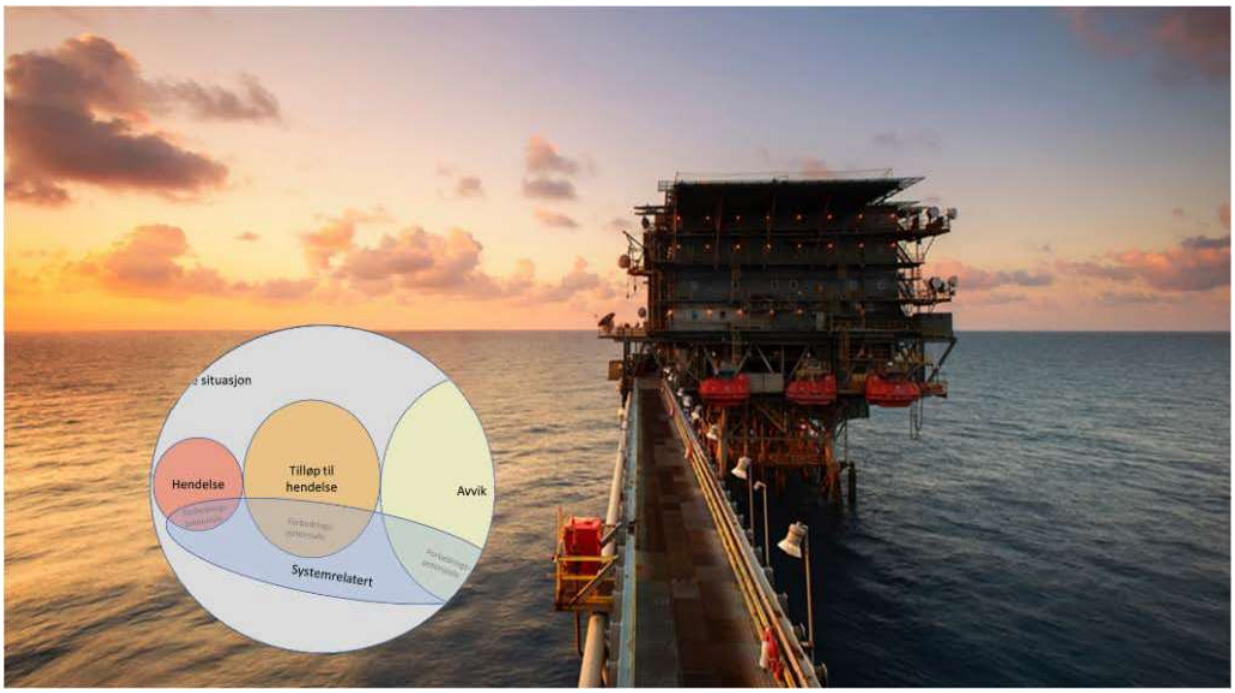


Report

Reporting of incidents in automated systems during drilling operations

Authors:

Maria Vatshaug Ottermo, Egil Wille, Knut Steinar Bjørkevoll, Lars Bodsberg, Tor Erik Evjemo, Kay Fjørtoft, Martin Gilje Jaatun, Thor Myklebust, Eivind Okstad

Report number:

2023:00191 - Unrestricted

Client:

Petroleum Safety Authority Norway

SINTEF Digital
Postal address:
Postboks 4760 Torgarden
7465 Trondheim

Switchboard: +47 40005100

info@sintef.no

Register of Business Enterprises:
NO 919 303 808 MVA

Report

Reporting of incidents in automated drilling systems

KEY WORDS:
Drilling
OT system
Control system
Safety

VERSION
1.0

DATE
2023-02-06

AUTHORS
Maria Vatshaug Ottermo, Egil Wille, Knut Steinar Bjørkevoll, Lars Bodsberg, Tor Erik Evjemo, Kay Fjørtoft, Martin Gilje Jaatun, Thor Myklebust, Eivind Okstad

CLIENT
Petroleum Safety Authority Norway

CLIENT'S REFERENCE
Kristian Solheim Teigen

PROJECT NUMBER
102025164

NUMBER OF PAGES AND APPENDICES:
62+ Annexes/appendices

SUMMARY

This work is a preliminary study of how incidents, near misses and deviations within automated systems are currently detected, registered and, if appropriate, reported to the Petroleum Safety Authority Norway (PSA), as well as the roles of various actors in the processing of data from such situations. A task within drilling and well operations is used as a starting point, but information has also been collated on the reporting and handling of incidents and deviations in other relevant industries. Collectively, this provides a basis for proposing how the reporting of incidents and deviations in automated systems, control systems and interconnected solutions can be established and systematised in the petroleum industry.

The report is a translation of the SINTEF report 2021:01416 (in Norwegian).

PREPARED BY
Maria Vatshaug Ottermo

SIGNATURE
Maria Vatshaug Ottermo
Maria Vatshaug Ottermo (9. mar. 2023 12:03 GMT+1)

CHECKED BY
Ranveig Kviseth Tinmannsvik

SIGNATURE
Ranveig Kviseth Tinmannsvik
Ranveig Kviseth Tinmannsvik (9. mar. 2023 19:27 GMT+1)

APPROVED BY
Anita Øren

SIGNATURE
Anita Øren
Anita Øren (10. mar. 2023 10:39 GMT+1)

REPORT NUMBER
2023:00191

ISBN
978-82-14-07960-9

CLASSIFICATION
Unrestricted

CLASSIFICATION THIS PAGE
Unrestricted

History

VERSION	DATE	Version description
1.0	2023-02-06	Translation of SINTEF report 2021:01416

Image crediting:
Cover page: Equinor
Other: Pixabay

Contents

Executive Summary

Introduction

The purpose of this report has been to provide the industry and the PSA with increased insight into how incidents, near misses, and situations/deviations in automated systems are detected, registered, classified, processed and, possibly, further reported to the PSA today. This also includes the role of various vendors and companies in reporting and processing the incidents and deviations. The report is focused on drilling and well operations, but information about how incident reporting and processing is handled in other relevant industries has also been collected. This information is further used as a basis for proposing how to establish and systematise reporting of incidents and deviations in automated systems, control systems, and interconnected solutions in the petroleum industry.

The work is mainly based on document review, interviews, and a workshop as well as internal work meetings.

Background

According to the management regulations § 19 the responsible party shall ensure that data of significance to health, environment, and safety is collected and processed. Further, the activity regulations § 49, states that the maintenance effectiveness shall be systematically evaluated based on registered performance and technical condition data for facilities or parts thereof. The evaluation shall be used for continuous improvement of the maintenance programme, cf. § 23 of the management regulations.

But what about deviations or near misses that in other circumstances could have led to an incident or a dangerous situation? What data is collected and processed in cases where, for example, humans have to override the automated systems or for seemingly insignificant deviations that are not followed up systematically? Are we able to capture and utilize available data and information about such situations so that it can be used for future analysis and learning? Can experience from comparable industries where automated systems have been introduced be utilized for better reporting in drilling and well operations?

Automated systems in drilling

Automated drilling systems are installed on a few rigs but are gradually being introduced. Automated systems are used, for example, in pressure management (Managed Pressure Drilling - MPD), in top drive systems, and for control of drilling parameters. The report provides a brief overview of various automated systems used in drilling. In addition, an assessment is given of what data can and should be logged for these automated systems to ensure that sufficient meaningful information is available about a possible incident or near miss.

Handling of incidents in drilling operations

A simplified process flow for handling an incident or near miss, from the time it occurs until it is detected, registered, classified, analysed, and followed up is used as a basis for this part of the report.

The interviewees expressed concern about the fact that increased reporting could lead to additional workload on the driller and that this could divert attention from the already complex drilling process. It is important to avoid a situation where increased focus on reporting minor issues results in inadequate handling of more serious incidents. Automated reporting and possible filtering of incidents and near misses is therefore desirable. Another important conclusion from the interviews and the workshop with the industry is that there is currently no standardized way of reporting that can facilitate sharing of information across company borders. Furthermore, there are no well-established company-internal requirements that describe which incidents and near-misses to report and how to report them.

How to gather and systematise knowledge about incidents and near misses and utilize it for learning and improvement?

One of the goals of this report has been to propose how to gather and systematise the knowledge about incidents and near misses. The proposals include the use of a standardised reporting system as well as more detailed and standardised taxonomies for incidents to enable automatic reporting and classification, as well as facilitating increased sharing of data across company borders. In order to make the industry work together on improvement and collaboration projects, it may be considered to establish a joint forum for vendors and companies with a special interest in drilling and wells.

Recommendations

Ten recommendations have been given for the industry, five of which focus on which incidents are reported and shared, while the rest concern how the incidents are reported and followed up. Four recommendations have been made for the Petroleum Safety Authority Norway, two of which are related to standardised reporting and classification and two concerning training and drilling workload, respectively.

We see a need to establish new and standardised ways of collecting, analysing, and sharing data and knowledge to ensure interoperability and future learning. In addition, there is a need to gather information about how to facilitate more automated reporting.

1 Introduction

1.1 Objectives and purpose

This work is a preliminary study of how incidents, near misses and deviations within automated systems are currently detected, registered and, if appropriate, reported to the Petroleum Safety Authority Norway (PSA), as well as the roles of various actors in the processing of such situations. In this context, 'actors' means the various companies that are involved in the drilling process (e.g. drilling contractors, drilling vendors, operator companies, etc.). A task within drilling and well technology is used as a starting point, but information has also been collated on the handling of incidents in other relevant industries. Collectively, this provides a basis for proposing how the reporting of incidents and deviations in automated systems, control systems and interconnected solutions can be established and systematised in the petroleum industry.

SINTEF's secondary goals for the assignment

The following secondary goals linked to ICT incidents and near misses were given special consideration in the assignment:

1. Present an overview of and assess how ICT incidents and near misses are processed [1], with a special emphasis on drilling and well technology.
2. Present an overview of and assess how ICT incidents are processed in other industries where automation and autonomy are in use or close to commercial realisation.
3. Present an overview of and assess the role of different actors in the processing of ICT incidents and near misses, including actors other than operator companies which have a reporting obligation with respect to the PSA.
4. Consider the extent to which the current processing of ICT incidents and near misses is sufficient to provide meaningful information that can be used for learning and future risk reduction.
5. Propose how we can establish and systematise the processing of ICT incidents and near misses in the petroleum industry, including whether they can be described as defined situations of hazard or accident (DSHA) or similar.

In the following, we use *industrial ICT systems* as a collective term for both automated and industrial control systems.

1.2 Limitations

The assignment is limited to ICT systems in drilling and well operations. When collating information from the industry, we chose to use a broad definition of the term 'ICT incident'. This reflected our desire to capture as many examples of incidents, near misses and deviations as possible. This means that it is not only the incidents that are typically reported to the PSA that are included, but also near misses which could have had a different outcome under other circumstances. It is therefore not the well incident itself that is the focus of attention, but rather errors (and weaknesses) in automated systems as a triggering or contributory cause of the incident (e.g. due to lack of detection, provision of confusing information to crew, incorrect response, etc.). Cases where software or the interaction between software and the user does not function as desired/expected are also covered. This could be anything from configuration errors, sensor data errors and user errors, to software bugs and cyber attacks. The assignment also includes passive automated decision support systems which advise the drilling team during operations. Systems that are particularly relevant in this context include pressure control during MPD and automated tripping, as these are pivotal operations where systems with a high degree of automation are often used.

[1] We use *processing of ICT incidents in industrial ICT systems* as a common expression to refer to recording, quality assurance, analysis, reporting, learning, and notification of the PSA of incidents and near misses.

An example is a well control incident ("Mærsk Gallant") where sensor failure led to excessive opening of the automatically controlled MPD valve, which in turn caused the well pressure to drop excessively until the drilling team understood the situation correctly.

1.3 Terms, definitions and abbreviations

1.3.1 Terms and definitions

Definitions are used to ensure that we have an equal understanding of key terms, but definitions can in themselves limit the understanding of a term, and there are often multiple definitions of the same term.

Table 1 Terms and definitions.

Term	Definition/description	Reference
24-7/ 24-hour meeting	Daily meetings during which the last and next 24-hour periods are discussed	This report
Deviation	Perceived functioning of an ICT system which is not in accordance with the intended function	This report
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, individually and collectively.	PSA 2020 (ptil.no) [1]
Emergency preparedness	Technical, operational and organisational measures that are planned to be implemented under the management of the emergency organisation in case hazardous or accidental situations occur, in order to protect human and environmental resources and economic values.	NORSOK Z-013:2010 [2]
Cybersecurity	Protection of ICT systems against ICT attacks which could impact on the confidentiality, integrity and availability of ICT systems. (Note: In some standards, the term also includes unintentional incidents)	IEC 62443 [3]
Defined situations of hazard and accident (DSHAs)	A collection of possible observable incidents which the companies must defend against in order to pursue prudent petroleum operations	Guidelines to Section 73 of the Activities Regulations [4]
Drillers forum	Forum where drillers and others meet regularly to share and discuss experiences.	This report
Drilling recorder	System that logs all time series data, commands, operations, screens and alarms during the drilling operation.	This report
Experience transfer system	Sharing of observations and experiences with relevant parts of an internal organisation or external actors	This report
Hazard	An unintentional, undesirable event	NSM 2015 [5]

Term	Definition/description	Reference
Incident	An incident is either an accident or a near miss/incident.	Bridges [6]
ICT	All systems that perform their function by transmitting, receiving, storing, processing and converting information from other systems	Office of the Auditor General, document 3:7 (2020-2021) [7]
ICT incident	An incident that could affect the confidentiality, integrity and availability of ICT systems. ICT incidents include both intentional actions and unintentional incidents	Office of the Auditor General, document 3:7 (2020-2021) [7]
ICT security	Protection of ICT systems, the interaction between the systems, the services provided by the systems, or information processed in the systems. ICT security includes the protection of all ICT equipment and digital equipment, including operational control systems	Office of the Auditor General, document 3:7 (2020-2021) [7]
Information Technology (IT)	Technology that processes information	This project
Near miss	A near miss is an unplanned sequence of events which could have caused damage if the circumstances had been different or if the incident had been allowed to develop, but did not do so in this case	Bridges [6]
Newsletter/Bulletin	Concise publication containing news, analysis, and comments on topical incidents or outcomes	This report
PDS forum	Professional industry forum concerning the reliability of instrumented safety systems in the petroleum industry	SINTEF [8]
PDS method	Method for reliability analysis of instrumented safety systems	SINTEF [9]
Risk	'Risk' means the consequences of the activity and its associated uncertainty	Guidelines to Section 11 of the Framework Regulations [10]
Safety alert	Concise information concerning safety observations or an incident which is disseminated to relevant parts of the organisation.	This report
Safety	Safety means protection against hazards and threats which could cause undesirable incidents	NOU2015: 13 [11]
Stand	A stand is normally two or three drill pipes which are screwed together. These are ready for use in tripping in connection with drilling operations. One stand is approx. 30 m.	This report
Surge	Overpressure in a well caused by the drill string being lowered into the well too rapidly	This report
Swab	Underpressure in well caused by the drill string being withdrawn from the well too rapidly	This report
Taxonomy	The science of classification, i.e. dividing objects or concepts into classes	Britannica [12]
Incident	See near miss	Bridges [6]
Threat	An intentional undesirable act	NSM 2015 [5]
Accident	An accident is a sequence of unplanned events and circumstances which result in damage to the environment, process, product or reputation and/or injury to people.	Bridges [6]

1.3.2 Abbreviations

Table 2 Abbreviations.

Abbreviation	Description
ADC	Automated Drilling Control
AF	Activities Regulations
APOS	Automated process for follow-up of instrumented safety systems (SINTEF project 2019-2022)
ASR	Annual Status Report
CMMS	Computerized Maintenance Management System
DDR	Daily Drilling Report
DDRS	Daily Drilling Reporting System
DSHA	Defined Situation of Hazard and Accident
HAZID	Hazard Identification
HSE	Health, Safety and Environment
JRCC	Joint Rescue Coordination Centre
IACS	Industrial Automation and Control Systems
IEC	International Electrotechnical Commission
IF	Facilities Regulations
ICT	Information and Communications Technology
IMS	Information Management System
SIP	International Standardization Organization
IT	Information Technology
NEK	Norwegian Electrotechnical Committee
NOG/NOROG	Norwegian Oil and Gas Association
NORSOK	The Norwegian shelf's competitive position
NOU	Norwegian Official Reports
NS	Norwegian Standard
NSM	National Security Authority
NTSB	National Transportation Safety Board
ODR	Organisational Data Risk
OT	Operational Technology
PSA (Ptil)	Petroleum Safety Authority Norway (Petroleumstilsynet)
RF	Framework Regulations
RNNP	Risk level in Norwegian petroleum activity
ROC	Rate of Change
SAR	Search and Rescue
SAS	Safety and Automation System
SF	Management Regulations
SIS	Safety Instrumented Systems
SJA	Safe Job Analysis

1.4 Methodology and implementation

The work was primarily based on a document review, interviews, internal working meetings, and a half-day workshop with the industry. It was carried out by a multidisciplinary project team with expertise in instrumented safety systems, ICT security, drilling and well operations, learning after incidents, 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. Nine group interviews were conducted with a total of 37 interviewees. The main topics covered by the interviews were:

- Types of incidents relating to automated drilling systems
- Notification systems, collection and classification
- Actors and framework conditions for reporting

A half-day workshop was also conducted with a total of eight representatives from oil companies, drilling companies and drilling vendors. The theme of the workshop was:

- What incidents and near misses in automated drilling systems should be reported?
- How should incidents and near misses in automated drilling systems be reported (actors and framework conditions)?
- What are the critical factors for implementation?

1.5 Report structure

Chapter 2 summarises the findings of previous studies concerning the reporting of incidents and near misses, the requirements stipulated in the PSA's regulations, as well as relevant standards and guidelines.

Chapter 3 provides a brief insight into automated systems in drilling and what relevant data can/should be logged for the various systems.

Chapter 4 summarises the findings of interviews and workshops with the industry and looks at details relating to what incidents and near misses are reported, and how they are detected, reported, classified, followed up and analysed.

Chapter 5 discusses some factors that should be taken into account in connection with the further development of reporting systems, as well as the difference between reporting/investigation and measures/learning.

Chapter 6 summarises SINTEF's recommendations regarding measures within the industry and the PSA, as well as the need for further work relating to knowledge acquisition.

There are six appendices (A-F). These appendices look in more detail at the reporting systems that are in use in industries other than drilling, including aviation, road transport, shipping, railways, power supply, and the water and wastewater sectors.

In addition to figures and tables, we use fact boxes (green boxes on the left-hand side of the page). Fact tables are also green, while result tables are blue.

2 Background

In accordance with the Management Regulations, Section 29 Notification and reporting of hazard and accident situations to the supervisory authorities [13], operators must notify the Petroleum Safety Authority Norway in the event of hazard and accident situations. Amongst other things, the guidelines state the following: "*b) well control incidents"* and "*i) situations where normal operation of control or security systems is disturbed by unplanned work (ICT event)"*. But what about all those situations where a hazard or accident situation could have arisen under different circumstances? Are we able to adequately capture the available data and information about such situations so that we can use it for future analysis and learning? Figure 1 shows examples of various factors which can influence whether we are able to capture and utilise data concerning incidents and deviations effectively.

Figure 1 Factors which can influence whether we are able to capture and utilise data from incidents and near misses.

Studies in several industries indicate that there are between 50 and 100 near misses for every accident.

There are perhaps 100 erroneous acts or conditions for every near miss.

This gives a total population of roughly 10 000 errors for every accident.

Bridges 2012 [7]

Studies in a number of industries suggest that there are between 50 and 100 near misses for every accident [6]. In modern and automated systems, this number may be even higher due, for example, to the use of beta software. When such deviations or incidents occur in autonomous and automated systems, they cannot always be readily resolved on site. For these cases, sufficient available data must be available to enable the incident to be analysed afterwards, enabling future undesirable incidents to be prevented before they occur. Even if such incidents can be resolved on site, the information needed for systematic improvement and learning should be secured. But what exactly is "sufficient available data"?

This report will provide assessments of *what data can and should be* logged for security-critical automated systems, to ensure that sufficiently meaningful information concerning security-critical events is available. This also involves assessing what information concerning incidents and near misses different users and roles in automated systems can contribute.

Figure 2 illustrates that there may be untapped learning potential from incidents, near misses and deviations in automated systems, and it is some of these that this report seeks to identify. In some cases, even minor changes in circumstances can mean the difference between a near miss and an incident, or between a

deviation and a near miss. It is therefore worth noting that a given learning potential is not necessarily "reserved" for one of the categories.

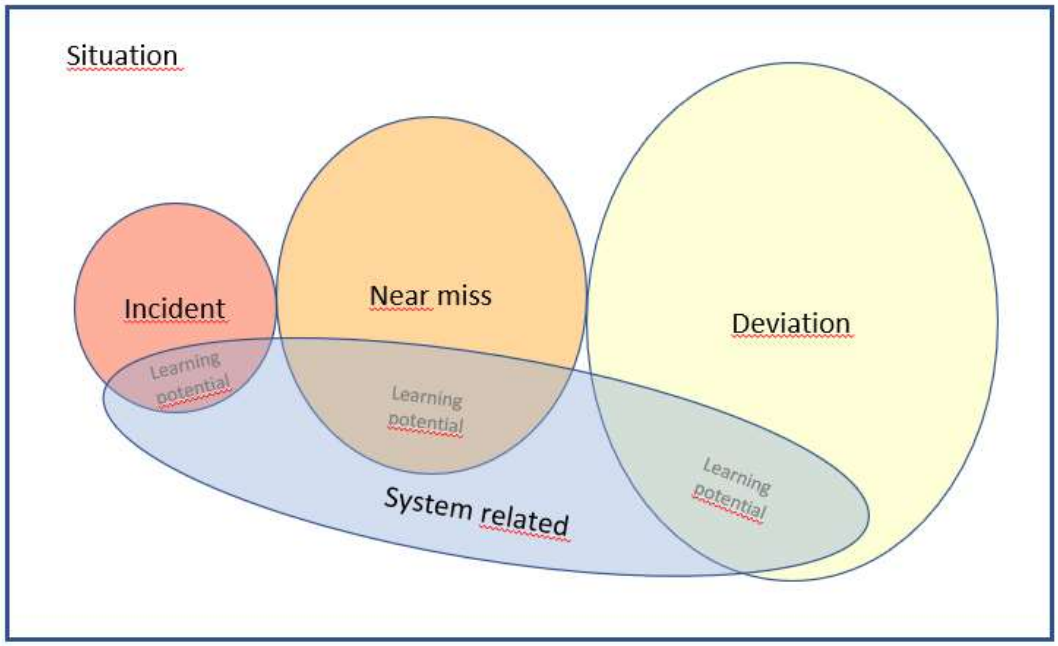


Figure 2 Visualisation of learning potential relating to deviations, near misses and incidents.

