce new threats, and because it takes time to develop the experience that is necessary to manage ICT security well. ICT vulnerability assessments should be carried out in accordance with current standards.
12	Inadequate segregation and independence between systems used during drilling operations.	Ensure compliance with the requirements of the regulations (Sections 32-34 of the Facilities Regulations [39]). In the case of machinery on fixed facilities where safety functions protect people from moving parts, there is no requirement for independent systems (the Machinery Regulations). For the other aspects, the requirement concerning independence apply.
13	New technology introduces new vulnerabilities.	Be aware of utilising technology and models to improve safety and optimise the drilling process.

Training also appears to represent a challenge, and although many of the companies have good training programmes in place, it is difficult to train users to handle every conceivable type of situation. This is because the models and systems are complex, and it can therefore be difficult to know how to deal with or detect outcomes or errors, and because it can be a challenge that over time users become so reliant on the systems that they no longer possess the necessary mental models of what going on down in the well. The importance of involving users early in the development phase was also clearly highlighted in several of the interviews. It will in most cases provide a better and more secure end result and increase the likelihood of it being adapted to the organisation. This report should therefore be viewed in the context of [19], where the focus is on human-centred designs for automated and autonomous systems.

7.2 PSA

Recommended measures for the industry are presented in Table 7.2.

Table 7.2 Summary of SINTEF's recommended measures for the PSA

No.	Challenge	Recommendation

1	No common communication standard for drilling equipment and many uncoordinated initiatives contribute to greater complexity.	Support the industry in establishing a common communication standard for drilling equipment.
2	Lack of standards and methodology for the development of models and applications for use in critical processes.	Act as a driving force in the development of more customised standards/methodology for model development for applications which are to be used in critical processes.
3	Inadequate use of elements from existing relevant standards and methodology for software development to ensure high-quality models, such as the requirements in 61508-3 [22] or ISO/IEC 12207 [23].	It is recommended that the PSA ensure that companies use elements of relevant standards and methods during development. Section 16 of the Management Regulations is relevant to both testing and operational purposes.
4	Lack of ICT expertise concerning the introduction of models.	Follow up and define clear requirements for companies regarding ICT expertise, for both professionals and managers. Consider developing more practical guidelines for the performance of ICT vulnerability analyses.
5	Inadequate segregation and independence between systems used during drilling, despite requirements in the regulations (Sections 32-34 of the Facilities Regulations [39]).	It is recommended that the PSA clarify how Sections 32-34 of the Facilities Regulations [39] are to be interpreted.
6	Inadequate sharing of experience concerning the use of models.	Actively share learning from both successful and less successful projects relating to drilling operations and in other relevant industries.

Input from the industry to the PSA is given in Table 7.3.

Table 7.3 Input from the industry to the PSA

No.	Topic	Input
1	Little transparency concerning the development of models and the sharing of data, which contributes to poorer quality and safety of solutions.	Parts of the industry want the PSA to act as a driving force as regards transparency and the sharing of data. Although many initiatives have been implemented to promote the sharing of underground data, any new commitment to share results openly could lead to operators deciding to wait for “free” results from adjacent licences, which could slow down and sub-optimise activity on the Norwegian shelf [40].
2	Follow-up by the PSA	During the interviews, a number of the interviewees said that the companies wanted close follow-up from the PSA, and that working with them worked well in several of the projects where models were used.

During the interviews, it was also mentioned that the PSA should avoid the use of “should” and stipulate minimum requirements instead, and thus facilitate the simpler development of new functionality. On the other hand, one company had difficulty achieving a breakthrough within its own organisation as regards projects that extended beyond the minimum requirements. We have not included any recommendations concerning this, as the PSA's strategy has been not to stipulate detailed requirements, with the intention that the companies themselves should assess what constitutes prudent measures and there does not seem to be any broad agreement in either one direction or the other in this regard.

7.3 Need for knowledge acquisition

The purpose of this report is to give the industry a greater understanding of the challenges and opportunities associated with the use of model-controlled operations, particularly relating to how the models and data from the models can be used securely and how ICT security can be safeguarded. The main focus has been on drilling operations.

Both experts in data-driven methods and domain experts believe that machine learning also has huge potential in drilling operations, as in many cases it can complement physics-based computations and make better use of higher quality measurements from a growing number of sensors than existing methods. However, the variation in the characteristics of the underground during drilling processes is so great and so few sensors have so far been installed that it is important that domain knowledge and physics-based models are also utilised in combination with machine learning. With regard to this, there is a strong need for a better understanding of the opportunities and limitations inherent in the various types of machine learning, and how machine learning can best combine different types of information, including physics-based computations and measurements, in order to improve safety and reduce costs [41].