2.1 Findings of previous studies

2.1.1 Automation and autonomous systems: Human-centred design in drilling and wells

The report entitled "Automation and autonomous systems: Human-centred design in drilling and wells" [14] was prepared on behalf of the PSA in 2020. There is uncertainty as to whether current users of autonomous drilling systems possess sufficient experience and knowledge of the technology in order to determine the types of incidents and near misses that should be reported as expressions of concern, and whether such systems are used sufficiently. The authorities also do not systematically collect data concerning less critical near misses, and it is therefore uncertain whether these situations are captured through the reporting of DSHAs or other RNNP reporting points.

Of the five measures covered in this report, the measure referred to above points to factors that are of particular relevance to this report: “Ensure systematic data reporting and facilitate the analysis of operations”. This measure was based on findings from investigation reports, workshops with actors from the PSA, SINTEF and industry experts, as well as a literature review. The investigation reports concerned were linked to various industries, including drilling and well operations, unmanned metro systems, autonomous road transport, as well as autonomy in shipping and aviation, where, with some exceptions, systematic data reporting and documentation were in use, especially concerning minor incidents. For example, in an investigation into an accident linked to autonomous cars by the National Transportation Safety Board (NTSB), it was pointed out that it was challenging to gather data for the accident analysis. As a result, one of the NTSB's recommendations was that data collection and reporting from autonomous systems should be given greater priority and a stronger focus. Other reports also pointed out that there were no taxonomies for data reporting. Taxonomies will be discussed in more detail in Chapter 2.4.7. In cases where systematic data reporting and documentation were available, or at least partially available, it was concluded that continuous data collection and reporting from sensors in the autonomous system both before and during the incident contributed to understanding, learning and measures [14].

One of the main conclusions of the workshop held as the basis for the report [14] was that "near misses are not being adequately captured by either the authorities or companies". There are currently limited requirements in place regarding what must be logged concerning incidents and near misses involving automated systems in the oil and gas industry, or how such data should be handled in connection with reporting and learning. It was therefore recommended that the authorities and the industry work together to establish requirements regarding which data should be logged for safety-critical automated systems. The report also noted that data collection is generally inadequate at both operator level and authority level. This may indicate that the need for detailed reporting and collection of historical data has not been assessed prior to an incident. This could lead to a lack of data and experiences from near-accidents, which in turn could lead to a lack of important information for use as a basis in risk-based supervision. Failure to report automation errors may also lead to a failure to achieve a correct and appropriate level of trust in the automated systems. The right level of trust in the technology is important if the end user is to be able to adopt it effectively. In other words, a balance should be sought between trust (a belief that the technology is working as intended) and having a critical view of the technology [15].

The study also pointed out that the operational time period is often much shorter in drilling operations than in the case of production processes, so that standard reporting and follow-up can take place on a daily basis or for each shift through a "Daily drilling report" and a "Daily mud report". Less serious incidents will be reported there without initiating a more comprehensive process, and it can be a challenge that those who submit reports have little knowledge of the automated systems and can therefore easily misinterpret, report errors or perhaps underreport where people take over and recover situations.

2.1.2 Use of models in drilling

On behalf of the PSA, SINTEF examined various aspects of the topic of ICT security – Resilience in the petroleum sector in 2020 [16]. The aim of one of the six subprojects in this assignment was to discuss challenges and opportunities associated with the use of models in drilling operations, particularly as regards how the models and data from the models can be used in a safe manner and how ICT security is addressed [17]. This work was primarily based on a document review, interviews and working meetings. Some relevant findings from this work which indicate the importance of putting a spotlight on the reporting of incidents for automated solutions were:

- Introducing new technology based on models (and automated solutions) also introduces new vulnerabilities which need to be followed up and addressed. However, it is necessary to also be aware that drilling using conventional solutions, where the systems are operated right up to the tolerance limit, can often be more dangerous.
- To ensure that models (and automated solutions) work as intended, they must be tested, verified, and validated. It will often be a challenge to identify all the possible scenarios to which a model may be exposed. In addition, a log must be kept of the changes that have been made to the models and automated systems, who made them and when. Such a history will make it easier to correct and identify both intentional and unintentional errors which have resulted in incidents.
- There is a need for more knowledge relating to the management of ICT incidents in connection with the use of model-controlled operations, along with a need for greater competence amongst professionals and management. There is also a need to collate more knowledge about how to drill and prepare employees and the organisation itself for such incidents.
- Models that are used for drilling often become so complex that it is difficult for users to have a complete overview and control over all the underlying calculations and processes. Having this overview often does not provide the user with any added value, particularly as models are increasingly being based on empirical data and the use of artificial intelligence, rather than physical models. Nevertheless, it is important that users do not lose their mental model of the process and

overall understanding of the system which 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.

2.2 Requirements regarding reporting in the PSA's regulations

In accordance with the PSA's Management Regulations, Section 19 [13] and the Activities Regulations, Section 49 [4], the responsible party must ensure that data that is of importance to health, safety and the environment is collected and processed, and that the efficacy of maintenance is systematically evaluated on the basis of recorded data concerning performance and technical condition. These sections refer to NS-EN ISO 14224 [18] and NS-EN ISO 20815 [19] (see the tables below). A separate section in the Management Regulations stipulates a requirement for drilling and well operations to be reported to the Petroleum Safety Authority Norway's and the Norwegian Petroleum Directorate's database.

SECTION - TOPIC	REQUIREMENTS
Management Regulations [SF] (and associated guidelines [13])	
Section 19 **Collection, processing and use of data**	The responsible party shall ensure that data of significance to health, safety and the environment are collected, processed and used for a) monitoring and checking technical, operational and organisational factors, b) preparing measurement parameters, indicators and statistics, c) carrying out and following up analyses during various phases of the activities, d) building generic databases, e) implementing remedial and preventive measures, including improvement of systems and equipment. Requirements shall be set as regards the quality and validity of the data, based on the relevant need.
Guidelines to Section 19	This section covers requirements for all types of data of significance to health, safety and the environment. Specific data requirements for various purposes are laid down in other sections of these Regulations, as well as in the Framework Regulations, the Technical and Operational Regulations, the Activities Regulations and the Facilities Regulations. To fulfil the data requirements as referred to in the first subsection (c) and (d), the ISO 14224 standard [18] should be applied for reliability and maintenance data for risk analyses within the field of health, working environment and safety if the position of the facility makes this possible. If two independent notification paths via fixed communication networks cannot be realised, one of the notification paths can be replaced with communication via the maritime mobile service.
Activities Regulations [SF] (and associated guidelines [4])	
Section 49 **Maintenance effectiveness**	The maintenance effectiveness shall be systematically evaluated based on registered performance and technical condition data for facilities or parts thereof. The evaluation shall be used for continuous improvement of the maintenance programme; see Section 23 of the Management Regulations.
Guidelines to Section 49	Maintenance effectiveness as mentioned in the first subsection, means the ratio between the requirements stipulated for performance and technical condition and the actual results. The standards NS-EN ISO 14224 [18] and NS-EN ISO 20815, Appendix E [19], should be used when registering data as mentioned in the first subsection, including failure data and maintenance data.

Management Regulations [SF] (and associated guidelines [13])	
Section 38 **Reporting drilling and well activities**	The operator shall report drilling and well activities to the Petroleum Safety Authority Norway's and the Norwegian Petroleum Directorate's database. The reporting shall use the well and wellbore terminology as well as the classification as mentioned in Section 10 of the Regulations relating to resource management in the petroleum activities.
Guidelines to Section 38	The reporting shall be in accordance with the criteria, the deadlines and the format provided in the user guidelines for the DDRS database as mentioned in the first subsection.

2.3 Defined situations of hazard and accident

Defined situations of hazard and accident (DSHAs) constitute a representative selection of hazard and accident situations used in the dimensioning of emergency preparedness (see the guideline to Section 73 of the Activities Regulations - Establishment of emergency preparedness [4]). These are facility- and location-specific, i.e. there is no fixed list of DSHAs. The Activities Regulations, Section 73, refers to the Management Regulations, Section 17 Risk analyses and emergency preparedness assessments, and in the guidelines to the Management Regulations, Section 17, reference is made to NORSOK Z-013 [2]. NORSOK Z-013 Annex C (informative) contains checklists for hazard identification (HAZID) which can be used as a basis. An emergency preparedness plan will normally contain in the range of 15-20 DSHAs (hydrocarbon leaks, fire and explosion, acute pollution, etc.), depending on how specific they are. For each DSHA, the emergency preparedness plan contains action plans that specify who (responsible) must do what (action), and when (emergency preparedness phase).

Notification constitutes the first of five emergency preparedness phases (see Section 77 Handling hazard and accident situations [4]). In many cases, it will be critical that the notification is given immediately in order to meet the requirements regarding emergency preparedness. Although the needs are somewhat different for the various DSHAs, for most DSHAs, it will be necessary to notify the rescue helicopter service, the Joint Rescue Coordination Centre (JRCC) in the north or south, and the second line emergency preparedness management within the company. This will normally be carried out as quickly as possible, preferably specified by time requirements (e.g. within three minutes for SAR, and within 10 minutes for the Joint Rescue Coordination Centre (JRCC) and second line). Many companies have hired an emergency preparedness team, who then makes up the second line [20].

The failure or loss of a power supply is often included as a DSHA by operating companies, but the interview study indicates that incidents within automated systems are not treated as a DSHA.

2.4 Standards and guidelines

In the following, reference is made to some relevant standards and guidelines for reporting HSE incidents and technical condition in automated drilling operations.

2.4.1 NS-EN ISO 14224

NS-EN ISO 14224 [18] provides a basis for the standardised collection of reliability and maintenance data for equipment in the petroleum sector, including equipment for drilling operations. Amongst other things, the standard defines the breakdown and classification of equipment, as well as failure modes, cause of failure and detection methods.

ISO 14224 (Appendix D-5) [18] distinguishes the following data sources for the establishment of reliability data:

1. Generic data (databases and manuals) based on operational experience of similar equipment
2. Company-specific data based on operational experience of the company's own equipment
3. Manufacturer data based on operational experience from the equipment vendor
4. Expert reviews based on statements from technical experts
5. Data concerning human error (e.g. ISO/TR 12489:2013, Annex H.2 [21])

2.4.2 IEC 615011/IEC 61508

The overall use of failure data is discussed in IEC 61511-1 [22], Sections 11.9.3 and 11.9.4. According to IEC 61511-1, reliability data used in quantifying the effects of random failures must be credible, traceable, documented and justified.

2.4.3 Norwegian Oil and Gas Association 070

In particular, the PSA refers to the guideline: "070 Norwegian Oil and Gas Association Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry (Recommended SIL requirements)" [23] in its regulations. The overall purpose of the guideline is to standardise and simplify the application of IEC 61508 [24] and IEC 61511 [22] in the Norwegian petroleum industry.

The guideline has a specific section 8.5 "Requirements to Failure Data", which largely refers to ISO 14224 [18].

2.4.4 SCSC-127E Data Safety Guidance

The Safety-Critical Systems Club (SCSC) [25] has issued guidance concerning the handling of safety-related data which can provide a useful basis in the development of reporting systems for autonomous systems.

The guidance represents best practice regarding how data (as opposed to software and hardware) should be handled in the context of safety. The purpose is to help organisations identify, analyse, evaluate and manage data-related risks, and thereby reduce the likelihood of data-related problems causing undesirable incidents. The guidance gives several examples where 1) *errors in data*, or 2) *inappropriate use of data* in automated systems has contributed to accidents. An example of the inappropriate use of data is a ship navigation system which, when displaying a broad field of view of chart data, removes shallow underwater features and thus also removes important safety-related information due to the image scale.

The guidance identifies a broad spectrum of safety-related data and data properties (such as accuracy and availability) which must be maintained in order for the system to function safely (see Appendix B to the guidance). It is not limited to performance data during operation, but it does specifically deal with how data concerning industrial control systems stored in IT systems can impact on the functional safety of industrial control systems (e.g. erroneous alarm limits registered in the industrial control system).

The guidance contains a set of questions for assessing organisational data risk (ODR) which include the severity of potential accidents, organisational maturity, legal framework, size, complexity and innovative features of the system. It results in a ranking from ODR0 (lowest risk) to ODR4 (highest risk), and thus the effort required to manage the data security risk. Part of the process is to understand the organisational culture, and a short questionnaire has been developed concerning data security culture (Appendix C to the guidance), which can help in this aspect.

The document is intended to be used as a supplement to existing standards and norms and is adapted to the structure of ISO 31000 [26]. Like IEC 61508 [24], the document was written for a number of sectors and must be adapted to the individual sector concerned. We are aware that there is a proposal that the new revision of the IEC 61508 standard should refer to this guidance.

Data security, data sources and data flow in the offshore industry are also discussed in the article entitled "Data safety, sources and data flow in the offshore industry" [27].

2.4.5 NORSOK D-010:2021; Well integrity in drilling and well operations

NORSOK D-010:2021 [28] has a specific section 5.10 "Experience transfer and reporting", which concerns how well activities and operations must be documented and made available for future use and continuous improvement. The document only provides overarching requirements regarding the reporting of incidents which are of importance to health, safety and the environment, and therefore contains limited information on how to classify incidents or establish a reporting system for automated systems.

The experience transfer and reporting system should comprise of:
-drilling and well activities reporting system;
-accident and incident reporting system;
-non-conformity/deviations/management of change;
-end of well/activity/operations reports;
-risk register for monitoring of risks;
-special reports addressing particular events or issues on the well;
-well Barrier Envelope status
-well design limits (Maximum Allowable Annulus Surface Pressure] for pressure on each casing annulus

NORSOK D-010:2021[28]

2.4.6 NORSOK I-002:2021 Industrial automation and control systems

NORSOK I-002:2021 [29] includes a specific section 8.2.2.2 "Data collection and storage", which requires industrial ICT systems to be able to record and report time-stamped process values, event data and calculated data, in addition to system and application data.

The IACS shall be capable of storing all collected data for 90 days or more without loss of data during normal operations.

The IACS shall be able to collect and store all data when the facility is performing a safety shutdown.

The IACS shall keep the data time stamp from the data source and if that is not available the IACS shall time stamp the data at entry.

NORSOK I-002:2021 [29]

2.4.7 Guideline PDS Forum/APOS

There is often uncertainty over the quality of maintenance and incident data which has been collected. An important starting point for eliminating some of this uncertainty is to ensure that failures are recorded in a consistent manner. By defining standardised equipment groups with well-defined system delimitations and facilitating a high level of confidence in the selection of parameters for failure recoding, e.g. for failure mode and detection method), it is possible to achieve consistent registration [30]. ISO 14224 [18] is currently actively being used in the acquisition of reliability and maintenance data for safety equipment in the petroleum sector. However, as a result of work under the auspices of the PDS forum[2], it has become apparent that there is a need for guidance, examples and explanations which can simplify the current application of ISO 14224 [18]. With support from the Research Council of Norway through the project "Automated process for follow-up of safety systems", SINTEF has therefore published guidelines for the standardised reporting of the classification of failures in instrumented safety systems in the petroleum sector [30]. These guidelines will also be relevant for failure reporting and the classification of drilling equipment. SINTEF's guideline is based on ISO 14224 [18] with a view to further standardisation and streamlining of the process for failure reporting and classification of safety equipment. A principal goal has been to operationalise and simplify taxonomies (classifications) and provide examples, descriptions and illustrations relating to parameter selection:

More specifically, this guideline is expected to contribute to:

- More efficient and better reporting of incident data by providing simpler and more intuitive taxonomies.
- More automated failure recording, classification and analysis. In connection with this, common taxonomies and reporting formats will be crucial.
- An improved framework for failure analysis and the implementation of measures.
- Easier and better provision for data sharing and comparison, between operators, between operators and vendors, and as input to the PSA (i.e. RNNP).
- Integration and application of automated failure reporting systems (IMS, ASR, condition monitoring systems, etc.).
- Greater trust in, and therefore better utilisation of, the data for learning purposes.

Standardised failure reporting is relevant for:

- Personnel who are responsible for developing and configuring information, maintenance and reporting systems (including both operators and vendors).
- Personnel who perform maintenance and write notifications.
- Personnel who classify and/or quality-assure incident data.
- Personnel who perform data analysis and further follow-up.

To simplify failure recording and classification, algorithms that can reduce parameter selection are proposed. An example is a limit on the number of possible failure modes based on equipment type, e.g. if a gas detector is selected, only failure modes relevant to gas detectors are included.

Some examples are presented below of standardised equipment groups, as well as recommended taxonomies for detection method and failure mode.

[2] *PDS forum is a co-operation between more than 20 participants representing oil companies, engineering oil companies, consultants, vendors and researchers, with a special interest in safety instrumented systems. The participants meet twice a year for workshops, presentations and technical discussions.*

2.4.7.1 Standardised equipment groups

The grouping of safety-critical equipment with comparable characteristics is important in order to:

- Structure failure data; equipment groups define how failures can be aggregated and combined with the aim of estimating equipment failure rates.
- Enable standardised (and equipment-specific) taxonomies and automated registration and classification of equipment failures in a group.
- Compare, combine and analyse data from different facilities and/or operators.
- Enable efficient and standardised operational follow-up of a facility (at an appropriate level).

SINTEF's guidelines [30] propose that equipment be grouped hierarchically into three levels (see the example for gas detectors in Figure 3). This structure is derived from analyses of current industry practice, international standards, expert assessments and identified needs and requirements for the subsequent use of data.

Main Equipment groups – L1	Safety Critical Elements (subgroups) – L2	Equipment attributes – L3								Equipment attribute categories and *Comments*
		Measuring principle	Design/mounting principle	Actuation principle	Medium properties	Dimension	Location/ Environment	Application	Diagnostics / Configuration	Test, maintenance & monitoring strategy	
Gas detectors	General – all gas detectors						x				**Location / environment:** location on installation (area, air intakes, etc.) and degree of weather, vibration, and temperature exposure
	Point HC gas detectors - catalytic										
	Point HC gas detectors – IR/optical		x					x	x		**Design/mounting principle**: Wired vs wireless, aspirated gas detector (flow monitoring switch or transmitter separately tagged) **Diagnostics/configuration:** Degree (in %) of self-diagnostic (*detector configuration important)* **Application:** cross duct vs open area (different response time requirements and configuration).
	Line HC gas detectors – IR/optical		x						x		**Design/mounting principle**: Traditional line detectors versus cross duct detectors (increased design / set-up complexity) **Diagnostics/configuration:** line monitoring only, self-verify in active use, state control – fault alarm and deviation from normal measurement value (*detector configuration important)*
	Line HC gas detectors – laser		x						x		**Design/mounting principle**: Traditional line detectors versus cross duct detectors (increased design / set-up complexity) **Diagnostic:** line monitoring only, self-verify in active use, state control – fault alarm and deviation from normal measurement value

Figure 3 Taxonomy for equipment groups [30].

2.4.7.2 Detection method

The classification of detection methods is important in order to distinguish between failures that are automatically notified (Detected) and failures that are notified manually (Undetected/latent) (see Figure 4). Failures that are notified through self-testing or condition monitoring are less critical, as corrective action can be taken immediately. On the other hand, undetectable/latent failures may be critical and prevent an intended safety function from engaging if an incident occurs before the failure is detected and corrected. These failures can be detected by both scheduled and unscheduled maintenance.

SINTEF's guidelines [30] propose a flexible and hierarchical taxonomy which both unites different company practices and is at the same time compatible with ISO 14224 [18].

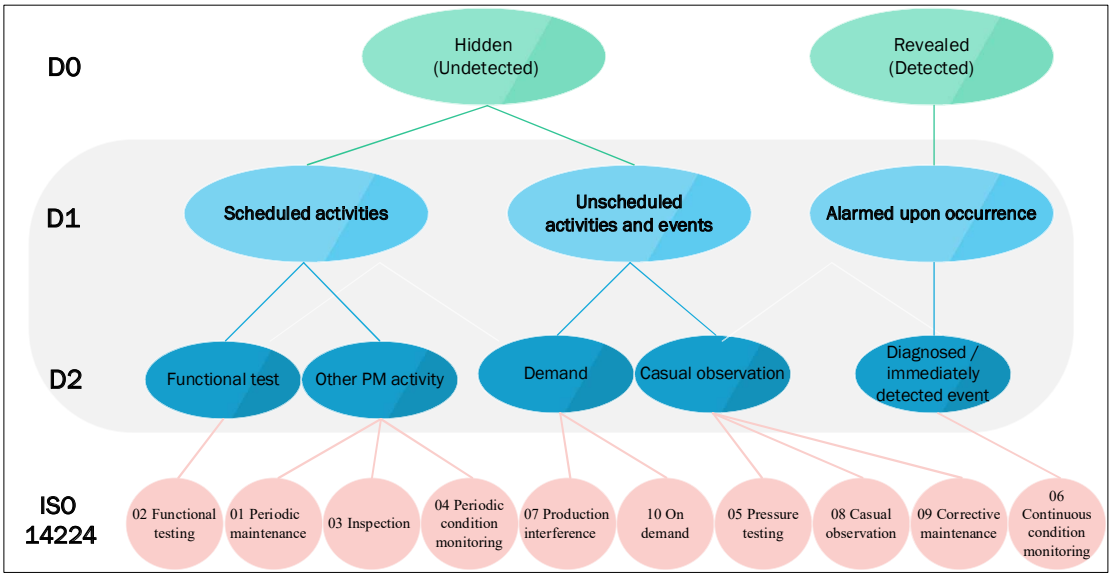


Figure 4 Taxonomy for detection method [30].

2.4.7.3 Failure modes

Failure modes describe the effects of failures on a system's performance. Important failure modes for safety equipment are:

- Dangerous failures ("Dangerous"): Loss of safety function (e.g. fire pump does not start).
- Maintenance-related failures:
    - Safe failures ("Safe/spurious"): Accidental triggering of safety function (e.g. false alarm from gas detector).
    - Non-critical failures ("Non-critical"): No impairment of safety function (e.g. valve can close if necessary, but must be repaired due to other circumstances). Can often be decisive for production.
    - Other failures: For some types of equipment, there will be different safety-critical failure modes compared with the primary safety function (e.g. leakage from valves or failure of ignition source protection).

SINTEF proposes a hierarchical equipment-specific taxonomy for failure modes for safety equipment (see Figure 5). The use of a few, carefully selected failure modes for each equipment group will simplify reporting, and thus improve both the quantity and quality of reporting. In other words, when selecting a Level 1 failure mode, the number of relevant Level 2 failure modes will be limited. The list of Level 2 failure modes will be complete in the sense that the failure modes "Other" and "Unknown" are avoided, and that an attempt will instead be made to capture all possible relevant failure modes for a specific equipment type.

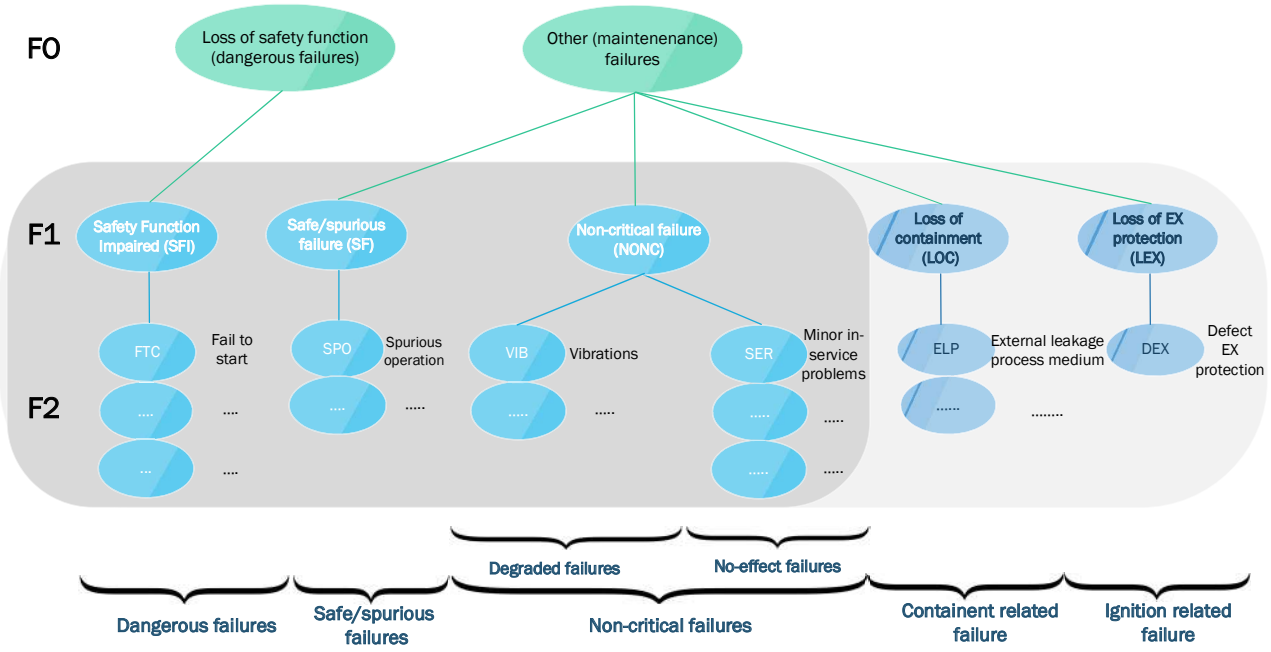


Figure 5 Taxonomy for failure modes [30].

Automatic user guidance is recommended to help with the correct choice of parameters, such as using pop-up windows, mouse-overs and pre-populated selections. Such help texts could, for example, appear in the maintenance system where the failure message is registered, or secondarily in the operating procedures associated with error reporting and classification. The automatic generation of some parameters is another suggested simplification. For example, once the detection method and failure mode have been selected, the error class could be determined automatically, and thus maintenance priority (high, medium, low) can also be suggested; see the examples in Figure 6 [31].

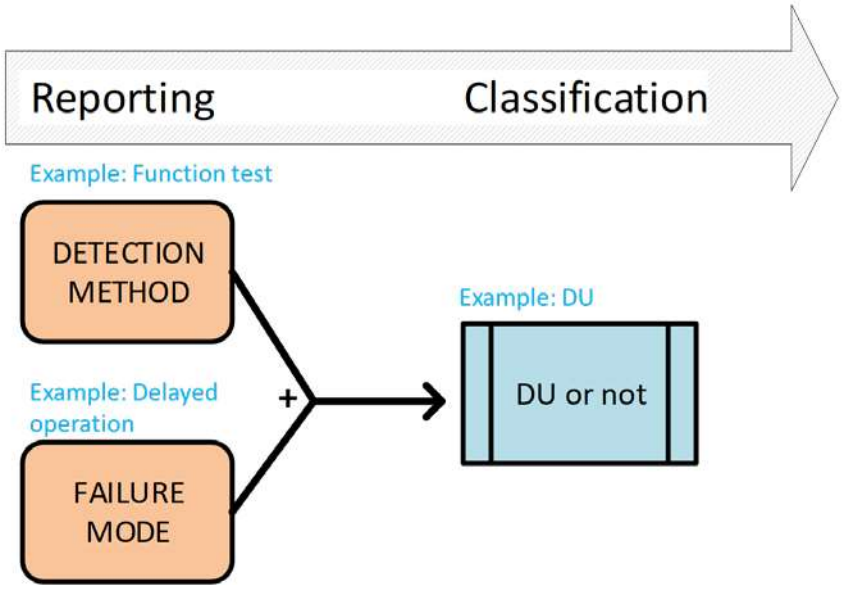


Figure 6 Potential for automatic failure classification [31].

2.4.8 Industry 4.0

Many items of equipment are installed on drilling facilities to assist with the drilling process and prevent hazardous incidents. To ensure good follow-up of this equipment, we must collect data about it and, in particular, establish knowledge about how to use and share data and information in order to create value. Traditionally, company- and discipline-specific solutions, tools and proprietary formats have prevented the sharing of information and data. However, as machines, products and facilities become smarter, they need to be able to communicate autonomously in digital global networks [32]. For many years, Germany has been conducting intensive research and development within this domain, and is a world leader in the field of integration of individual system solutions through their Industry 4.0 initiative. The fundamental aim of Industry 4.0 is to enable seamless interoperability between objects in the physical world, thereby facilitating new levels of automation and productivity gains. The physical objects must therefore be virtually represented and connected, and Industry 4.0 does this by using a translator which is often referred to as the "digital twin" of the physical object. This digital representation of the object is known as an “Asset Administration Shell” (AAS). Some industries, such as the manufacturing industry, have progressed relatively far in defining and systematising properties and information regarding their equipment, but for the petroleum industry, there remains a need to define and develop open standards and solutions which facilitate a digital ecosystem for the entire value chain.

3 Automated systems in drilling

Automated drilling systems are still in use on a few rigs, but such systems are, for example, used for pressure control in Managed Pressure Drilling (MPD) and in systems that are used to control hoisting operations (e.g. automated tripping and connection and auto drillers which are available in a range of designs for optimisation of the drilling process itself). Table 3 describes key components and equipment used in drilling and tripping, as well as data that can/should be logged in order to facilitate the best possible detection and learning. Table 4 describes key control system functions used in automated operations, as well as what data these systems need in order to function optimally.

Table 3 Overview of drilling components and equipment, as well as relevant (sensor) data that can/should be logged.

System/component	Relevant data that can/should be logged
Drill string: A collective term for all pipes and equipment that connect to the top drive in order to carry out drilling. It is often divided into a drill bit, bottom hole assembly (BHA) and drill pipes. The drill bit does the actual drilling, while the drill pipes transport the drill bit and BHA in and out of the well, and transfer rotational forces from the top drive and transport drilling mud into the well. The BHA is the lower part of the drill string and includes a number of specialised components, including drill collar, equipment for controlling the drill bit, as well as measuring and logging equipment. Data from sensors in the BHA is transmitted either through the well itself and the drilling mud via electromagnetic or acoustic signals, or via a special type of drill pipe with a built-in signal cable, known as a 'wired pipe'. Signal transmission via a wired pipe is significantly more expensive, but it does make it possible to transmit data up to the drill floor with unparalleled bandwidth and latency, enabling parameters from the well to be measured and logged much more accurately and rapidly, providing a clearer and more accurate picture of conditions in the well.	A BHA normally includes many sensors, and loss of or errors in these measurements can be safety-critical, as less or inaccurate information will be received concerning conditions in the well. An example is sensors which measure well pressure or drilling mud density. Many of the measurements in the BHA and top side are important in order to limit wear on the drill bit and BHA, such as the weight on the drill bit, torque and vibrations. Unfavourable conditions can damage the drill bit and BHA components. These are not normally safety-critical events, but could, for example, result in a need for extra tripping and thus lead to an increase in overall risk. Should therefore be logged in order to obtain the overall picture.
Drilling mud: Drilling mud primarily serves as a tool for well control (by creating the necessary pressure at the bottom of the well in order to prevent kicks and blowouts), but it also lubricates and cools the drill bit (and string), and transports cuttings up to the surface through the annulus. The correct mud flow and pressure are achieved by controlling relevant pumps and valves, and adjusting the specific gravity of the drilling mud (density).	In order to obtain an overview of the properties of the drilling mud, a range of parameters is measured, including specific gravity (density), level/quantity, viscosity and temperature. It is common to measure the properties of the drilling mud using manual sampling, but a lot of work is also being done with regard to automatic measurement. In order to obtain more frequent measurement data (and thus better control of the drilling mud), automatic measurement of the drilling mud properties is desirable.
Casing: The well is reinforced in sections by lowering casings (also known as liners) into the well and cementing them in position permanently. To prevent collapse of the well wall, casings ensure that gas and liquid do not seep out of or into the well.	Few/no sensors directly linked to casings, but other well-related measurements can indirectly provide information on the condition of the lining.
Safety valves/BOP: Safety valves constitute an additional barrier against undesirable well incidents such as kicks and blowouts, and work by allowing one or more valves to "shut off" the well if well control cannot be maintained via the drilling mud. If there is a drill string in the	On the BOP, it is the status of valves and control hydraulics, as well as communication, that is most relevant. This is especially true for the parts of the BOP

System/component	Relevant data that can/should be logged
well, the safety valves can be closed around the drill string or cut it. In the case of managed pressure drilling, the safety valves in the BOP will take over from the MPD system, while a the same time maintaining a high pressure when an inflow from the reservoir into the well has been detected.	that are used by the MPD system. In addition, drilling mud pressure is measured in the annulus at the BOP
Risers and riser tension system: Risers are used as an "extension" of the well to transport drilling mud and cuttings from the seabed up to the surface. The riser also acts as a kind of "umbilical cord" for the safety valves on the seabed, in that dedicated lines and cables for hydraulic pressure and electrical power/communication are attached to the riser. There will be some relative movement between the riser and the drill floor due to movements/forces in the sea, as well as rig movements in the case of a floating facility. A riser tension system (riser tensioner) is therefore required to hold the riser tight with an almost constant force in order to prevent the relative movements from causing problems.	Key parameters/conditions for risers and tension systems are angles, forces and various status signals. This data is primarily influenced by forces of nature and rig movements, and is important for dynamic positioning (DP) and automatic disconnection sequences on the BOP. Riser data is less relevant for automated systems for drilling and tripping.
Heave compensator: In the case of floating facilities, there will be vertical movements between the drill floor and the seabed/well, which necessitate a system that compensates for these movements during drilling. Without such compensation, the drill bit would be subjected to substantial variations in bit weight, or even lifted up from and dropped onto the bottom of the well due to the facility's vertical movements (heave). Heave compensation can be achieved in a number of ways, e.g. by lifting the crown block up and down in counterphase with the heave movements, or by controlling the lift system in a way that compensates for the facility's movements.	For a heave compensating system, pressure/force, position, speed and acceleration are the most important measurements. Command and status signals are also relevant.
Drawworks: To raise and lower the top drive and drill string, a robust hoisting system dimensioned for the loads concerned is essential. The most common approach is to use a drawworks, which has a large drum which rotates in order to draw in or play out the drill line. In combination with a set of pulleys consisting of a crown block and travelling block, the drawworks creates the necessary lifting force. An alternative to drawworks is to use hydraulic cylinders to raise and lower the top drive and drill string. In such systems, one or more pulleys are attached to the top of the lifting cylinders, and the top drive is lifted by one or more cables which run from the attachment point(s) on the drill floor, over the pulley(s) and down to the top drive.	For drawworks, force (torque, hook load, etc.), position, speed and acceleration are the main parameters. These are measured either directly or indirectly in various ways. It is also important to maintain an overview of the temperature, command and status of brakes, motors and gears.
Top drive: A drilling machine which is hoisted up and down in the derrick, and makes it possible to support the load of the drill string and rotate it at the same time. The top drive (and drill string) is raised and lowered by the drawworks, and the vertical range (the distance from the lower position to the upper position) determines the length of stands (pipe sections) that can be used for drilling and tripping.	Vertical force (hook load), torque and rotational speed are important measurements. To prevent the top drive from being raised or lowered too far, a set of position sensors is also used (in addition to position measurements from the drawworks and heave compensator). Command and status signals are also relevant.
Pipe racking system: When the drill string is withdrawn from the well, it is necessary to store stands efficiently as they are removed from the drill string. When the string is to be run into the well, the stored sections must be retrieved and threaded onto the string. This pipe racking process involves interaction between a number of machines:	For the machines that are involved in pipe racking, it is especially their respective positions and velocities relative to each other, as well as pressures/forces, that are important.

System/component	Relevant data that can/should be logged
• Iron roughneck: Machine for screwing or unscrewing pipe connections. • Pipe racker: Machine (or machines) which transports stands to/from the well and to/from fingerboards (a place where stands are stored in the vertical position) • Fingerboard: The place where stands are stored is called a fingerboard. In addition to acting as a storage location, the fingerboard also keeps the pipes in position so that they cannot move or tip over. In addition to transporting stands between the well and fingerboard, the pipe racking system assembles and dismantles stands, and transports individual pipes between the pipe decks/pipe store and drill floor. These tasks involve even more machines, which must interact both with each other and with the iron roughneck and pipe stacks: • Pipe handling crane: Crane for transporting single pipes (in the horizontal position) between the pipe store and the catwalk machine. • Catwalk machine: Transports single pipes (in the horizontal position) between the pipe deck and the drill floor. • HTV machine: HTV stands for “horizontal-to-vertical”, and this machine lifts individual pipes out/up from the catwalk machine so that they go from being horizontal to being vertical. The vertical single tubes are then screwed together to form stands (using the iron roughneck) and transported to the fingerboard by the pipe stacker.	Various status signals for sensors, communication and hydraulic and power supply are also relevant, in order to detect problems which could for example lead to a stoppage or collision.

Table 4 Key control system functions for automated drilling and tripping.

Function	Important input data
Managed Pressure Drilling (MPD): There are various variants/-concepts in use for managed pressure drilling. Common to them all is that they make it possible to control the pressure in the well much more accurately than is the case with traditional drilling. In traditional drilling, it is primarily the specific gravity of the drilling mud which determines the pressure in the well, while in the case of MPD, valves and pumps are used to adjust the pressure in a more dynamic and flexible way. This enables pressure variations in the well to be significantly reduced, making it easier to drill in narrow pressure windows, where there is little "leeway" between the formation pressure and the fractional pressure. MPD entails additional automation, hardware and software which must work well with other equipment for drilling. Volume control is also more accurate than in the case of traditional drilling.	In the case of managed pressure drilling, it is important to maintain an overview of all parameters that are relevant to well control. In addition to the properties of the drilling mud, it is important to maintain an overview of all relevant pressure measurements, the status/position of valves and the status and fluid flow in pumps. Well pressure is also affected by the vertical velocity of the drill string. Excessively rapid lowering of the drill string can cause overpressure (surge), while excessively rapid raising can underpressure (swab) because the MPD system is unable to control the valves and fluid flow fast and accurate enough to compensate for the movements of the drill string.
Automated control of drawworks: The well, drill string, top drive, drawworks and heave compensator (if relevant) collectively make up a complex mechanical system, and maintaining control over all the forces and movements is far from a trivial task. During drilling,	In order to control the drawworks optimally, information on a range of factors is needed, including:

Function	Important input data
the weight on the bit (WOB) should be stabile and correct, while during tripping, it is important to avoid overly rapid lowering or raising, which could lead to excessive surge or swab pressures. Amongst other things, drawworks control must take account of spring effects (the drill line and drill string become significantly stretched under load with the result that the length is not constant), and dynamic forces (the top drive and drill string are so massive that it takes a lot of force to stop them or set them in motion) in order to achieve the desired velocity, position and force. Internal forces in the drawworks must be compensated for, unless the force of the drill string is measured more directly. The drawworks is also limited by the amount of power that is available from the generators/power supply and how much/powerful braking is possible before components overheat.	• Forces (force in the drill line, torque in the drum, hook load, etc.) • Positions (drum angle, heave, heave compensator, top drive) • Velocities (drum, heave movement and heave compensator movement) • Accelerations (drum, heave movement and heave compensator movement) • Extension (how much drill line is reeled in before the top drive starts to move) • Temperatures (motors, gears, brakes, etc.) • Power available from the power supply • Various command and status signals
Automated rotation of the drill string: In the same way as the drill string is extended in a longitudinal direction, it also behaves like a long torsion spring. This means that the shaft from the top drive must rotate slightly before the rotational force in the torsion spring becomes sufficient to overcome the friction and rotate the drill bit. Without good control over the rotational force and velocity from the top drive, there is a risk of torsion vibrations, which will increase the wear of the downhole equipment. An example of torsion vibration is “stick-slip”, where the lower part of the drill string varies between rotating "too slowly" (stick) and "too fast" (slip). During the stick phase, the drill bit has little or no rotational speed, while the force in the torsion spring gradually builds up because the top drive continues to rotate. The slip phase begins when the stored torsional force becomes so great that the drill bit begins to rotate rapidly, and the rotation continues until the drill bit has "passed" the top drive, causing it to be retarded and a new stick phase to start. These undesirable phenomena can largely be avoided through smart control of the top drive and/or drawworks (drawworks can affect the friction by adjusting the weight on the bit). Examples of functions to reduce torsion vibration are "soft torque" and stick-slip detection.	Relevant parameters/measurements for drill string rotation management are: • Force (torque in motors and shaft) • Rotational speed • Rotational acceleration • Vibration indicators • Weight on bit • Drilling mud flow • Temperatures (motors, gears, etc.) • Power available from the power supply • Various command and status signals • Axial and torsional forces and movement in the BHA and along the string (in some cases, these are measured directly at certain positions; otherwise, they must be calculated)

Much of the input data that is used in automated systems consists of "direct" sensor values, but some indirect/derivative variables are also important, e.g. the amount of extension in the drill line or the distance between the drill bit and the bottom of the well.

Automated drilling and tripping systems will typically contain many of the functions of Table 4, as both drilling and tripping involve the coordinated control of drawworks, top drive and drilling mud in order to optimise the process, while at the same time maintaining well control. The functions are often included as "modules" in an overall automated system which handles the coordination between the systems involved. Common to the automated functions (and the overall system) is that the control algorithms use models to optimise the process. Some automated systems are used for direct control, while others provide decision support only.

Key components from Table 3 are shown in Figure 7 and Figure 8, in order to visualise couplings and interactions during drilling and tripping, respectively. In addition to the components discussed here, the figures also show components from higher levels in an overarching network architecture.

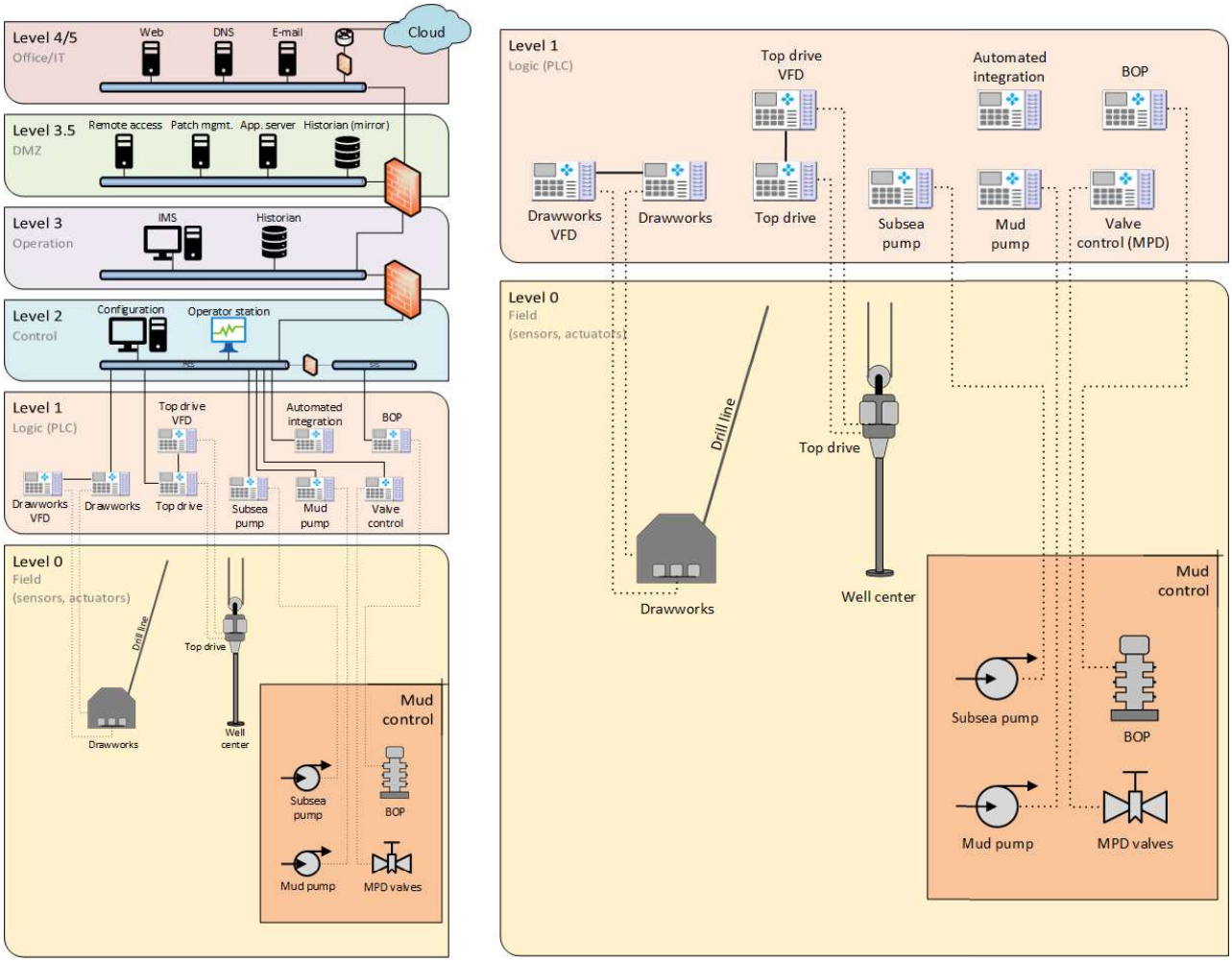


Figure 7 Simplified topology figure to visualise communication and interaction between different components during drilling. Does not necessarily include all couplings and components found in automated systems.