We also see a need to develop physics-based models which are even better adapted to real operational needs, and to make these models as simple and robust as possible both in relation to specific issues (including the optimal management of sub-processes) and in relation to the entirety. This can be done partly by improving existing models and the integration of different models, and partly by re-implementing key aspects of existing models in a better way. To succeed in this, domain experts, modelling experts, IT experts and end users will all need to be involved.

It may also be a challenge that models that are used in drilling operations often become so complex that it is difficult for users to maintain a complete overview and control over all the underlying computations and processes. Having this overview often does not provide the user with any added value either, particularly as models are increasingly being based on empirical data and the use of artificial intelligence, rather than physical models (black boxing). Nevertheless, it is important that users do not lose the mental model of the process and the overall understanding of the system that will enable them to intervene in the event of an incident. There is a need to bring in more experience and knowledge concerning how such meaningful human control can be enabled in cases where users do not necessarily understand the underlying models.

During the interviews, we got the impression that no specific standards, best practices or frameworks were being followed to ensure high quality the during development process. It may be useful to obtain more information on this and make specific recommendations regarding a framework that can be used. A good starting point will be DNV GL's best practice “Framework for assurance of data driven algorithms and models” [24], but with a stronger focus on applications which entail high risk.

There is also a need for more knowledge relating to the management of ICT incidents in connection with the use of model-controlled operations, and there will be a need for greater competence amongst professionals and management. There is also a need to collate more knowledge regarding how to drill and prepare employees and the organisation itself for such incidents.

Finally, we see a need for a greater understanding of man-technology-organisation (MTO) interaction, especially in connection with the implementation of new technologies which impact on roles and work processes, which is covered by the parallel report entitled “Automation and autonomous systems: Human-centred design” [19].

References

[1] DSIWG, *Data safety guidance, Version 3.2- The data safety initiative working group*. 2020.

[2] DNV-GL, *IKT-sikkerhet - Robusthet i petroleumssektoren: Resiliens mot cyberhendelser og kan blokkjede bidra?* . 2020.

[3] NTNU, *NTNU Strategy for Oil and Gas*, in *BRU21 Better Resource Utilitzation in the 21st century*. 2016, NTNU.

[4] Petroleumstilsynet. *Veiledning til Styringsforskriften (18. desember 2019)*. [cited 2020 31.10]; Available from: https://www.ptil.no/contentassets/332166193108427e978accb21449436c/styringsforskriften20_veiledning_n.pdf

[5] Bainbridge, L., *Ironies of automation.* Automatica, 1983. **19**(6): p. 775-779.

[6] Godhavn, J.-M., et al., *Drilling seeking automatic control solutions.* IFAC Proceedings Volumes, 2011. **44**(1): p. 10842-10850.

[7] Petroleumstilsynet, *IKT-sikkerhet – robusthet i petroleumssektoren*. 2020.

[8] *Petroleumstilsynet, Fagstoff, Ord og uttrykk*. Available from: https://www.ptil.no/fagstoff/ord-og-uttrykk/.

[9] SINTEF, *SINTEF 2018:00572, Kunnskapsprosjekt IKT-sikkerhet; Industrielle kontroll- og sikkerhetssystemer i petroleumsvirksomheten*. 2018.

[10] Petroleumstilsynet, *Veiledning til Rammeforskriften*. 2019.

[11] Standard Norge, *NS 5814:2008. Krav til risikovurderinger*. 2008.

[12] Standard Norge, *NS 5832:2014. Samfunnssikkerhet - Beskyttelse mot tilsiktede uønskede handlinger - Krav til sikringsrisikoanalyse*. 2014.

[13] NOU 2015:13, *Digital sårbarhet – sikkert samfunn. Departementenes sikkerhets- og serviceorganisasjon.* 2015.

[14] *Society for Risk Analysis Glossary*. 2018 31.10.2020]; Available from: https://www.sra.org/wp-content/uploads/2020/04/SRA-Glossary-FINAL.pdf.

[15] Sugiura, J., et al., *Drilling Modeling and Simulation: Current State and Future Goals*, in *SPE/IADC Drilling Conference and Exhibition*. 2015, Society of Petroleum Engineers: London, England, UK. p. 27.

[16] Deloitte. *Industry 4.0 and the digital twin*. 2017; Available from: https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/cip/deloitte-cn-cip-industry-4-0-digital-twin-technology-en-171215.pdf.

[17] Kaasa, G.-O., et al., *Simplified Hydraulics Model Used for Intelligent Estimation of Downhole Pressure for a Managed-Pressure-Drilling Control System.* SPE Drilling & Completion, 2012. **27**(01): p. 127-138.

[18] IRIS, *Digitalisering i petroleumsnæringen*. 2017, International Institute of Stavanger.

[19] SINTEF, *Automatisering og autonome systemer: Menneskesentrert design*, Petroleumstilsynet, Editor. 2020.

[20] Bjørkevoll, K.S., B. Daireaux, and P.C. Berg, *Possibilities, Limitations and Pitfalls in Using Real-Time Well Flow Models During Drilling Operations*, in *SPE Bergen One Day Seminar*. 2015, Society of Petroleum Engineers: Bergen, Norway. p. 14.

[21] SINTEF, *IKT-sikkerhet - Robusthet i petroleumsindustrien: Datakvalitet ved digitalisering i petroleumssektoren*, Petroleumstilsynet, Editor. 2021.

[22] IEC, *IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems.* 2010.

[23] ISO/IEC/IEEE, *ISO/IEC/IEEE 12207 Systems and software engineering – Software life cycle processes.*

[24] DNV-GL, *Recommended Practice: Framework for assurance of data-driven algorithms and models*. 2020.
[25] Loeliger, J., *Version Control with Git: Powerful tools and techniques for collaborative software development* 2012.
[26] Schwaber, K., Sutherland, J., *Srcumguiden -Den definitive guiden til Scrum: Spillereglene*. 2017.
[27] OPC-UA, *OPC 10000, OPC UA Online Reference, Online versions of OPC UA specifications and information models*. 2020.
[28] IEC61511, *IEC 61511 Functional safety - Safety instrumented systems for the process industry sector*. 2016.
[29] DNV-GL, *Digitale sårbarheter olje og gass - Rapport til Lysneutvalget*, Lysneutvalget, Editor. 2015.
[30] DNV-GL, *IKT-sikkerhet - Robusthet i petroleumssektoren, Trening og øvelse*. 2020.
[31] SINTEF, *Ptil IKT sikkerhet: Fjernarbeid og HMS*. 2019.
[32] SINTEF, *IKT-sikkerhet - Robusthet i Petroleumssektoren: Premisser for digitalisering og integrasjon IT-OT*, Petroleumstilsynet, Editor. 2021.
[33] Cavazos, C.J., *Ensuring Data Security for Drilling Automation and Remote Drilling Operations*, in *SPE Asia Pacific Oil and Gas Conference and Exhibition*. 2013, Society of Petroleum Engineers: Jakarta, Indonesia. p. 6.
[34] NIST, *NIST: Framework for Improving Critical Infrastructure Cybersecurity*. 2018.
[35] ISO/IEC, *ISO/IEC 27001 Ledelsessystemer for informasjonssikkerhet*. 2017.
[36] NEK/IEC, *NEK IEC 62443: Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program*. 2010.
[37] SINTEF, *IKT-sikkerhet - Robusthet i petroleumssektoren: Regulering av IKT-sikkerhet i petroleumssektoren*. 2021.
[38] SINTEF, *IKT-sikkerhet - Robusthet i petroleumssektoren: Grunnprinsipper for IKT-sikkerhet i industrielle IKT-systemer*, Petroleumstilsynet, Editor. 2021.
[39] Petroleumstilsynet, *Veiledning til Innretningsforskriften*. 2019.
[40] *Rapport for ekspertgruppen for datadeling i næringslivet*. 2020.
[41] DNV-GL, *OG21-study on Machine Learning in the Norwegian petroleum industry*. 2020.

Appendix A: Literature search

Much has been written on the subject, and a search on https://www.onepetro.org/ with the keywords “model AND controlled AND drilling AND operation” yielded 15,988 hits (May 22, 2020). If only more recent articles are included, from 2019 onwards, the number of hits is reduced to 897. These cover the entire world, and the impression is that many are very specific and most are probably more concerned with presenting and justifying a given solution than illuminating challenges critically. Narrowing down the search to “model AND controlled AND drilling AND operation AND quality AND norway” yields 1,097 hits, of which 699 date from 2005 onwards. With this limitation, there are many familiar names amongst the authors. “model AND controlled AND drilling AND operation AND (quality OR safety OR security) AND norway” yields 986 hits over the same period.

Technology for a better society

www.sintef.no