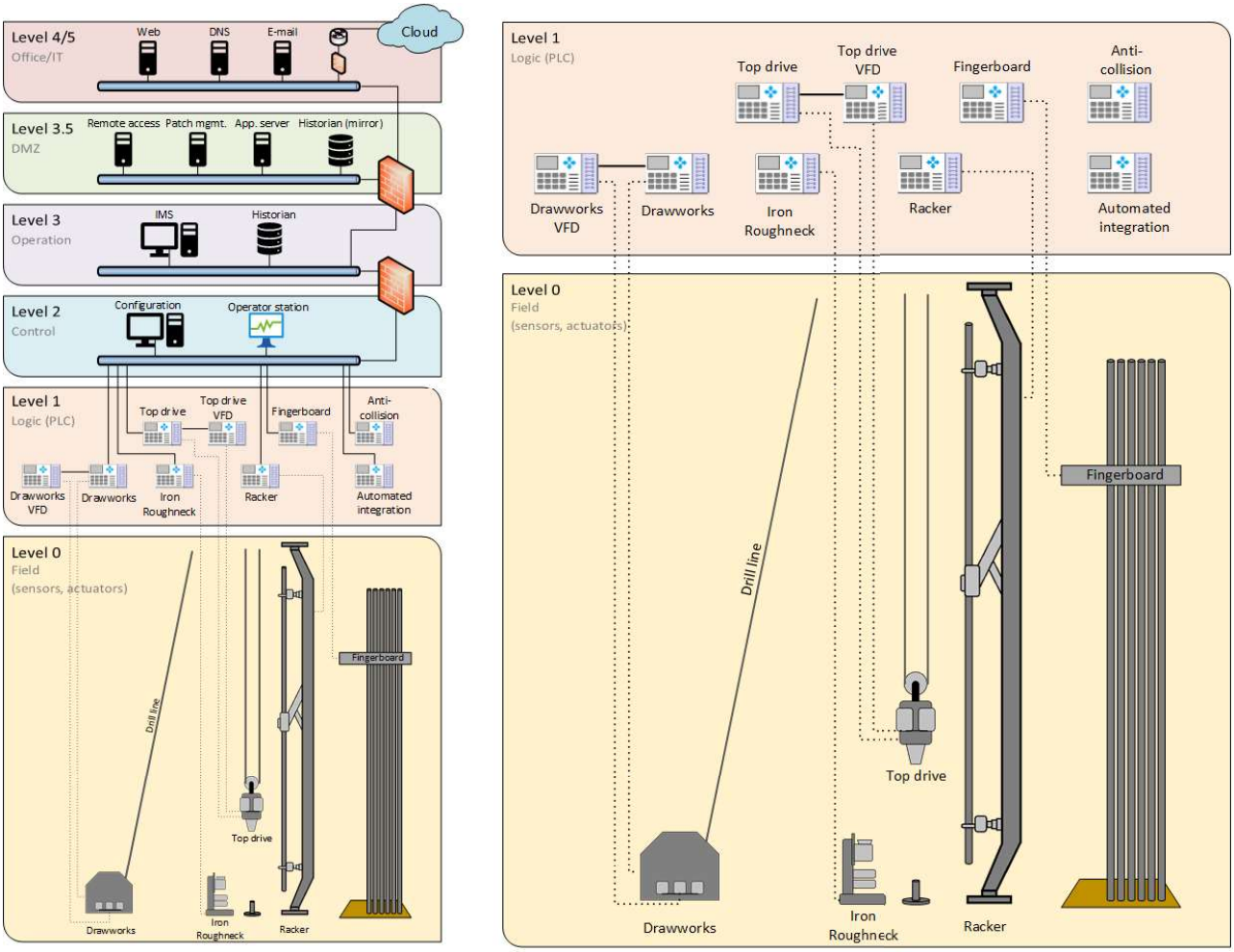


Figure 8 Simplified topology figure to visualise communication and interaction between different components during tripping. Does not necessarily include all couplings and components found in automated systems.

4 Incident management in automated systems

At present, it is not clear to either the authorities or the industry how information and data from incidents, near misses and deviations should be secured for future risk reduction in connection with the use of automated systems. There is considerable variation as regards which incidents and deviations are recorded, how and by whom or/which system incidents are detected, the system that are used to record them, how they are classified, and by whom and how they are followed up further. Figure 9 shows a simplified process flow for handling an incident, from the time it occurs until it is detected, recorded, classified, analysed and followed up. Each of these points is discussed in more detail in subsequent sub-chapters.

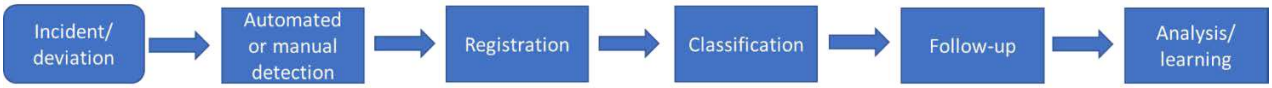


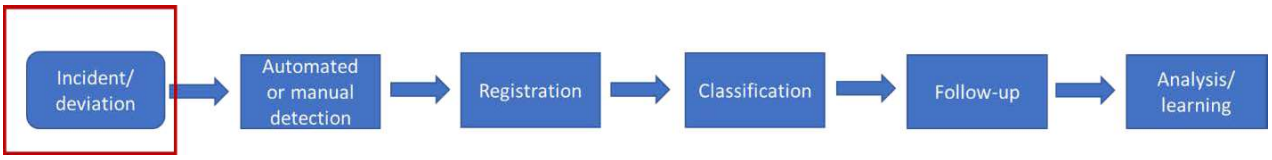
Figure 9 Simplified process for incident management in drilling.

4.1 Which incidents and deviations are reported?

This sub-chapter discusses the incidents, near misses and deviations that trigger handling according to the simplified process flow outlined in Figure 10. According to the interviewees, downtime incidents are the type of incident that are most systematically reported, and such reports are processed methodically by their organisation. What is reported and prioritised depends on criticality. A distinction is often made between:

- Downtime (i.e. rig out of service/not in operation)
- System downtime (i.e. the rig is able to operate, but one or more systems are out of operation). Examples include equipment that needs to be re-started, the replacement of hard drives, etc. which does not directly impact on the drilling operation.

Minor incidents and requests for support which impact on system downtime are also reported, but this reporting is less systematic. For example, a report may be submitted by e-mail and processed within the organisation as "lessons learned", or considered as an item on the agenda at daily meetings etc. Minor incidents are assessed on a daily basis so that improvements or minor adjustments can be proposed. In general, an attempt is made only to report what is directly critical for the driller in order to prevent unnecessary distractions during the drilling process itself.



The following are some examples that the companies themselves have identified as being deviations, incidents and near misses which are typically currently being reported or recorded, and which will therefore be included in the first part of the process flow diagram. All the examples are taken from the interviews conducted with industry representatives.

Manual override/operation in deviation situations:

- Overriding of anti-collision systems due to failure or loss of sensors
- Overriding of anti-collision systems in a movement space that is too confined/strict
- Operation in a deviation situation with the simultaneous use of Automated Drilling Control (ADC) and wired pipe, which are not compatible with each other (wired pipe requires people on the drill floor, while it is a condition for the use of ADC that there is no one on the drill floor). Operation in deviation situations requires a SJA.

- Operation in a deviation situation pending rectification of a physical fault or software error. Requires a SJA.
- Situations where an operator forgets to activate automated systems/functions after they have been disabled in connection with remediation/maintenance, etc. Can create erroneous assumptions that automated systems are operational and will intervene if necessary.

Errors linked to the sharing and input of data:

- Incorrect configuration file
- Incorrect drilling pressure profile

Errors relating to alarm limits (the system issues an alarm or intervenes automatically):

- Stopping of movement of top drive in the event of force exceedances
- Pressure deviations (e.g. in connection with leaks or blockages)
- Fault on high-voltage panel
- Deviation in drilling mud level
- Deviation in liquid flow

Errors linked to communication/dropout:

- Communication failure for software used to control automated systems
- Loss of communication with mud pump
- Software failure

Errors linked to commissioning/upgrades

- Errors in parameter setting
- Real-time simulation differs from preliminary simulation
- Non-conformant pre-simulations from different vendors
- Minor software components which need to be updated etc.
- Lack of experience of new system

Other

- Errors in detection of poor hole cleaning
- Error in connection with the shutdown of mud pumps
- Drawworks stopped due to faults in associated automated management system
- Software error

4.1.1 What incidents and deviations are not reported?

During the interviews, examples of incidents, near misses and deviations which are rarely or never reported were also requested. Typical examples mentioned were:

- Errors due to confusion over decimal points and thousand separators
- Errors due to confusion over units
- Error entering values
- Incorrect parameters/limit values received by third party
- Some deviations from expected values are reported by telephone and resolved on site without being systematically recorded.
- Loss of communication with support services on land. Does not lead to downtime, but often leads to functions that are affected by the loss (system downtime) being disabled.
- Dynamic variation in hook load upon withdrawal from the hole because the automated system introduces a speed limit in order to avoid excessive pressure in well. The speed limit is applied and periodically cancelled, with the result that it can be perceived as "jerks" in the string. Some operators think this is perfectly acceptable, while others prefer to have complete control themselves.

- The use of override or the fact that crews choose not to use certain functions, because they tend to lead to stoppages and error messages. These are examples which are often considered to be improper use and may in some cases result in barriers built into software being removed.

It is worth noting that although few or no cyber incidents or attacks have actually been recorded, the industry is questioning whether this is actually the case.

4.1.2 Findings linked to which incidents and nonconformities are reported

The result tables with findings in the upcoming sub-chapters summarise input from the industry and reflect how some interviewees perceive the status and challenges associated with the reporting of incidents via automated systems. In the last column, we have included SINTEF's general remarks relating to statements from the interviewees. SINTEF's assessments and further recommendations, which are largely based on findings from these tables, are summarised in Chapter 6. In some places in the tables, the term "events" is used as a collective term for deviations, near misses and incidents in automated systems.

Table 5 Input from the industry regarding which incidents and deviations are reported.

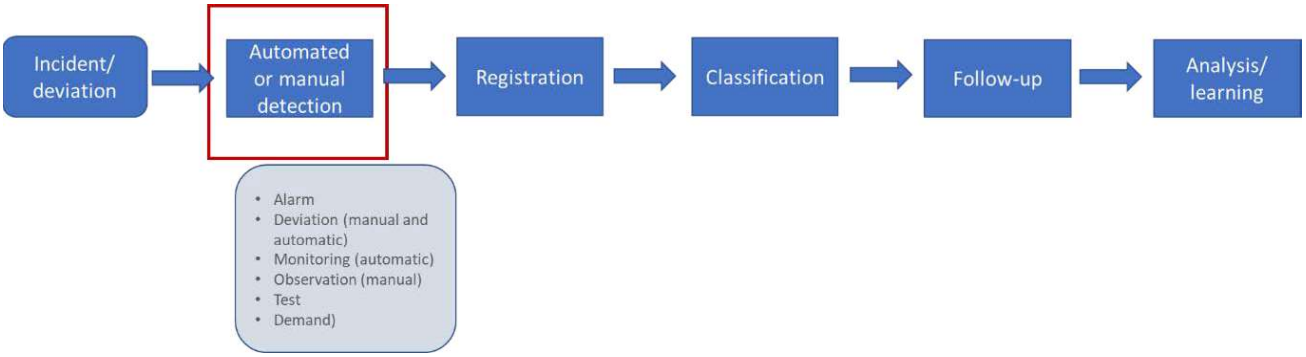
	Input from interviews/workshop	SINTEF's remarks
1.	Very few (no) cyber incidents recorded. There is a question mark over whether this is actually true.	• Is there a need for stricter/clearer requirements concerning the reporting of such incidents? • There is no category for ICT incidents (which end up under "Other"?). • Can the HSE reporting tools be expanded/adapted to also cover ICT incidents, in order to utilise the ability and motivation of the personnel to use these tools?
2.	Good culture and low threshold for reporting deviations. The threshold for reporting has been lowered.	Why might this be the case? • Focus on reporting through observation cards renders reporting harmless? • Simpler reporting systems? • Reporting via the automated system, not human error (does not feel directly responsible)? • Could greater automation lead to both a lower reporting threshold and fewer incidents, or could it be due to underreporting?
3.	Desire for more continuous and detailed recording of operational data and automatic reporting of deviations, e.g. • Automatic detection of changes to important input parameters, such as diameters, which affect the calculation of the maximum velocity in connection with tripping. • Record the number of occasions on which personnel have manually made corrections before a deviation is detected. At present, some companies are dependent on transmitting such messages orally, without any possibility of finding out subsequent follow-up.	What consequences will automated reporting have? • There will be many positive effects, but it could also lead to degraded system understanding or too much trust in the systems? • Who will take over reporting if the system goes down? • Could it cause unnecessary noise (detect too much)?

	Input from interviews/workshop	SINTEF's remarks
4.	The incidents that are being reported today are person-dependent. Feedback is often so subjective that it is difficult to interpret. Demand for requirements and a framework for saying what needs to be reported and who it needs to be reported to.	Is this due to a lack of understanding of systems, unclear criteria, culture, other? • Can criteria be identified which will make what should be reported less ambiguous? • Does the operator have clear criteria, both for incidents which must be reported to authorities and for other types of deviations?
5.	A lack of process understanding could be an obstacle to good reporting. Perhaps more than a lack of system understanding. The driller generally has a good understanding of the system itself, but it is still important that he or she understands the limitations of the systems.	• Could this lead to underreporting? • In a future scenario where the systems do significantly more and the operator does significantly less than at present, it is conceivable that the driller may not have sufficient understanding to be able to submit good reports. However, in such a scenario, the drilling operator may not be needed at all?
6.	Challenges relating to the quality of software and data could lead to misunderstandings and error reporting.	Is there a best practice regarding how data and software should be handled in a safety-related context?
7.	Strong focus on reporting of incidents which result in downtime and which vendor/system the downtime can be linked to.	• This could be at the expense of safety (if reporting is affected by the allocation of responsibility and cost). • Does the industry need a more independent assessment of incidents?
8.	Raising of awareness concerning deviations and incidents linked to efficiency. Easy to mobilise in the event of downtime, but maybe we need to become better at capturing more of what concerns efficiency as well?	• Lack of understanding of the impact that reduced efficiency has on the process? • How much does efficiency need to be reduced by in order for it to be meaningful to report (and how can this be predicted)?
9.	It is generally difficult to predict the potential consequences of a deviation under other circumstances (worst case), with the result that often only incidents with significant consequences are reported. In connection with tripping, for example, it is possible to impose too great a load on the drawworks in relation to what the rest of the system is able to handle. One then does not necessarily see the extent of the fact that it is possible to cause a power black out. Rate of Change (ROC) filter to eliminate this possibility added.	• Could it help to include multiple deviation scenarios in training simulators?

4.2 How are incidents and deviations detected?

This sub-chapter deals with findings relating to the way in which incidents and deviations are detected. Incidents and deviations are detected through either automatic or manual detection. Various manual and automatic detection methods are listed in the figure below, but some concrete examples of how deviations and incidents are detected are:

- If the system operates outside limit values or deviations from the expected response occur, this could be detected both automatically and manually, i.e. it is possible to be alerted via an alarm/other alert or, for example, visual detection.
- Deviations from the expected response can be detected both automatically and manually, e.g. by running old and new systems in parallel and observing (visually) or receiving an alarm about non-conformant responses where the systems are actually expected to be identical. For such situations, it is important to define what is considered to be a deviation, so that it can be detected both manually and automatically. The same applies to deviations both between different simulations and between simulations and operations.
- Incidents and deviations can also be detected during testing and in operation (demand), or based on feedback from subcontractors who perform a monitoring function.



Technical resources that are used to detect incidents could for example be:

- Self-diagnostics and condition monitoring
- Information Management System (IMS)
- Alarm systems
- Safety and Automation Systems
- Simulations
- Drilling recorder

Examples of organisational and operational resources relevant to the detection of incidents:

- Maintenance programme
- Maintenance/technical personnel
- Inspection programme
- Inspection personnel
- Daily operation and random observation
- Control room operators (both onshore and offshore)
- Expert monitoring (from system provider)
- Field operators
- Training programme

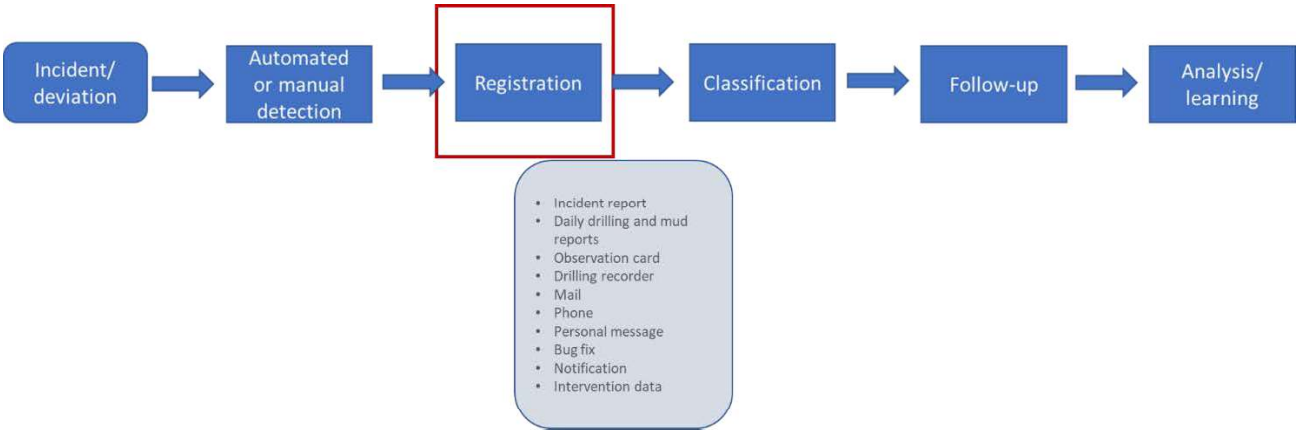
4.2.1 Findings relating to how incidents and nonconformities are detected

Table 6 Input from the industry regarding how incidents and deviations are detected.

	Input from interviews/workshop	SINTEF's remarks
1.	In the drilling recorder, the driller has a "button" which must be pressed if the driller feels that something is not quite as expected. This is normally followed up later, but there are no formal requirements regarding follow-up.	• Will the potential be fully exploited while there are no requirements or systematics concerning the follow-up of such deviations?
2.	High alarm density and "unnecessary" alarms represent a challenge, and alarm management and prioritisation become important in order to avoid operator overload in such contexts. Alarm texts also cannot be too similar (one or more almost identical alarms with different meanings) or difficult to understand.	• How can we make sure that we collect data relating to the less important alarms without creating noise? • How can we distinguish between alarms aimed at drilling personnel and 'system alarms' for maintenance personnel? • How can we strike a balance between what is perceived as 'noise' and important messages? • Adapt alarms to user profiles?

4.3 How incidents and deviations are reported/recorded

This sub-chapter deals with how incidents and deviations are detected and reported. Reporting/recording an incident or error depends on the type of incident, the criticality of the incident, and who (or what) is detecting the incident. Most companies make a distinction between reported incidents and near misses relating to HSE and quality respectively and have different systems for dealing with these two areas. Some also have different reporting paths for process-related incidents (reported to management) and software/technical errors (reported to development teams or technical personnel). Vendors who receive downtime reports from their customers see considerable variation as regards how informative and structured the various customers' descriptions are. Some reports are detailed and tidy (what has happened, during which operation, etc.), while other reports provide little information except that "something has happened". Examples of possible reporting/registration methods are listed in the figure below. Below the figure is a list of technical, organisational and operational resources of relevance to the reporting of incidents and deviations.



In addition to the reporting systems described in Chapter 4.3.1, examples of technical resources used for recording incidents are:

- Tablets
- Workstations

Examples of organisational and operational resources relevant to the recording of incidents are:

- Framework/taxonomy for reporting
- Reporting guidelines
- Systems/algorithms for automatic error detection
- Personnel
- Training/motivation programme and competence

4.3.1 Reporting systems and methods

The following provides a brief description of different reporting systems. A distinction is made between two main groups of reporting system: HSE&Q and maintenance. However, some of the reporting methods may include both HSE&Q and maintenance, such as observation cards.

In many cases, as illustrated in the example scenario in Chapter 4.3.3, the first report that an incident or situation has occurred will be received by phone, personal message or e-mail. During the interviews, it was pointed out that the advantage of telephone and personal messages is that it is possible to provide a more detailed account of the incident. The possible drawback is that they are not recorded systematically, which can lead to underreporting and reduced opportunities for future learning. An e-mail will provide written documentation, but not systematic storage or follow-up. There is also a risk that important messages do not reach the recipient and will therefore never be followed up.

4.3.1.1 HSE and quality systems

SYNERGI Life etc.

Incidents concerning HSE&Q are typically reported via programs such as Synergi Life and Tracker. Both of these programs are well-known HSE&Q reporting systems which are in widespread use in different enterprises/industries. Incidents are typically reported by logging on to a PC, but it is often also possible to report on a smartphone. When an incident/deviation is reported, the time and place and a description of the incident are generally recorded. Photographs and other attachments can also be added.

Both quality and security incidents are recorded via such programs. This also includes downtime. A distinction is also often made between administrative and process-related incidents. Not all incidents are open to everyone. Some incidents can only be accessed with special permission or by employees who belong to a specific part of the organisation.

According to some of the interviewees, the most important HSE-related incidents are open, and there are mechanisms in place for sharing with rig companies which have a contract with the operator company, but there is uncertainty as regards whether or not this applies to the industry as a whole.

Synergy also records the potential and actual consequences of an incident, e.g. personal injuries, lost-time injuries, fire, discharges into the environment, financial loss, etc.

Observation cards

'Observation card' is a common term for cards which are used to report conduct or unsafe conditions at the workplace. Different companies use different names for these cards, including "Stop card", "Safe card" or

”Obs card”. The companies often use observation cards as part of their improvement process and as a means of increasing the focus amongst employees on health, safety and the environment (HSE). There is often a desire to keep the reporting frequency high, and several of the companies which were interviewed have run campaigns relating to this. Observation cards are often used to report minor observations and incidents which do not require immediate action. An important aim with observation cards is to make the reporting threshold as low as possible and to familiarise users with the system, so that it is easier to report more serious incidents.

Daily drilling reports

All operators which carry out drilling operations on the Norwegian continental shelf are required to submit daily reports on drilling operations to the PSA. These reports provide an overview of the progress of drilling operations and show, amongst other things, the time spent on individual operations, with separate codes for each phase.

The reports have a specific section for reporting undesirable incidents. An example of the reporting of an incident in the daily drilling report to the PSA is shown below (shows text only). The drilling report refers directly to any incidents that are recorded in Synergi.

Start Date/Time	End Date/Time	Activity Code / Aborted Operation	
			BOP – Run BOP, Other Set up BOP to drilling mode. Not able to set up BOP to drilling mode. Performed at controlled disconnect of LMRP with weight down.

Report status:	Finish Date	Total Down Time	Service	Failure Code
Completed				

Equipment Type	Trade Name	Manufacturer	Serial no	Equipment Part
BOP stack				

Synergi no	Description Non-conformities – Failure to set up ADS (Automatic dis) system upon landing of BOP (Automatic dis
Hazard	Upon landing of BOP and setup of the Automatic Disconnect System failed on attempt to operate the ADS reset function from the ROV panel. Operation of the ROV valve 'ADS reset isolation' did not give any indication of pressure on subsea gauge 'ADS reset pressure'. Further troubleshooting confirmed hydraulic fluid vent via 'ADS reset isolation' valve to sea. However, due to concerns over the lack of system functionality, further configuration of the system was done with positive weight on the LMRP connector. Upon opening of the ROV valve 'ADS supply isolation' the LMRP connector and C/K connector unlatched prematurely and unintentionally. Decision was made to recover LMRP to surface for further investigation. Ref: Synergi xxxxxx

Company	Service	Description	Downtime %
	RIG	Rig Operations	100

Figure 10 Example of extract from a daily drilling report.

A new standard was adopted in 2008 based on cooperation between Norwegian and foreign oil companies. The format is XML-based and is based on WITSML. Three options are available for transferring the XML file from the operator to the PSA: 1) Web form for manual uploading of XML, 2) Web service for automated transfer process, and 3) EPIM Reporting Hub (ERH). All these options use secure data communication.

Daily mud reports

The drilling mud company prepares a daily drilling mud report (mud report). The report focuses on muds which are used in the drilling operation and additives, both properties and the logistics associated with the handling of this. In some cases, this may complement the information that is provided in the daily drilling report. As mud and chemical management processes are also automated, this may become more relevant for the reporting of deviations, near misses and incidents.

4.3.1.2 Maintenance system

Computerised Maintenance Management System (CMMS)

Operating companies report, classify and document equipment condition and faults which are detected during operation, testing and maintenance in a data-based information and management system. A typical example on the Norwegian continental shelf is the SAP maintenance system. Each observation is typically stored as a notification that is linked to an equipment tag, which is a unique physical identification tag attached to the equipment.

Condition monitoring system

Condition monitoring systems continuously collect data on the condition of equipment, such as vibration and temperature. This data will trigger alarms in the event that the condition of the equipment is degraded and provides a basis for decisions concerning the essential maintenance of equipment. Rigsentry is an example of such a condition monitoring system.

Drilling recorders

Some vendors offer solutions which log all time series data, commands, operations, screenshots and alarms during a drilling operation. All operations are then numbered with a tag. By logging everything from operator input to operational characteristics, the entire drilling process can be saved and recreated afterwards. Some systems also have the option of marking specific timestamps during the process (by pressing a button), making it easy to find the right information at a later date. When this button is pressed, it is also possible to enter a brief description of the problem at given times. It is worth noting that there is no systematic follow-up of incidents recorded in Drilling recorder. An e-mail will be sent to the responsible personnel each time the button is pressed, but there are no formal requirements regarding the follow-up of this.

Data from Drilling recorder is actively used in investigations, as well as in minor improvements and optimisation. An example that was highlighted during an interview was a situation involving a mud bucket which did not behave as expected. With the aid of Drilling recorder, it was then possible to determine that the cause of the issue was a function that had been activated that should not have been. It was pointed out that the system is not used to apportion blame, but for active improvement and optimisation, as well as causal analysis.

Operations such as tripping and drilling are logged continuously, usually by several vendors, and changes in the operation are monitored. This is also used for optimisation, but it is a general impression that there is the potential to exploit this data in a more systematic way.

Update request

Vendors of automated drilling systems make continuous updates and improvements to their systems. The various companies report a need for upgrades and bug fixes amongst the various systems concerned. Assessments of the criticality and prioritisation of tasks are carried out on an ongoing basis by the vendor (possibly in consultation with the operating company or others). The vendors have a registry for the version control of software and firmware, but there are varying practices as regards risk assessment of the software itself before it is modified/updated.

Intervention statistics

Some vendors stated that they keep what are known as ‘intervention statistics’. Here, logs are kept of cases where an automated system has intervened or performed an action which has prevented an incident or deviation situation. These interventions are reported daily to the responsible operating company. One of the vendors stated that they had up to 300 registered interventions during the period January to April 2021.

4.3.2 Who reports incidents and deviations

According to the interviewees, it is considered to be a collective responsibility to report incidents and deviations in the companies' internal reporting system, i.e. employees of operating companies, vendors and service companies are expected to report incidents on an ongoing basis in their respective reporting systems. The same incident can sometimes be reported via more than one system. The incidents then sometimes make reference to each other, but duplicates and possible misunderstandings can occur. There is an expectation that the operating company will have a complete overview and manage the reporting obligation with respect to the PSA.

Operating companies and subcontractors are in agreement as regards having a low threshold for reporting incidents and deviations. Some of the interviewees believed that if incidents are reported which could easily have been overlooked, it is a good sign which testifies to a good reporting culture. A strong emphasis is generally placed on training concerning the various reporting systems, and some companies also run campaigns with rewards for the best suggestions for improvements.

It is important to note that, in the case of technologically complex systems, the actors who understand the criticality and scope of a deviation best may well be not those who are actually operating the systems. In such cases, it is conceivable that incidents that should have been reported are not detected due to a lack of understanding or competence. In the following, two example scenarios are presented for the handling of incidents and near misses in drilling operations. Various roles in handling of the incident and reporting are also highlighted through these examples. These examples are based not on interviews, but on previous experiences, and are designed to illustrate how communication *can* take place between different actors.

4.3.3 Example scenarios

Example scenario 1 (Figure 11):

1. Data engineer sees an unexpected increase in active volume
2. Data engineer talks to driller by radio
3. Driller calls the mud engineer to find out whether they have seen anything in the mud returns or in the pump room and/or elsewhere
4. Driller calls drill supervisor and reports the matter
5. Drilling supervisor looks at the change, and if necessary discusses it with the drilling manager or drilling engineer
6. Depending on the conclusion:
    A. Temperature effect: Continue the operation. *Not reported.*
    B. Error in sensor which is not considered to be critical; operation continues. *Reported in DBR/DDRS?*
    C. Possible inflow from the formation. Stop the operation, close the well and monitor the pressure. Involvement of people on land. *This will be included in the daily drilling report. Perhaps Synergy.*

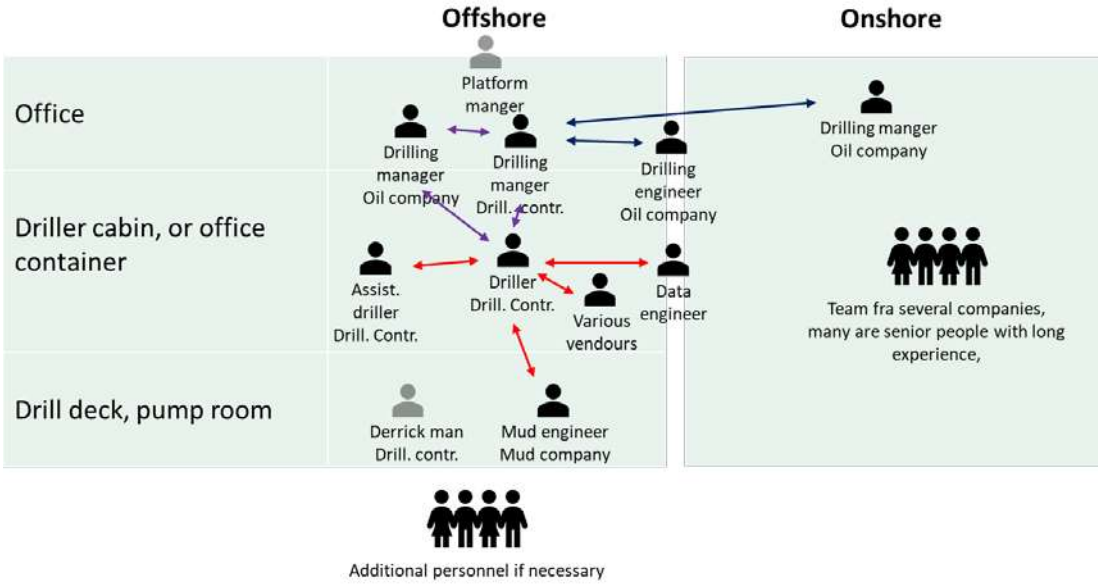


Figure 11 Example scenario 1 for handling of incidents and near misses in drilling operations.

Example scenario 2 (Figure 12):

1. Data engineer sees an unexpected increase in the *difference* between measured active volume and estimated active volume in the digital twin
2. Data engineer talks to driller by radio
3. Driller calls the mud engineer to find out whether they have seen anything in the mud returns or in the pump room and/or elsewhere
4. Driller calls the drill supervisor and passes on the information he has
5. If there is only a small or no increase in *measured* active volume, so that the deviation is due to a reduction in *calculated* active volume, the vendor of the digital twin will be involved and asked to assess the situation. One possibility is that the deviation is due to an inaccurate model or input data to the model. If this possibility can be excluded and if a sensor fault can also be eliminated, it may be a situation where the increase in active volume is masked by another physical effect, such as a temperature effect. In other words, the situation could be serious even if the sensors alone showed no signs of any significance.
6. The drilling supervisor assesses the information and may discuss the situation with the drilling manager or drilling engineer
7. Depending on the conclusion:
    A. It is overwhelmingly likely that inaccuracy in the model or input data is the cause of the deviation: Continue the operation and monitor closely. *Probably not reported.*
    B. Fault on sensor which is not considered to be critical: The operation continues. *Reported in DBR/DDRS?*
    C. Possible inflow from the formation. Stop the operation, close the well and monitor the pressure. Involvement of people on land. *This will be included in the daily drilling report.*

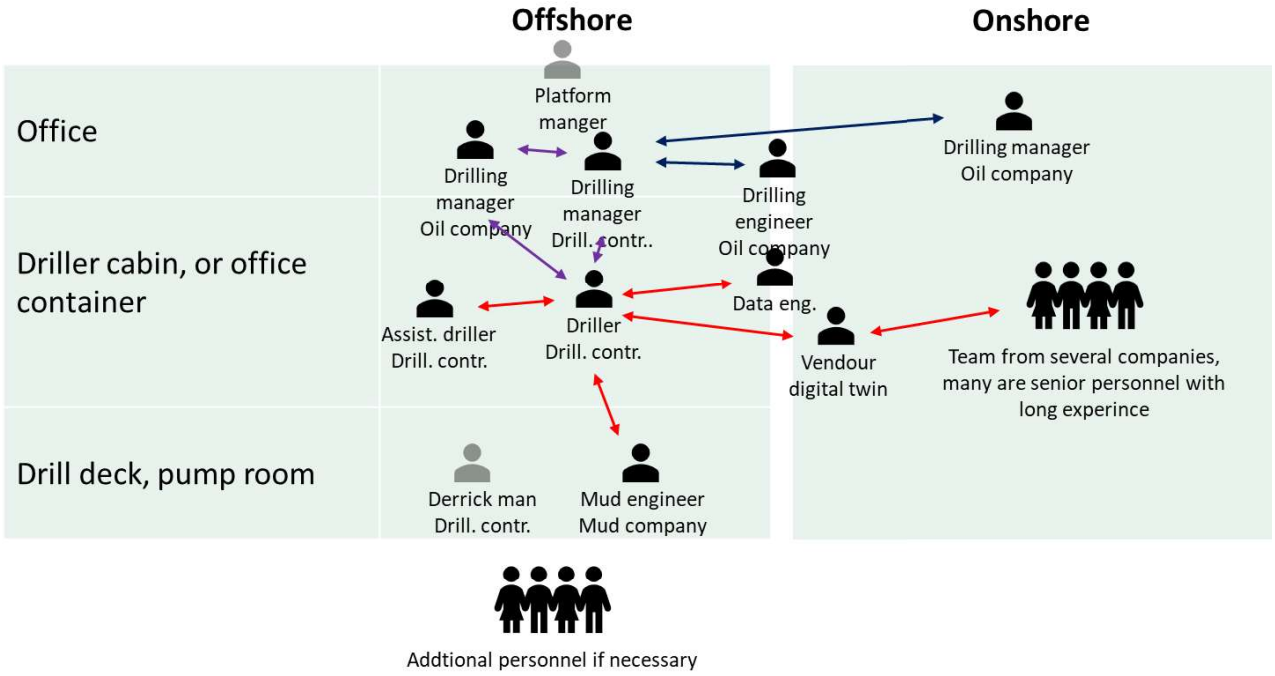


Figure 12 Example scenario 2 for handling of incidents and near misses in drilling operations.

4.3.4 Transaction error

As the example scenarios show, many links and communication channels may be involved in the transmission of information. At the same time, this gives rise to many opportunities for different failure modes to occur. During the interviews, for example, examples were given where incidents/deviations are reported by e-mail or other channels where no confirmation is given that the notification has been received. In Table 7, which is based on Salmon, Waler and Stanton [33], examples of transaction errors relating to the transfer of information are given, and the e-mail example will belong to the "Absent transaction" category. There will also be a possibility that information that was transferred was incorrect (e.g. when values are entered manually). Another example is point 4 of Example scenario 2: “Driller calls the drill supervisor and passes on the information he has”. This will work as long as the drilling supervisor has all the available information and at the same time communicates this information, but not if the transaction is incomplete. Similarly, the recipient may, in turn, interpret the information incorrectly (misunderstood transaction).

Table 7 Examples of transaction errors [33]

Type of error	Explanation
Absent transaction	There was a need to transfer information between the actors, but this transfer did not happen. Includes cases where such transfer is not part of normal operations (described procedures, aids in use, organisation and management).
Incorrect transaction	The transfer of information is initiated, but the information is incorrect. Includes both incorrect factual information and incorrect individual situational awareness on the part of the sender.
Incomplete transaction	Not all the information that the recipient needed is transferred.
Misunderstood transaction	The correct information and individual situational awareness are transferred, but the recipient misunderstands.

4.3.5 Findings relating to how incidents and deviations are reported

Based on the interviews and previous studies from the process industry concerning the handling of incidents and deviations, it is apparent that deviations at system or component level are often linked to a deviation cause such as normal degradation, overloading, user error, design error, etc. and these are recorded in the maintenance system for follow-up and correction. Accidents, incidents and near misses are to a greater extent linked to the consequences of deviations, such as personal injury, material damage, etc., and these are registered in HSE and the quality system.

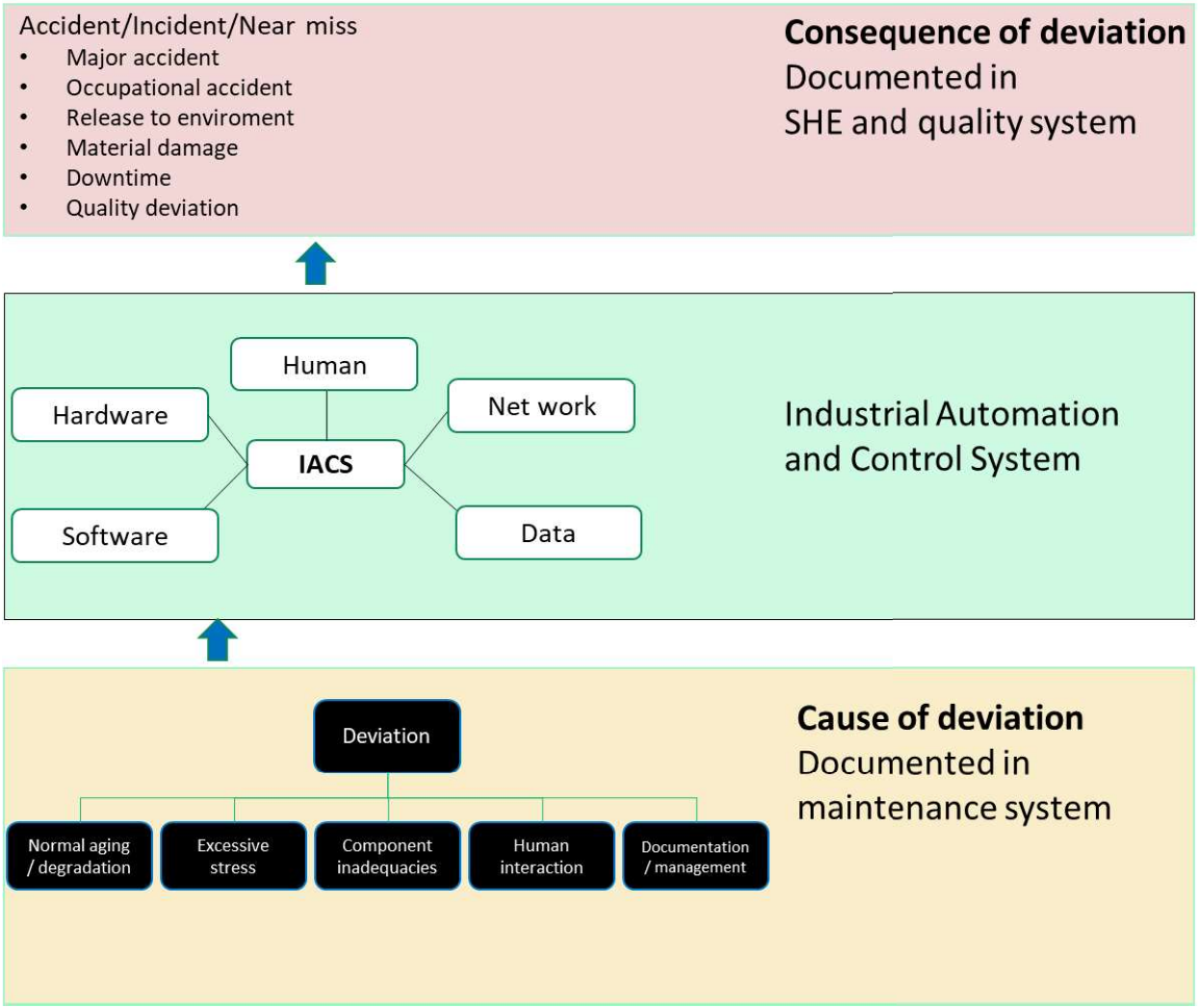


Figure 13 Cause of deviation recorded in maintenance system versus consequences of deviations recorded in HSE and quality system.

The table below summarises the findings from interviews and workshops linked to the way in which incidents and deviations are reported.

Table 8 Input from the industry regarding how incidents and deviations are reported

	Input from interviews/workshop	SINTEF's remarks
1.	Persons who call and report deviations may convey more nuances than automated reports. It is still human beings who have the greatest credibility.	• Does this mean that the reporting is not detailed or good enough? • What does this mean for the opportunities regarding automated reporting?
2.	User-friendliness when reporting is important. Why is training necessary? E.g. mobile banking and mobile payment apps are tools that are easy to use without any training. Improved user-friendliness may contribute to more accurate reporting and leave less scope for misinterpretation.	Why do we need training? • Do we need better training or just better systems? • Have we designed the systems incorrectly, or is it motivation and ownership that is lacking? • Chatbot might be useful?
3.	Lack better feedback (feedback loop) for those who report. Especially mentioned by vendors.	See point 4.
4.	Many different reporting systems both internally in companies and for different actors. A lot of time is spent recording the same incident in several systems. Should do this in a smarter way, e.g. common or standardised system for both reporting and training. Will also facilitate the sharing of experiences and learning. The initiative must come from the operator.	What will be the limitations in getting such a project carried out?
5.	Some incidents/deviations are reported by e-mail or other channels where no confirmation is given that the notification has been received. This entails a risk that messages will not arrive at all or that they will arrive too late. For example, e-mails may be filtered out as spam.	• Could a standardised reporting system be useful here too? • In addition to the "absence of transaction", there may also be opportunities for other transaction errors (ref. Table 7), especially when many actors are involved?

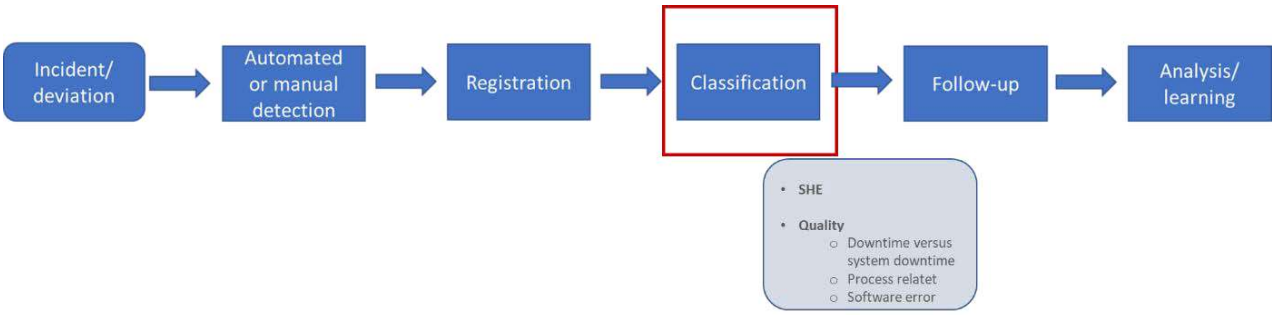
4.4 How are incidents and deviations classified?

This sub-chapter deals with the way in which incidents and deviations are classified. As pointed out in Chapter 2.4.7, the classification of incidents and deviations is important both because it can provide information on the severity of an incident and because it will make it easier to compare data on similar deviations or incidents.

No mention was made during the interviews of specific standards, and the practices followed mainly appear to be company-specific. However, a few classification methods were mentioned:

- HSE versus quality
- Downtime (linked to equipment group)
- System downtime (lowest level), downtime, safety
- For operational incident reporting, one of the companies had different categories for classifying incidents, examples of categories: Well control incidents, Procedural errors, Delays caused by customer, Delays due to weather conditions, Equipment failures, Corrective maintenance, etc.

Some technical and organisational resources that may be relevant for classifying events are listed under the figure.



Some examples of technical resources of relevance to the classification of incidents are:

- Maintenance system
- Technical aids, such as tablets, workstations, etc.
- Drilling recorder

Examples of organisational and operational resources of relevance to the classification of incidents are:

- Framework/taxonomy for classification
- Guidelines for classification
- Systems/algorithms for automatic error classification
- Personnel
- Training/motivation programme and competence
- It is common for each rig to have an onshore HSE&Q advisor, who provides an additional check on the classification of incidents.

A general impression gained from the interviews is that there is a widespread strong focus on downtime and the equipment and vendor to which the downtime can be linked.

One of the operator companies had a separate guide in the management system for the classification and processing of ICT incidents, but most vendors were unaware of this. As regards the classification of maintenance errors, the interviewees said that they applied international standards, but no specific standards were discussed further during the interviews.

Few people thought it was a problem that no detailed classification guidelines were available, but several people thought it would be a good idea to have a common, standardised framework. Several people also thought that it could be a problem that the classification will often be person-dependent, and it will therefore be harder to establish consistent and comparable data for learning purposes. The question is therefore whether it is possible to get away from person-dependency in relation to reporting with clearer guidelines and simpler classification methods.

Some of the interviewees had noticed that the categories "other" or "unknown" were often used when linking downtime to equipment type, but this was not seen as a major challenge in the follow-up of the systems. However, for the follow-up of safety-critical equipment for the petroleum sector, it is considered that the extensive use of these categories could lead to searching in, for example, free text fields in order to find the relevant information that is needed. An internal study recently conducted over a six-month period for a Norwegian offshore facility showed that failure mode was classified as either "other" or "unknown" in more than 50% of the notifications.

4.4.1 Defined situations of hazard and accident

The interviewees had little knowledge of DSHAs and most did not know what they were. However, some people had a good overview of IT DSHAs (hacking, malware, social engineering/phishing, misuse, error).

- Several believed that DSHAs relating to drilling are sufficient
- There is no DSHA linked to automated pipe racking
- Defining new DSHAs is considered to be a challenge because it will complicate analyses and standards
- Cyber security is an area where consideration is being given to the introduction of a new DSHA.

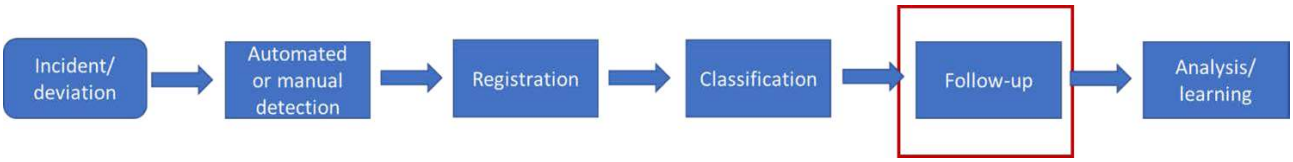
4.4.2 Findings relating to how incidents and deviations are classified

Table 9 Input from the industry regarding how incidents and deviations are classified

	Input from interviews/workshop	SINTEF's remarks
1.	There is a need for reporting that is more systematic and easier to measure. Feedback is often so subjective that it is difficult to interpret. Example of incident classifications: service interrupt, non-productive time, safety.	• Can this subdivision be standardised? • Are these examples of subdivision too coarse to provide meaningful data and feedback?
2.	Systems are often complex; some have had to assign several people to ensure a satisfactory complete overview. Challenging to understand how they work and thus report correctly. Strong focus on savings can lead to inadequate training.	• Who makes such assessments about extended staffing, and is the issue picked up on sufficiently? • Lack of understanding of/focus on learning after near misses?
3.	Conflicting interests of different actors: Although there is both a desire and an intention for operating companies, drilling companies, vendors and service companies to act as an integrated team with shared interests, it was also mentioned that some reporting may be influenced by internal and/or external pressure to shift responsibility and cost. The way in which an incident is categorised can, for example, impact on who is responsible for follow-up and remediation.	The allocation of blame could come at the expense of safety. • Might a more unambiguous classification and threshold for what to report help? • Does the industry need a more independent assessment of incidents?

4.5 How are incidents and deviations followed up?

This sub-chapter discusses how incidents and deviations are followed up; see the process flow diagram below. After incidents are reported, they are incorporated into the company's management system. Depending on the type of incident, an initial notification is filled in for the management/discipline managers, etc. It will also be stated whether the incident should be investigated and, if so, at what level. The impression is that many vendors of advanced subsystems practise detailed logging and reporting internally for troubleshooting and improvement purposes. At the same time, it is assumed that the responsibility for overarching and external reporting rests with other companies. The reporting of incidents to the PSA is handled by the operator companies. Some incidents and errors/faults are also reported to DNV (e.g. technical effects concerning classes etc. and this will usually result in an order and a deadline for rectification).



Some examples of technical resources of relevance to the follow-up of incidents are:

- Maintenance system
- Drilling recorder

Examples of organisational and operational resources of relevance to the follow-up of incidents are:

- Work processes for handling incidents and notifications
- Operations and maintenance managers
- Work orders
- 24-hour meetings
- Drillers forum/crane forum/webinar
- Monthly meetings with safety managers
- Training and competence

There is not the same degree of systematics as regards the handling of near misses. A good example is “the button" that the driller has available to him during drilling operations (when using Drilling recorder) which can easily be used to register that something abnormal is happening at any given time. In this case, it is not possible to record *what* has actually happened, only that *something* has happened. There are also no requirements regarding the follow-up of such registrations, although in most cases they will be processed after the drilling operation has been completed.

RACI (Responsible, Accountable, Consult, Inform) was mentioned in some of the interviews as a tool for following up incidents and deviations. RACI is typically a matrix or linear responsibility diagram which describes the participation of different roles in the follow-up of tasks or deliverables for a project or business process.

4.5.1 Findings relating to how incidents and nonconformities are followed up

Table 10 Input from the industry regarding how incidents and deviations are followed up.

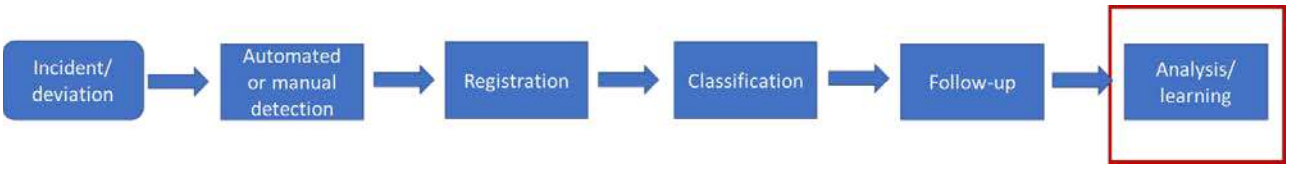
	Input from interviews/workshop	SINTEF’s remarks
1.	Vendors are sometimes informed that an incident or near miss has occurred, without becoming involved in a root cause analysis.	Complicated actor picture: • How can we create a common information sharing and learning arena?
2.	Unclear division of responsibility for responding and taking action over an incident, which in the worst case scenario could lead to the incident not being followed up at all. You must report to the person who can do something about the matter (or learn something from the reporting).	• How can the areas of responsibility be readily communicated to ensure that the right information ends up in the right place? • More active and standardised use of RACI (Responsible, Accountable, Consult, Inform)?
3.	Some companies have their own Cyber/IT security contact who can be contacted in the event of a ICT incident.	This only applies to a small number of the companies. • Should it be a requirement? • Are actors aware of this contact person?

	Input from interviews/workshop	SINTEF's remarks
4.	Human-machine interaction is more important than follow-up at equipment level.	Perhaps this is only true for the current situation? • Will human-machine interfaces become more important as a result of an increase in the use of automated systems (ensuring a good understanding for intervention by personnel in the event of deviations in automated systems)? • Will it become more important to follow up technical errors when the use of automated systems becomes more widespread?

4.6 How are incidents and deviations analysed?

This sub-chapter deals with how incidents and deviations are analysed and shared. Most companies seem to have good solutions for information sharing, especially internally. As regards the sharing of information after incidents, several interviewees said that the experience transfer system is used. This system is used both internally and externally, depending on the type of incident and relevance for the various actors. Both images and text can be shared, often in the form of newsletters. The drilling companies also arrange "drillers forums", where typical incidents on drill floors are presented in order to share expertise across rigs. There are also specific crane forums for sharing expertise relating to crane handling. In addition to the sharing of incidents, there is also active sharing of both technical and operational improvements implemented with each company. These will often be announced via a "bulletin" or, in more critical cases, as a "safety alert".

A summary of technical, organisational and operational resources of relevance to information sharing and learning is presented below the figure.



Examples of technical resources of relevance to information sharing and learning from incidents are:

- Maintenance system
- Incident databases
- Safety bulletins/newsletters/experience transfer system
- Machine learning

Examples of organisational and operational resources of relevance to information sharing and learning from incidents are:

- Review of incident data
- Data processing personnel
- Frameworks and taxonomies for follow-up
- Training and competence
- 24-7 meetings
- Weekly/monthly meetings between rigs/vendors, etc.

There are numerous factors which can impact on and prevent the sharing of technical, operational and incident data. One is a contractual relationship. Some contracts facilitate more transparency, while others require cards to be held closer to the chest. According to the interviewees, sharing is often easier when the oil company has established direct agreements with the actors involved, while it is more difficult if the well is delivered by a single turnkey manager ('turnkey responsibility' means that one company has full responsibility for the well with respect to the operator company, so that subcontractors have a contract with that company, rather than directly with the operator company). Commercial circumstances also come into play. For example, it can be difficult to share technical data if it concerns innovations which are expected to offer commercial benefits for a vendor. However, this varies between companies; some prefer to have a lot of input and greater transparency, while others do not. Cultural differences were also mentioned as an important factor which influences transparency. A general perception is that there is a strong willingness to share amongst the actors on the Norwegian shelf, although this may be somewhat more difficult internationally. The degree of automation also impacts on the sharing of technical information. Not all facilities have equipment that is relevant for the sharing of incident data relating to automated systems. In such cases, the sharing of information will not be as natural. Finally, a strong desire to move on in an operation may come into conflict with the follow-up of near misses. It is therefore important that the operation is not delayed unnecessarily by such follow-up, partly because a delay to an operation could increase the risk of incidents. Instead, the parallel management of near misses should be facilitated with a view to later improvements and learning.

Despite the fact that there are several arenas for the sharing of information, it is not a given that they will lead to improvements or learning. This is discussed briefly in Chapter 5.

4.6.1 Findings relating to how incidents and deviations are analysed and shared

Table 11 Input from the industry regarding how incidents and deviations are analysed and shared.

	Input from interviews/workshop	SINTEF's remarks
1.	Disseminating experience effectively is challenging because of the many actors involved.	Could a clearer and more detailed classification of incidents in relation to the actor picture result in more targeted information sharing?
2.	Some vendors receive feedback in the event of problems, but they sometimes receive no feedback concerning normal operations. For example, some vendors would prefer to have access to daily drilling reports and mud reports (and preferably digital sharing of parameters). Greater transparency and sharing of important configuration information could have prevented quite a few problems. The transparency and sharing of information that is normally reported internally within each company will help to promote greater learning.	More advanced tools/systems combined with collaboration between a number of actors are making openness/transparency increasingly important. Perhaps a combined initiative from the major actors is what is needed, so that information can be shared across companies regarding incidents, near misses and interventions and the sharing of technical information?
3.	Greater involvement of end users will make it easier to exploit the learning potential and improve systems. This requires both flexibility on the part of the vendor, and the operator and drilling company to facilitate such initiatives.	• How can end users be involved in vendors' improvement processes? • How can vendors be involved in improving end user competence?
4.	Automation contributes to shorter improvement loops (no need to fix errors by "updating" all users, just need to update the system).	Nevertheless, it is important to have user interfaces which ensure that operators possess sufficient insight into and understanding of the process?

4.7 Other feedback from the industry

The following summarises findings from interviews and workshops which are not directly relevant to the assignment, but may nevertheless be of interest in connection with near misses and incidents in automated systems.

Table 12 Other input from the industry.

	Input from interviews/workshop	SINTEF's remarks
1.	It is challenging for personnel to deal with more and more features which provide decision support, such as a recommendation to operate three times faster.	• Who makes this decision and who is responsible? • Could it impact on other systems? • How can we assess (quantify) reduced/increased risk in such contexts?
2.	It is important to have good user interfaces. Good presentation (HMI) is essential to ensure that the operator does not misunderstand the situation or make decisions based on the wrong information.	• How can we ensure adequate user involvement?
3.	Preventive maintenance and monitoring functions generally work well on the Norwegian continental shelf and help to reduce the number of incidents. However, it is apparent that uptime is frequently given greater priority than maintenance (from a vendor's perspective). Problems relating to old or poorly maintained equipment gradually arise, particularly when the willingness to invest is low.	It is possible to strike a good balance between overcoming challenges in the short term and a holistic approach in the longer term.
4.	Much is about ownership and a willingness to adopt new things. New solutions may be better adapted to the competence of the new generation of people who will use them.	How can we secure ownership at all levels?
5.	There are no requirements regarding training concerning automated systems. This could lead to degraded situational awareness.	Could the standardisation of training contribute to better system understanding amongst drillers and other technical personnel?
6.	Adopting new systems time after time, and this results in a lot of reporting because the systems have not been tested in advance, and this could have been better – the industry's problem is that the quality of what is being taken into use is not good enough.	• Is there an adequate system for requirements regarding testing in advance? • Or is the main challenge the fact that it is difficult to predict situations to test for?
7.	There are few formal requirements for drillers other than the well certificate. The industry believes that there is a need for more training concerning the use of automated systems, and perhaps also vendor-specific systems, as there is a belief that different systems that perform similar functions have very different user interfaces?	• Reassess the formal requirements for the competence of drillers in addition to the well certificate.

4.8 What reporting systems are in use in industries other than drilling?

As part of the study, an overall review of the systems used for reporting incidents in automated systems in the following industries was carried out:

- Aviation
- Road transport
- Maritime shipping
- Rail
- Power supply

The review, which was conducted by SINTEF researchers with special expertise in the individual industries, is documented in Appendix A-F.
Table 13 provides a general overview and summary of the results of this survey.

Table 13 Reporting of incidents in other sectors.

Sector	How are they detected?	How are they reported?	What is reported/how are they classified (criticality)?	How are they followed up?
Aviation	Each aircraft's Flight Data Monitoring (FDM) system records operational data during a flight. An external analytics company will report deviations in operational data to the airline after each flight. In addition - manual detection by pilots.	Incidents are reported to the authorities through Altinn.	Operational FDM data is divided into three levels.	"Minor issues" in FDM data are followed up through, for example, an automatic e-mail to the pilot. In the case of serious deviations, representatives of the airline will be involved in further follow-up of incidents. An external analytics company will send summary reports to the airlines in accordance with individual agreements.
Road transport	Modern cars record operating data which is transmitted "Over the air" to the manufacturer. Modern cars automatically report accidents to the nearest “110 centre” (emergency centre) via eCall, which is a common European emergency reporting system. Road users can report accidents using an "SOS button". In the USA, road users can use a hotline for reporting safety issues.	FOR-2005-06-30-793 [34]: The "Regulations on public investigations and reporting of road traffic accidents, etc." contain a number of requirements regarding this. There is no automatic reporting to authorities by road users. The Norwegian Police and the Norwegian Public Roads Administration notify and report to the	Manufacturers classify and report technical faults in their maintenance systems.	Manufacturers store operational data, which is reviewed by the manufacturer's analysis team. Only manufacturers follow up on operational data, and authorities do not have access to this data.

Sector	How are they detected?	How are they reported?	What is reported/how are they classified (criticality)?	How are they followed up?
		Norwegian Safety Investigation Authority concerning serious road traffic accidents and/or serious road traffic incidents		
Maritime shipping	Low degree of automatic detection	Companies must submit reports verbally immediately and in writing within 72 hours concerning maritime accidents to the Joint Rescue Coordination Centre (JRCC), the Norwegian Maritime Authority and the Norwegian Coastal Administration, depending on the type and severity of the incident. Technical faults are only reported to the authorities if they are an important cause of an accident.	Companies classify and report technical faults in their maintenance systems. Companies classify and report accidents and incidents according to a number of characteristics (e.g. type of accident: Fire, Grounding, Loss of propulsion, etc.).	Follow-up of technical incidents is handled internally by the companies. Accidents are included in public statistics. The class companies follow up technical incidents on vessels. In the case of incidents which lead to an investigation report, technical findings are included in the report.
Rail	The European Rail Traffic Management System (ERTMS) continuously collects data on signalling and train speeds. Requirements regarding onboard systems for the continuous collection, storage and use of audiovisual information (audio and video recordings) from the driver's cab when a train is being driven (see IEC 62625-1,-2 and 3) [35].	Manual reporting of incidents by railway undertakings and traffic control centres. HSE&Q incidents and near misses are reported in Synergy. Delays/cancellations are reported via the Traffic and Follow-up System (TIOS). Infrastructure faults are reported in an "AT notification". Bane NOR's whistleblowing channel for reporting irregularities which could result in a risk to life and health.	Synergi and TIOS use "cause codes". Bane NOR's whistleblowing channel requires a description of the circumstances, the time of the incident, source for more information, and anything else that may be useful.	Automatic handling of deviations in ERTMS.

Sector	How are they detected?	How are they reported?	What is reported/how are they classified (criticality)?	How are they followed up?
Power supply	Equipment in the OT networks automatically provides a list of assets, software versions, etc. Failure and interruption statistics across the entire network are recorded. Virtual Desktop Infrastructure (VDI) automatically detects attempted internet attacks. The level of use of Intrusion Detection Systems (IDS) varies internally within power systems. Many incidents are detected manually.	VDI alerts are sent automatically. Grid companies report incidents manually to KraftCERT.	Advanced Persistent Threats (APT) must be reported to NSM. In accordance with the Regulations relating to security and emergency preparedness in the power supply sector, units in the power supply sector's emergency preparedness organisation (*Kraftforsyningens beredskapsorganisasjon,* KBO) must notify [KraftCERT] of a wide range of faults, including cases of attempted intrusion in the operating control system and interruptions in distribution. Power outages are classified on the basis of time (after two hours), but there is no classification of data breaches.	Follow-up in VDI is not publicly disclosed.

The table shows that a number of industries have developed systems and processes which provide automatic reporting and the storage of incidents in control systems.

Although today's industrial automation and control systems in drilling operations are able to record and report time-stamped process values, incident data and calculated data, in addition to system and application data (ref. the requirements of NORSOK I-002:2021 [33]), other industries have progressed further with the automatic reporting and analysis of data.

Some learning points based on the review of reporting systems on both production facilities and in industries other than the petroleum industry are:

- Use of more detailed and standardised taxonomies for incidents which facilitate automatic reporting and classification of deviations (ref. PDS forum/APOS, Chapter 2.4.7). Common equipment categories and taxonomies, including detection methods and failure modes, are particularly important for learning across companies.
- Facilitate automatic follow-up and handling of deviations (ref. rail, Appendix D)
- Give vendors greater access to operational data for review by vendors' analysis teams (ref. road transport, Appendix B).

- Give external analysis companies access to operational data (ref. aviation, Appendix A). Analysis companies will be able to report deviations and follow up through, for example, automatic e-mails to the relevant personnel, and prepare summary reports at set intervals.
- Introduce systems for the continuous collection, storage and use of audiovisual information (ref. rail, Appendix D). Audio and video recordings will be useful for the causal analysis of incidents which have occurred.

5 How can our understanding of undesirable events be established and systematised and converted into learning and improvement?

One of the objectives of this report was to propose how the reporting of ICT incidents and near misses can be established and systematised in the petroleum sector. This chapter discusses other proposals regarding how an understanding of undesirable incidents can be established, systematised and converted into learning and improvement.

Figure 14 shows various activities which form part of a learning process after an incident has occurred, from reporting and investigation, to further follow-up and learning within the companies involved. As regards automated systems in drilling, the results of this preliminary study may indicate that there is potential for improvement in terms of both the reporting/investigation of incidents and measures/learning.

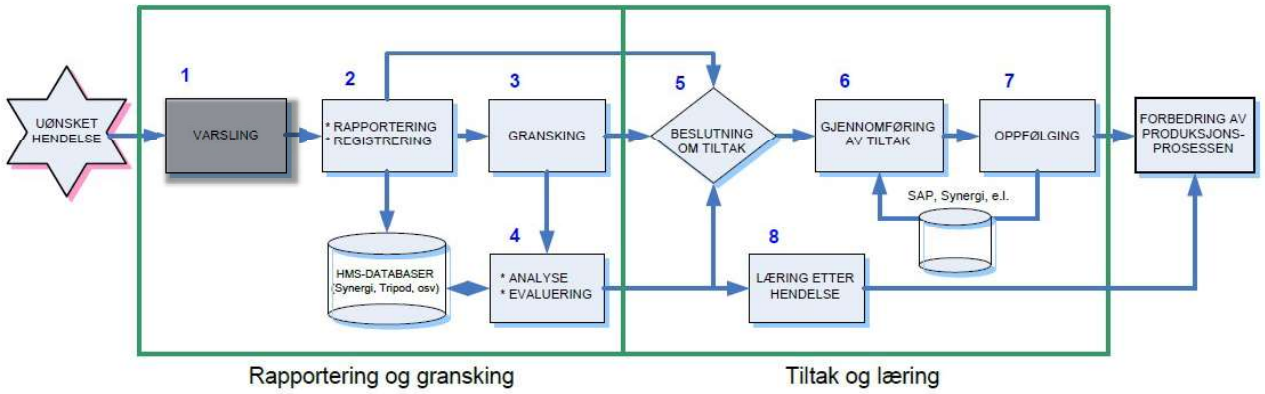


Figure 14 Flowchart for incident follow-up [36].

A lot of data is available on the reporting page, but in some cases there is a lack of systematics and guidelines as regards what data should be logged, what the threshold and criteria for reporting should be, and how and where the reporting should be done. This is particularly true for deviations and near misses, but it also applies to incidents to some extent too. Chapter 2.4.7 described a guideline [30] for the standardised reporting of errors in instrumented safety systems in the petroleum sector, and there appears to be a need for similar guidelines for automated systems in drilling operations. In this regard, Table 3 could be used as a starting point in order to establish an understanding of what data can or should be logged to facilitate the best possible detection and learning. There is a desire within the industry for reporting to take place automatically to a greater extent. Guideline [30] referred to above also includes suggestions regarding how a higher degree of automated reporting can be achieved. In addition, experience of the use of drilling recorders can be used to assess how data from this system can be exploited and followed up in an even more systematic way than is the case at present (see the requirements of the revised NORSOK I-002) [29]. In this regard, there is also the possibility of obtaining input from, for example, aviation and experience of the use of Flight Data Monitoring (Appendix A.1).

In order to bring about a standardised reporting system, many pieces need to be put in place, one in particular being that the actors themselves take ownership of the establishment and use of the system. It is important that the system is easy to use, but this can be a challenge if one system is to capture every type of deviation, near miss and incident for all the actors involved. In the aviation sector, NASA has developed a voluntary reporting system that personnel from different actors can use. This can be used to obtain an indication of how reporting across actors is working; see Appendix A.3.

To facilitate the development of both standardised guidelines for reporting for automated systems in drilling operations, and facilitate experience sharing across actors, a joint interest body may be an appropriate step for actors involved in drilling and well operations. The PDS forum, which is discussed in Chapter 2.4.7, is one example of such a cooperation. The main aim of the PDS Forum is to provide a professional meeting place for the exchange of experience between vendors and users of control and safety systems. This has resulted in a number of collaborative and improvement projects over the years, including the ongoing APOS project (see Chapter 2.4.7).

"Learning means that something changes, for example that a task is performed in a different way than before."

Safety Forum, 2019 [37]

A key challenge in the work relating to learning after incidents and near misses is the transition between reporting and investigation on the one hand, and measures and learning on the other.

"Learning means that something changes, for example that a task is performed in a different way than before." The sharing of information and other forms of experience transfer are important steps on the road to learning, but they are not learning in themselves. It is only when something changes that a lesson has been learnt" [37].

Chapter 4.6 presents findings relating to how incidents and deviations are analysed. Most of the findings dealt with arenas for experience sharing, while less focus was placed on improvement and learning. Learning can take place at different levels. For example, deviation management is about detecting, reporting, correcting and preventing deviations and incidents, while learning at a more general level can be about:

- Whether the right equipment is available.
- Whether the interaction between onshore and offshore actors is sufficient.
- Whether the right training/expertise is in place.

6 Recommendations

This chapter summarises SINTEF's recommended measures for the industry and the Petroleum Safety Authority Norway, as well as the need for further work relating to knowledge acquisition. The recommendations are primarily derived from the findings in Chapters 4 and 5.

6.1 Recommendations for the industry

Recommended measures for the industry are presented in Table 14.

Table 14 Summary of SINTEF's recommended measures for the industry.

No.	Challenge	Recommendation	Ref.
What is reported/shared			
1.	Few reported incidents limit the possibility of systematic improvement and learning.	Develop and apply methods and systems for the automatic registration and follow-up of incidents based on, amongst other things, experience gained from production installations, as well as other industries such as aviation, road traffic and rail. See also point 4 on establishing a joint interest forum for the industry to secure the exchange of experience across companies.	4.6/4.8
2.	No unambiguous specification regarding which incidents and deviations (clear delimitation) should be reported, and how reported incidents and deviations should be classified.	Establish common guidelines for the industry regarding which incidents and deviations should be reported, and how they should be classified in order to: a) Ensure reporting at the correct level (avoid both over- and underreporting) b) Prevent duplications and extra work c) Bring about competence enhancement across companies d) Prevent the threshold for reporting and further classification from becoming person-dependent e) Facilitate comparable data across companies in order to improve safety, learning and development f) Ensure a clear understanding of roles In order for such guidelines to be appropriate, they must be established by the industry itself. In particular, operator companies which often have a number of vendors in their portfolio can contribute to the initiation of such work.	4.4/5
3.	No category for the classification of ICT incidents.	Introduce a specific category for the reporting and classification of ICT incidents; see point 2 above.	4.1.2
4.	Lack of sharing of information and expertise	Share information across companies concerning incidents, near misses and interventions. Sharing of technical information is recommended for competence enhancement. Facilitate the exchange of experience through the establishment of a joint interest forum for drilling and well (ref. PDS forum).	4.6.1/5
5.	A lot of data is available, but it is not always utilised for learning or improvement.	Use intervention statistics more actively for learning. Extract more information and statistics about incidents and near misses in retrospect (e.g. during operational reviews), for example annually, and use this for learning. Establish more procedures for using deviation and	4.6.1/5

No.	Challenge	Recommendation	Ref.
		incident data for learning and improvement, rather than just for experience sharing.	
Factors which impact on reporting and follow-up			
6.	Lack of confidence in automated systems impacts on their use and results in "unnecessary" user errors.	Actively work on processes to build trust in automated systems. Greater involvement of end users in system development.	4.7
7.	New reporting tasks can steal valuable time/attention from technical personnel/drillers.	Facilitate automated reporting, analysis and sharing of incidents, partly on the basis of experience from other industries (see recommendation no. 1).	4.1/4.3.5
8.	Lack of system understanding, difficult to understand or predict the possible consequences of a deviation under different circumstances.	More simulator training (with error scenarios) could increase understanding and the ability to report. a) Should reporting be given more attention in connection with training? b) Could the standardisation of training contribute to better system understanding amongst drillers and other technical personnel (see recommendation no. 3 to the PSA)?	4.1.2
9.	In connection with manual reporting, it can often be too onerous to fill in a form.	Create simple, recognisable reporting systems with good user interfaces. Use the same system for all incidents and deviations and across companies. The operator companies in particular can contribute to the establishment of a standardised system for the entire industry.	4.3.5
10.	The driller's tasks are constantly changing.	The driller's tasks need to be revised and adapted to take account of a higher degree of automation as more and more aspects of the process are automated.	4.1.2

6.2 Recommendations to the PSA

Recommended measures for the Petroleum Safety Authority Norway are presented in Table 15.
These are preliminary recommendations that SINTEF will continue to work on and update in the final report.

Table 15 Summary of SINTEF's recommended measures for the PSA.

	Challenge	Recommendation	Ref.
1.	Considerable variation within the industry as regards the registration and reporting of ICT incidents.	Be a driving force for the industry in establishing common guidelines as regards which ICT incidents and near misses should be reported, and how these should be classified to ensure future follow-up and learning. Strengthen the follow-up aimed at the roles of different actors in the processing of ICT incidents and near misses, including actors other than operator companies which have a reporting obligation with respect to the PSA.	4.1.2/4.4/5

	Challenge	Recommendation	Ref.
2.	There are few formal requirements for drillers.	Consider whether the PSA's regulations should clarify the need for formal requirements regarding the competence of drillers over and above well certificates. Perhaps there should also be requirements regarding training which is directly linked to vendor-specific automated systems (e.g. two systems which perform similar functions, but have very different user interfaces)? Act as a driving force for the industry in defining common training requirements to avoid different operating companies having different requirements. Reinforce the role of the PSA in the sharing of knowledge and experience concerning the safe design and operation of automatic systems in drilling operations.	4.7
3.	New reporting tasks concerning ICT incidents can steal valuable time/attention away from the driller.	Act as a driving force for the industry in facilitating a higher degree of automatic registration of deviations in automatic drilling systems. Consider referring to the revised NORSOK I-002 in the guidelines to the Management Regulations, Section 19 Collection, processing and use of data.	4.1/4.3.5
4.	The current reporting of ICT incidents and near misses is too general in order to provide a sound basis for learning and future risk reduction.	Act as a driving force for the industry in working more systematically with regard to the reporting and processing of ICT incidents for own learning and future risk reduction.	4.4/5

6.3 Need for knowledge acquisition

The purpose of this report is to provide the industry and PSA with greater insight into how incidents, near misses and deviations within automated systems are currently registered, processed, classified and, where appropriate, further reported to the PSA, as well as the roles of various actors in the processing of such situations. Information has also been collected on the handling of incidents and deviations in other relevant industries, as a basis for proposing how to establish and systematise the reporting of incidents and deviations in automated systems, control systems and interlinked solutions in the petroleum industry. The results are based on a document review, input from interviews and workshops, as well as internal working meetings.

We consider one of the biggest challenges to be the absence of clear guidelines as regards what deviations, near misses and incidents should be reported, what the threshold and criteria for reporting should be, how and where the reporting should be done, and how they should be analysed and followed up for further learning. There is therefore a need to establish such guidelines.

Furthermore, it is important to ensure that the load on the drill bit does not become excessive, both as regards requirements regarding reporting and in the use of the new automated systems. There is therefore a desire within the industry to introduce a higher degree of automated reporting. To enable this, we

recommend that a study be conducted to specifically look at which systems and processes must be put in place in order to facilitate a higher degree of automated reporting:

- What taxonomies and internal reporting requirements must be put in place to enable the automated reporting of deviations and near misses, including incidents caused by signal errors (false positives) and intentional incidents such as cyber attacks?
- What can already be reported automatically now (e.g. anomaly detection, equipment failure, etc.)?
- What opportunities are there for automated reporting within a short time horizon of 1-5 years and in the longer term (5-10 years)?

At the same time, we believe this should be viewed in the context of looking at how we can move forward with automation in order to make the drilling process more autonomous and therefore less dependent on the driller and other personnel. However, an important step along the way will be to look at how the systems can be improved in order to help drillers, service personnel, engineers, etc. in their daily tasks. For both of these perspectives, it will be necessary to identify new and standardised ways of sharing data and knowledge. There will then be a need to define and develop open standards and solutions which facilitate digital sharing and information exchange for all actors throughout the value chain. Such interoperability could for example be achieved through the implementation of Industry 4.0 (see Chapter 2.4.8) or a similar concept.

References

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

[2] *NORSOK Z-013:2021, Risiko- og beredskapsevaluering, Utgave 3, oktober 2010*.

[3] 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.

[4] Petroleumstilsynet, *Veiledning til Aktivitetsforskriften (25. januar 2019).* .

[5] NSM, *Nasjonal sikkerhetsmyndighet (NSM), 2015. Helhetlig IKT-risikobilde 2015*.

[6] Bridges, W.G., *Gains from Getting Near Misses Reported*, in *Global Congress on Process Safety*. 2012: Houston, Texas.

[7] Riksrevisjonen, *Riksrevisjonens undersøkelse av NVEs arbeid med IKT-sikkerhet i kraftforsyningen, Dokument 3 av 7 2020-2021*.

[8] *PDS forum*. Available from: https://www.sintef.no/projectweb/pds-main-page/.

[9] *PDS metode*. Available from: https://www.sintef.no/projectweb/pds-main-page/pds-handbooks/pds-method-handbook/.

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

[11] NOU, *NOU 2015: 13 Digital sårbarhet – sikkert samfunn — Beskytte enkeltmennesker og samfunn i en digitalisert verden*.

[12] *Britannica Dictionary*. Available from: https://www.britannica.com/.

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

[14] Johnsen, S.O., Holen, S., Aalberg, A.L., Bjørkevoll, K.S., Evjemo, T.E., Johansen, G., Myklebust, T., Okstad, E.,Pavlov, A., Porathe, T., *Automatisering og autonome systemer: Menneskesentrert design*. 2020.

[15] Safetec, *Petroleumstilsynet: Et menneskesentrert perspektiv på kognitiv teknologi i petroleumsindustrien.* 2021.

[16] SINTEF, *IKT-sikkerhet – robusthet i petroleumssektoren II*.

[17] Ottermo, M.V., Bjørkevoll, K.S., Onshus,T., , *IKT-sikkerhet – Robusthet i petroleumssektoren 2020, Bruk av modeller i boring*. 2021.

[18] *NS-EN ISO 14224, Petroleumsindustri, petrokjemisk industri og naturgassindustri - Innsamling og utveksling av pålitelighets- og vedlikeholdsdata for utstyr*. 2016.

[19] *NS-EN ISO 20815:2018, Petroleumsindustri, petrokjemisk industri og naturgassindustri - Regularitet og pålitelighetsstyring*

[20] Øien, K., Bernsmed, K., Petersen, S, *IKT-sikkerhet - Robusthet i petroleumsindustrien: Kommunikasjonssystemer for ekstern nødkommunikasjon* Ptil, Editor. 2021.

[21] *ISO/TR 12489:2013 Petroleum, petrochemical and natural gas industries — Reliability modelling and calculation of safety systems*.

[22] *IEC 61511 Functional safety - Safety instrumented systems for the process industry sector*. 2016.

[23] NOROG070, *Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry (Recommended SIL requirements)*. 2020.

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

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

[26] *ISO 31000:2018 Risikostyring – Retningslinjer, Utgave 1, April 2018*.

[27] Myklebust, T., Onshus,T., Lindskog, S., Ottermo, M.V. og Bodsberg, L, *Data safety, sources and data flow in the offshore industry*, in *ESREL*. 2021: Angers, France.
[28] *NORSOK D-010:2010, Brønnintegritet i boring og brønnoperasjoner, Utgave 5, januar 2021*.
[29] *NORSOK I-002:2021, Sikkerhets- og automasjonssystemer (SAS), Utgave 2, mai 2001.*
[30] Hauge, S., Håbrekke, S., Lundteigen, M.A., *Guidelines for standardised failure reporting and classification of safety equipment failures in the petroleum industry, Version 4*. 2020.
[31] Ottermo, M.V., Håbrekke, S., Hauge, S., Bodsberg, L., *Technical Language Processing for Efficient Classification of Failure Events for Safety Critical Equipment*, in *PHM Society European Conference*. 2021.
[32] *Plattform industrie 4.0 Interoperability – Our vision for Industrie 4.0: Interoperable communication between machines within networked digital ecosystems.* .
[33] Salmon, P.M., Walker, G.H., Stanton, N., *Pilot error versus sociotechnical systems failure? A distributed situation awareness analysis of Air France 447.* Theoretical Issues in Ergonomics Science, 2016. **16**(1): p. 64-79
[34] *FOR-2005-06-30-793: Forskrift om offentlige undersøkelser og om varsling av trafikkulykker mv.*
[35] *IEC 62625-1:2013 Electronic railway equipment - On board driving data recording system - Part 1: System specification*.
[36] *HMS-ytelse – Hendelsesoppfølging. Gjennomgang av Ptils brukerrapport (2007)*.
[37] *Rapport fra Sikkerhetsforum, Læring etter hendelser*. 2019.
[38] Yan, J., *Identifying Opportunities of Tracking Major Human Factors Risks through Flight Data Monitoring. UWSpace.*, in *Systems Design Engineering*. 2014, Waterloo.
[39] Luftfartstilsynet. 2021; Available from: https://luftfartstilsynet.no/aktorer/flysikkerhet/rapportering/important-information-about-occurrence-reporting/.
[40] *Aviation Safety Reporting System*. Available from: https://asrs.arc.nasa.gov/index.html.
[41] *Forskrift om utprøving av selvkjørende motorvogn.* 2017.
[42] *SAE J3016:Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*.
[43] *SAE J 2980-2015: Considerations For ISO 26262 ASIL Hazard Classification.*
[44] *UL 5500: Standard For Safety For Remote Software Updates, Ed. 1-2018*. 2018.
[45] *ISO/DIS 24089: Road vehicles — Software update engineering, draft.*
[46] *ISO/IEC AWI TR 5469 Artificial intelligence — Functional safety and AI systems, draft.*
[47] *PAS 1882:2021: Data collection and management for automated vehicle trials for the purpose of incident investigation. Specification.* 2021.
[48] *LOV-1981-03-13-6: Lov om vern mot forurensninger og om avfall (Forurensningsloven)*.
[49] *LOV-2001-06-15-79: Lov om miljøvern på Svalbard (svalbardmiljøloven).*
[50] Kystverket. *Varslingsinstruks*. Available from: https://www.kystverket.no/oljevern-og-miljoberedskap/beredskapsvakt/.
[51] *Forskrift om endring i forskrift om melde- og rapporteringsplikt ved sjøulykker og andre hendelser til sjøs*. Available from: https://lovdata.no/dokument/LTI/forskrift/2012-12-10-1188.
[52] *Sjøloven*. Available from: https://lovdata.no/dokument/NL/lov/1994-06-24-39?q=sj%C3%B8loven.
[53] *Skipssikkerhetsloven*. Available from: https://lovdata.no/dokument/NL/lov/2007-02-16-9?q=skipssikkerhetsloven.
[54] *FOR-2011-04-11-389: Forskrift om sikkerhetsstyring for jernbanevirksomheter på det nasjonale jernbanenettet (sikkerhetsstyringsforskriften).*
[55] *IEC 62625-2:2016 Electronic railway equipment - On board driving data recording system - Part 2: Conformity testing.*

[56] *NIS-direktivet: Europaparlamentets og Rådets direktiv (EU) 2016/1148 av 6. juli 2016 om tiltak som skal sikre et høyt felles sikkerhetsnivå i nettverks- og informasjonssystemer i EU*. Available from: https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2014/sep/nis-direktivet/id2483374/.

Appendix - What reporting systems are used in industries other than drilling?

A Aviation

A.1 Flight Data Monitoring (FDM)

Flight Data Monitoring (FDM) is a sensor-based aviation system which collects large quantities of sensor data from an aircraft during a flight. There can be up to several hundred sensors, depending on the type of aircraft. More specifically, FDM is about identifying, quantifying and assessing risks associated with the execution of flights on the basis of deviations between practice and standardised operating procedures.

FDM is statistics-based, and the data that is collected is continuously stored in databases and analysed after flights to identify specific incidents where the aircraft was flown in a way which exceeded certain values, and to identify any suboptimal trends in the way in which it was flown. If FDM parameters exceed predefined values, it will trigger some form of follow-up from the analytics organisation and/or the airline, depending on the severity of the issue. The starting point for the analysis of FDM is three levels which are defined in advance by the airlines. The levels and values that are set may vary from company to company, but level three always constitutes a serious incident, which involves a breach of one or more procedures. Level one could for example be movement on the ground that is somewhat higher than desired.

Through the helicopter safety studies conducted by SINTEF for the Norwegian Oil and Gas Association, the analysis of FDM data is related to the topic “offshore helicopter safety”. An example from this and level one is the identification of an undesirable trend in one of the companies regarding helicopters during take-off, more specifically an undesirable low nose position which involved take-offs with a nose position of 20 degrees below the horizon. This was an undesirable trend that was addressed before it could escalate. The helicopter operators point out that FDM is a very useful tool for stopping negative trends at an early stage.

The actual analysis and organisation of how FDM analyses are followed up internally varies somewhat from company to company, but strict rules and procedures apply when pilots are directly involved, usually relating to level three incidents. This is about sensitive material and privacy, which also involves employee representatives. FDM data must also not be used to punish individual pilots retrospectively, or be handed over to other actors. Follow-up based on the analysis of FDM data should only be carried out for learning purposes.

At the same time, little research has for example been conducted regarding how FDM data can be used proactively to better understand incidents and contexts in which human performance and human-automation technology are important. In such a context, FDM data could potentially be used to investigate how different factors which impact on human performance are made visible through variations in different FDM parameters. In this context, Yan (2014) [38] points out how FDM has the potential to better understand risks relating to, for example, a lack of follow-up of rules, lack of situational awareness and high workload. Yan (2014) [38] identifies seven flight parameters, as well as how FDM data can be used to monitor risks associated with human factors, such as how FDM data can be used to monitor “automation confusion” [38].

The application of FDM data in aviation is essentially a reactive approach to safety by identifying and following up, with respect to crew members, undesirable incidents where a significant deviation from the aforementioned predefined sensor values has been recorded. At the same time, the analysis of FDM data also involves a proactive approach to aviation safety by introducing measures in the event of undesirable trends with a focus on learning from incidents, which involves not pointing to individuals per se and apportioning blame.

A.2 Reporting of incidents and accidents to the authorities

Regulations

The starting point for the reporting of incidents and accidents ("occurrences") is linked to Regulation (EU) No 376/2014 of the European Parliament and of the Council, which deals with the reporting and investigation of accidents and incidents in aviation - this Regulation entered into force in Norway on 1 July 2016. This has resulted in national provisions, BSL A 1-3, being replaced by pan-European legislation through Commission Regulation (EU) No 2015/1018, where provisions pursuant to Regulation No 376/2104 have been issued [39].

The regulations cover all aviation organisations and their employees or hired personnel. Organisations must be able to report aviation occurrences through their own internal systems, including the receipt of reports, analysis and follow-up. Risk and quality management must be based on company-specific safety management systems.

What is reported

In aviation, all occurrences must be reported to the civil aviation authorities, more specifically the Norwegian Civil Aviation Authority. The Civil Aviation Authority defines an occurrence within aviation as an operational issue, failure or other form of irregularity relating to operations which impact on aviation safety [39]. There is a deadline of 72 hours to submit a report after an accident or incident has occurred, or alternatively 72 hours after the organisation becomes aware of what has happened. This reporting takes place through Altinn.

Examples of occurrences which must be reported are cases where the crew misinterprets an automation mode or other information which is received in the cockpit, which in turn could lead to a danger to aircraft or persons. Loss of situational awareness is also mentioned, including losing an overview of the environment within which one is operated, which relates to spatial disorientation and poor time perception. Another example is the technical loss of redundancy in a system, such as malfunction or the failure of an indicator, which in turn leads to misleading information being given to the crew.

Who is responsible

This is linked to who is subject to the reporting obligation, which is viewed in the context of a number of different roles. It could be the captain on board the aircraft, or other crew members if the captain is unable to submit a report him- or herself. Persons involved in the design, construction, airworthiness or continuous maintenance of aircraft are also subject to the reporting obligation. In the same way as those persons who, for example, carry out various forms of inspections to determine the airworthiness of an aircraft. Furthermore, there is a reporting responsibility which provides air traffic services, including the air traffic control service. Persons who carry out ground services (refuelling, cargo documentation) in and around an aircraft are also responsible for reporting.

The Norwegian Civil Aviation Authority (CAA) points out that the reporting obligation and the fulfilment thereof must always be viewed in the context of compliance with the principle of a "just culture" within the aviation industry.

A.3 Voluntary reporting of incidents

In the USA, NASA has developed a voluntary reporting system which actors in the aviation sector can use (see the figure below) [40].

Figure 15 Voluntary reporting system for the aviation sector developed by NASA.

B Road transport

B.1 Introduction

Norway was one of the first countries to draw up a separate law in 2017 for the "Testing of autonomous vehicles" [41]. Through permits for the testing of autonomous vehicles, the Norwegian Public Roads Administration applies applicable Norwegian legislation and associated regulations.

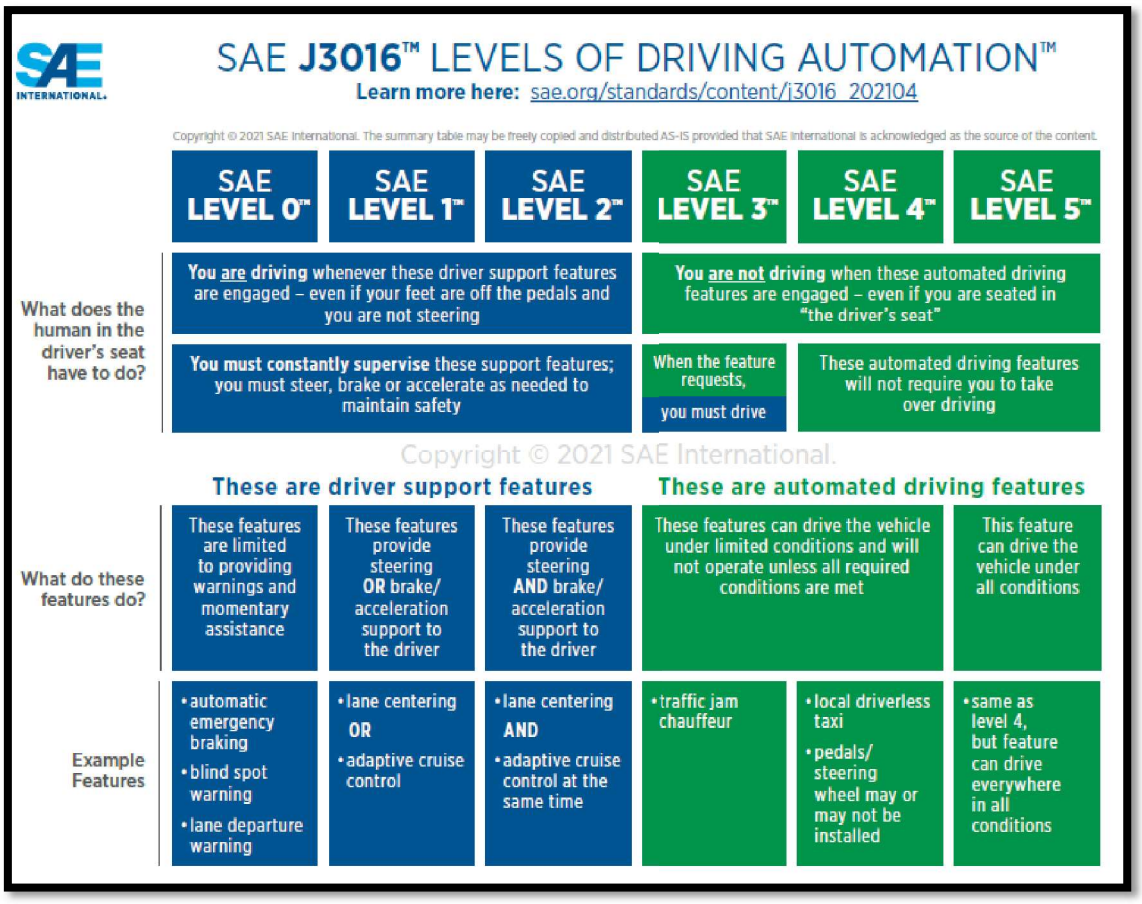
SIS functions are often included in vehicles without being part of the approval.

In Europe, the vehicles are approved in one of the EU/EEA countries. The vehicle can then be used in every country.

Amongst legislators and in the media and various legal court cases, there has been a lot of discussion concerning "AutoPilot". The discussion concerns the responsibility of the driver and how autopilot is advertised by the manufacturer.

The table below shows different degrees of automation and autonomy in road transport.

Table 16 Different levels of automation, SAE J3016 [42].



Within the field of road transport, it is natural to distinguish between cars with built-in automatic functions and autonomous buses.

As regards cars with automatic functions and "SIS", current SILx (called ASILx, where the “A” stands for “automotive”) have been proposed, but these are only specified in a somewhat obsolete standard from SAE, J2980:201804 [43].

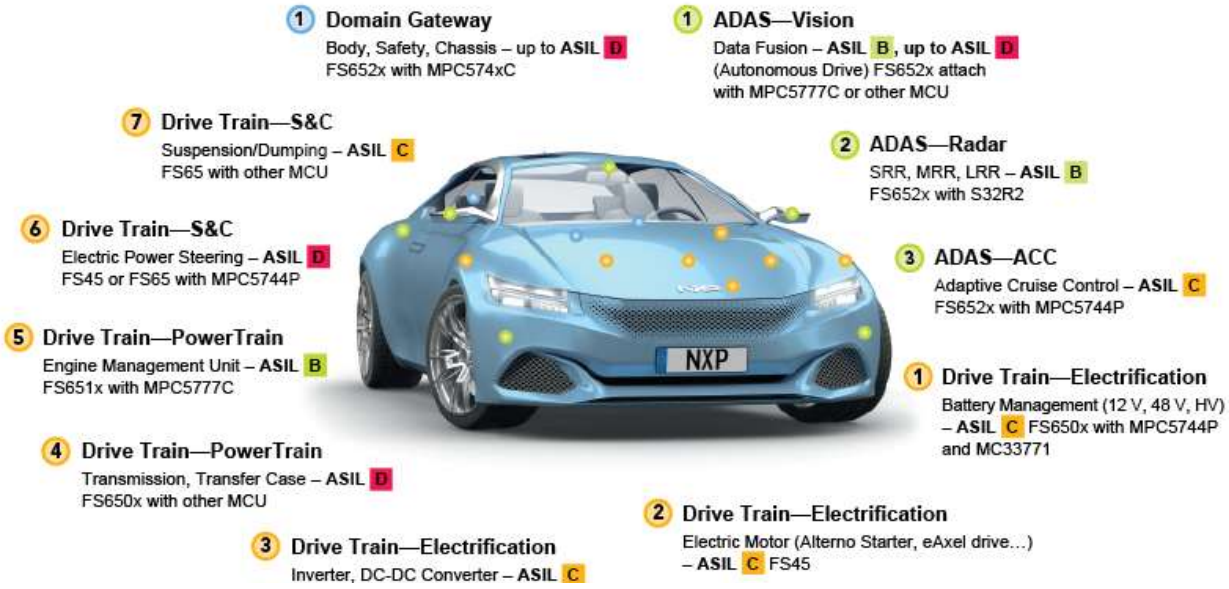


Figure 16 Automotive and current "SIS" and associated ASILx.

B.2 Reporting systems, collection and classification

In recent years, more and more cars have been equipped with Over The Air (OTA) systems. Manufacturers use this for a variety of purposes, including the updating of data and software. Authorities and other bodies do not normally have access to this data. However, in cases where accidents relating to these automatic functions occur, information is disseminated around the world via the media within a few hours.

A standard has been published for OTA; "UL 5500:2018 Standard for safety, remote software updates" [44]. In addition, ISO is preparing a corresponding standard: "ISO/DIS 24089 draft CD Software update engineering" [45].

Manufacturers use OTA both to monitor driving and for software updates (also known as DevOps). ISO and IEC are now developing a new standard ISO/IEC TR 5469 [46] for functional safety and artificial intelligence. Manufacturers have been able to update these systems without further approval even though the update included safety systems. Tightening is under way in this field through requirements regarding software updates issued by UNECE. These requirements will probably be incorporated into future legislation.

When the software in cars is updated, the owner will receive an updated version of the user manual, for example. The version number may be shown on the display in the vehicle. It is up to the individual driver to familiarise him- or herself with the new version. It is important to note that, according to the user manual, it is the driver who is responsible. This is why automotive manufacturers avoid the responsibly and drivers are left in the responsibility.

In the USA, NHTSA has established a "hotline", via which perceived vehicle safety issues (tyres, car seats or equipment) can be reported. You can submit a complaint, which will then be reviewed by NHTSA.

NHTSA (**) has also established a voluntary system for reporting from authorities and companies concerning experiences from the testing of automated vehicles, as part of the "AV TEST initiative". Manufacturers of automated driving systems improve their systems through validation in internal tests and simulations with controlled testing on public roads.

eCall is a pan-European emergency notification system for reporting road traffic accidents. If a vehicle equipped with eCall is involved in a road traffic accident, a notification will automatically be sent to the nearest “110 centre” (emergency centre). More and more vehicles are now equipped with an SOS button which is connected to eCall. You can also notify manually by pressing the SOS button, but this button should only be used in a genuine emergency.

The country's 110 centres spend a lot of time dealing with unnecessary alarms from new cars. In 2020, the fire service had to deal with 4,405 such alarms. 92% of these alarms were false.

Vehicle projects based on permits from the Norwegian Public Roads Administration:
The decision that the operator receives before trial operation is commenced states the following (this is an adapted example. The requirements can be changed from project to project):

> *The responsible company shall ensure that a continuous log is kept as described in Section 12 second paragraph of the Regulations relating to the testing of autonomous motor vehicles. We therefore request access to a data log which can show the movement pattern of the vehicle towards the end of the commissioning phase. If the safety measures do not work as intended or other circumstances arise with regard to safety and accessibility, the applicant shall immediately notify the local authorities and the Norwegian Public Roads Authority*.

BSI published its own document earlier this year: PAS 1882:2021, Data collection and management for automated vehicle trials for the purpose of incident investigation [47], which specifies requirements regarding the collection, storage and sharing of information during trials of autonomous cars in the United Kingdom. The goal is to help organisations which conduct trials involving autonomous vehicles to collect data in a standardised format.

Vehicles generally:
In Norway, there is a specific regulation on the notification and reporting of road traffic accidents and incidents: FOR-2005-06-30-793: Regulations on public investigations and reporting of road traffic accidents, etc. [34].

> *"Section 4. Immediate reporting of serious road traffic accidents and incidents*
> *The Norwegian Police and the Norwegian Public Roads Administration shall immediately notify the investigating authority of any serious road traffic accidents which:*
> *a) have occurred in a tunnel*
> *b) involve a bus or vehicle with a total weight exceeding 7.5 tonnes,*
> *c) involve a vehicle which is transporting dangerous goods (ADR).*
>
> *The Norwegian Police and the Norwegian Public Roads Administration shall also immediately report serious road traffic accidents and/or incidents:*

d) which are covered by specified criteria set by the investigating authority, and where this authority has requested such notification in writing, or

e) which they believe, on the basis of an overall assessment, the investigating authority may have an interest in investigating; see Section 3, first paragraph.

Notification must be given via the investigating authority's specified hotline.
If notification is given by the Norwegian Public Roads Administration, the Police shall be notified of the notification immediately.

Section 5. Reporting of serious road traffic accidents and incidents
As soon as possible, the Police shall submit a written report to the investigating authority on all traffic accidents and incidents that are subject to mandatory notification pursuant to Section 4. The Police's "Report on road traffic accidents" may be used as a report pursuant to this provision."

C Maritime shipping

In maritime reporting, a distinguish is made between internal and external reporting:

Internal reporting	Reporting onboard a vessel Reporting to the company and own fleet Reporting to system vendors/class (engine manufacturers, etc.)
External reporting	Reporting to authorities Mandatory reporting in connection with incidents

C.1 Internal reporting

Current practice is for internal reporting only within operator and/or owner companies (shipping companies), as well as to class companies. At the time of writing, we are unaware of any common independent database, but class companies such as DNV, Lloyds, ABS etc. have their own databases based on the ships for which they provide class services. There are significant differences in the way in which reports are submitted, and the sector is generally in a maturation phase as regards the collection and use of data. A lot is measured, but few have an overview of quality and needs. The SFI group system is the most widely used method for the technical follow-up of ships, a method which first saw the light of day back in 1972 and was developed by SFI: Skipsteknisk Forskningsinstitutt, which became MARINTEK, which in turn has now become SINTEF Ocean). The method has been continuously improved and is now maintained by SpecTec.

The SFI Group System is the most widely used classification system in the maritime and offshore industry globally. It is an international standard, which provides a functional subdivision of technical and financial ship or rig information. SFI consists of a technical account structure which covers all aspects of ship/rig specifications. It can also be used as a basic standard for all systems in the shipping/offshore industry. More than 6,000 SFI systems have been installed worldwide. SFI is used by shipping and offshore companies, shipyards, consulting firms, software vendors, government agencies and classification.

Figure 17 SFI Quality loop.
Source: SFI Group system

The SFI Group System is divided as follows:

- Primary group 1 - General
- Primary group 2 - Hull systems
- Primary group 3 - Cargo equipment
- Primary group 4 - Ship equipment
- Primary group 5 - Crew and passenger equipment
- Primary group 6 - Main components of the machine
- Primary Group 7 - Systems for the main components of the machine
- Primary Group 8 - Common Systems

The two groups that stand out as being most relevant to this report are:

- Primary group 6 - Main components of the machine: Primary components of the engine room, such as main and auxiliary engines, propellers, systems, boilers and generators.

- Primary Group 7 - Systems for the main components of the machine: Systems which serve main components, such as fuel and lubrication systems, air starting systems, exhaust systems and automation systems.

C.2 External reporting

C.2.1 Reporting in conventional shipping

Within Norway's maritime segment, it is incidents which determine the reporting requirement. Accidents and near misses must be reported to the various agencies, based on the type of incidents that must be reported. When an incident is serious in nature, an investigation into the incident will be necessary, which will ultimately lead to the preparation of an investigation report.

Amongst other things, the captain or shipping company must report maritime accidents and occupational accidents to the Norwegian Maritime Authority using a designated form within 72 hours of the incident. The reporting obligation applies regardless of whether or not the accident has been reported. The captain or shipping company must verbally provide information on the following, amongst other things:

- loss of ship or life,
- material damage to the vessel or injury to persons,
- occupational accident where the injured person had to be evacuated,
- actual or probable discharges of oil and/or other harmful substances
- fire, explosion, impact or similar,
- grounding and collision.

This also applies when external personnel carrying out work on board a vessel are party to an accident on board or have an accident on board.

Accidents and incidents are classified according to a number of characteristics such as: Capsizing, Collision, Contact with another object, Floating object (cargo/container, ice, other), Flying object, Land-based object), Damage/loss of equipment, Fire and explosion, Water ingress, Grounding, Damage to hull, Loss of control: Propulsion, Electrical, Directional, Not Found, War, Crime, Illegality. It is also important to emphasise that there are different ship categories, ranging from passenger ferries to fishing boats, and from container ships to cruise ships.

Technical faults are not reported, unless they are part of the cause of an accident. There is no common database for collecting technical faults in the maritime sector. It is the vessel's shipping company which collects information about the condition of the vessel, such as the condition of the propulsion mechanisms.

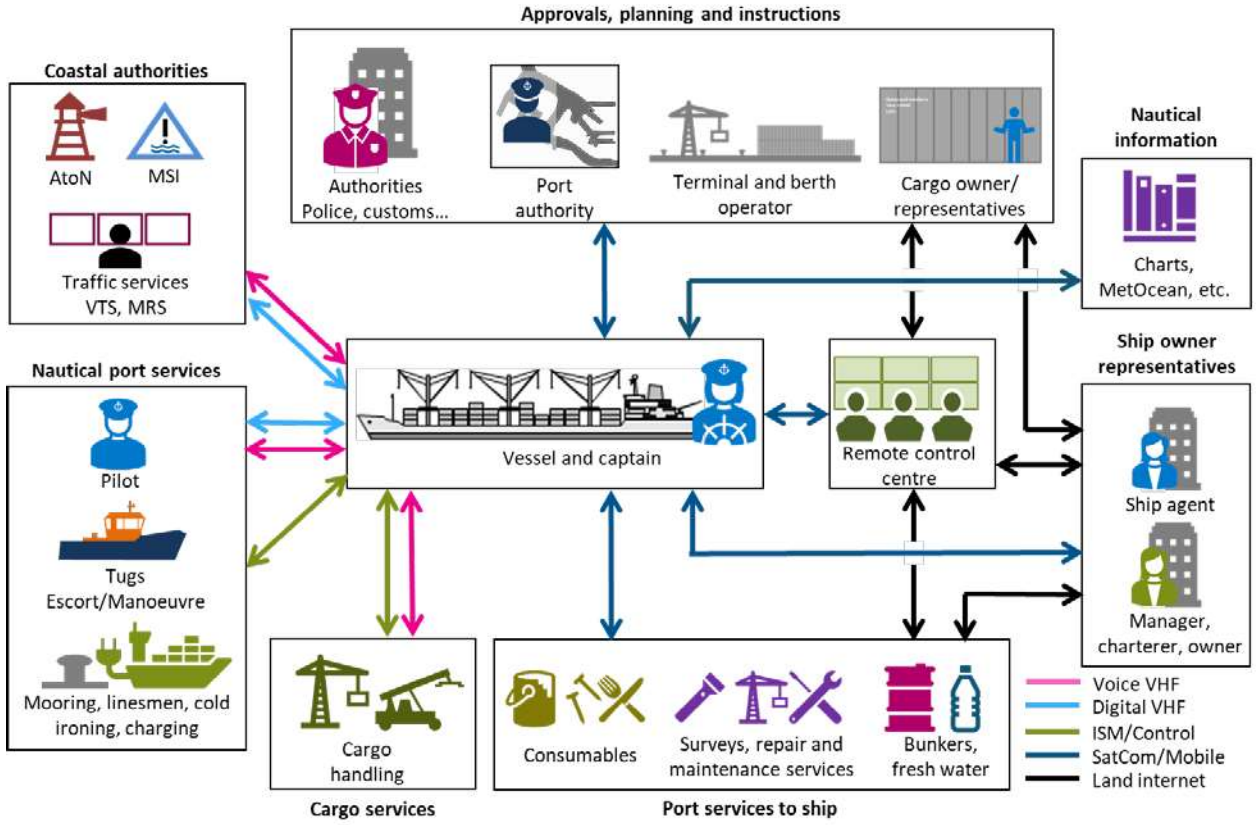


Figure 18 Conventional interaction. Source: SINTEF.

A composite picture of the reporting requirements in conventional shipping is illustrated in Figure 18. The figure shows the information flows for voice, digital and control. The figure is complex, and there are several types of systems involved, some for navigation, others more for status reporting.
In connection with the reporting of incidents, we do not currently have a specific reception centre for technological incidents which are caused by faults in technology or sensors. This is something that the individual companies themselves have, which must be in place for approval granted by the flag state or class, which will also be useful when insurance policies are taken out with insurance companies. Incidents are reported to various government agencies, depending on the nature of the incident. As a general rule, the three agencies Norway, the Norwegian Coastal Administration, the Joint Rescue Coordination Centre and the Norwegian Maritime Authority, have different mandates and areas of responsibility:

- Joint Rescue Coordination Centre: Responsible for the rescue of people.
- Norwegian Coastal Administration: Responsible for limiting the extent of damage when an incident results in discharges into the environment.
- Norwegian Maritime Authority: Responsible for the inspection of vessels and ensuring that vessels have the correct certificates.

C.2.2 Joint Rescue Coordination Centres

The country's two joint rescue coordination centres are located at the Port of Bodø and in a dedicated building in Sola, outside Stavanger. The official designations of the two centres are *HRS Sør-Norge*, Stavanger (Southern Norway) and *HRS Nord-Norge*, Bodø (Northern Norway). As is apparent from the designations, these have overall responsibility for Southern Norway and Northern Norway respectively. The boundaries

of the areas of responsibility follow the 65th parallel north in the marine areas, and the boundary between the police districts of Nord-Trøndelag and Helgeland.

Samlet statistikk Hovedredningssentralen 2020

SJØ			Jan	Feb	Mar	Apr	Mai	Jun	Jul	Aug	Sep	Okt	Nov	Des	Total
	% av Alle	% av Sjø													
Assistanse fartøy	10,8 %	29,0 %	30	42	74	72	92	110	152	92	82	47	31	39	863
Brann - Større fartøy	0,3 %	0,8 %	1	1	1	1		3	1				1		9
Brann - Mindre fartøy	1,2 %	3,2 %	2	5		7	12	16	22	16	4	4	3	4	96
Drivende fartøy/større objekt	0,4 %	1,1 %	5	4	2		2	1	2	1	2	1	6	6	32
Drivende fritidsbåt/mindre objekt	4,2 %	11,5 %	11	8	13	20	36	29	67	48	47	30	22	10	341
Drukning - kantring - UTGÅTT HENDELSESTY															
Dykkerulykke	0,1 %	0,2 %	1					2		3			1	1	8
Akutt forurensning															
Grunnstøting - mindre fartøy	3,0 %	8,3 %	8	7	5	24	22	32	54	28	20	16	15	15	246
Grunnstøting - større fartøy	0,2 %	0,5 %	1	1	3	1	1	2	2			3		2	16
Kantring - slagside	0,8 %	0,8 %	2		3	1	1	1	7	3	1	4	1		24
Kollisjon	0,1 %	0,2 %					1	2	1	3					7
Lekkasje - Mindre fartøy	0,7 %	1,9 %		1	3	2	5	14	14	8	3	3	3	2	58
Lekkasje - Større fartøy	0,0 %	0,1 %			1				1						2
MAS	0,5 %	1,3 %	5	4	4	3	1	2	6	1	5	1	2	6	40
MEDEVAC	1,7 %	4,7 %	11	10	11	11	9	9	16	16	13	14	13	8	141
MEDICO	0,4 %	1,2 %	1		6	2	3	4	5	2	4	4	2	3	36
MOB-drukning	1,2 %	3,3 %	4	3	5	9	9	15	17	11	12	3	5	6	99
Nødsignal - DSC	0,2 %	0,6 %	1		1		1	3	3		2	2	1	2	16
Nødsignal - Inmarsat	2,6 %	7,2 %	18	16	15	10	13	19	25	20	26	13	19	19	213
Nødsignal - Pyroteknisk	0,8 %	2,4 %	7	4	5	6	4	3	12	10	3	4	8	5	71
Nødsignal - Telekomm	0,4 %	1,0 %	4	1	2		2	1	4	7	5		2	1	29
Nødpeilesender - EPIRB	4,8 %	13,4 %	39	29	30	22	34	39	42	37	23	36	34	35	400
Offshorehendelse	0,6 %	1,6 %	2	8	3	4	5	2	6	5	2	3	2	4	46
Savnet fiskebåt	0,0 %	0,0 %					1								1
Savnet fritidsbåt	0,7 %	2,0 %	1	1	3	4	5	9	10	13	5	6	1	1	59
Savnet kommersielt fartøy															
SSAS	0,5 %	1,4 %	6	8	4	3	3	3	1	3	1	4	4	3	43
SUBMISS - SUBSUNK															
Andre - UTGÅTT HENDELSESTYPE															
Udefinert Sjø	1,0 %	2,7 %	4	4	8	6	10	10	6	8	7	4	7	5	79
Sum Sjø	36,8 %	100,0 %	165	157	202	208	272	331	476	335	267	202	183	177	2975

Figure 19 Statistics for the Joint Rescue Coordination Centres 2020 (maritime). Source: Joint Rescue Coordination Centres

The statistics for 2020 indicate that a total of 2,975 incidents were reported. The corresponding figure for 2019 was 3,227, while 3,427 incidents were registered in 2018, and 3,809 in 2017. This applies to both centres. The figures show the distribution based on categories, where assistance provided to vessels covered a total of 863 incidents, while signals from emergency beacons, DSC, Inmarsat, Pyrotechnics (flares) and EPIRB also account for a high proportion. Previous studies have shown that many incidents involving emergency beacons are the result of false alarms, although the percentage in these statistics is uncertain.

C.2.3 Norwegian Coastal Administration

The Norwegian Coastal Administration is the agency that is responsible for maritime transport and traffic monitoring in Norway. The Norwegian Coastal Administration is a transport agency under the Ministry of Transport. The agency's mandate is to ensure safe and efficient traffic in coastal shipping lanes and into ports, and safeguard national emergency preparedness with regard to acute pollution. The most important tasks are:

- Development and maintenance of shipping lanes
- Lighthouse and marking services
- Traffic centre services
- Pilot services
- Messaging services and navigation alerts
- State preparedness with regard to acute pollution
- Development and transport planning
- Port safety (ISPS)
- The Norwegian Coastal Administration is also responsible for the maritime sector of the National Transport Plan (NTP), as well as government and administrative tasks relating to laws and regulations for ports, shipping lanes and the pilot duty.

As regards the reporting of ship information, SafeSeaNet Norway is the portal which must be used to report ship arrivals in Norwegian ports. This portal contains information about vessels, cargoes and planned routes. The portal also contains information on the transport of dangerous goods, which could constitute a risk. SafeSeaNet is connected to similar single window solutions in other European countries.

The Norwegian Coastal Administration also offers a service where they can recommend routes for maritime traffic. This service is called routinfo.no, and currently covers routes from the southernmost tip of Norway up to Vesterålen. The recommended routes have waypoints with position designations (Lat/Lon) which can be used by vessels in their charts (ECDIS), which the vessels can follow during a voyage. These are routes that are recommended based on depth conditions and safe shipping lanes. They do not contain real-time traffic information.

Another service provided by the Norwegian Coastal Administration is Barentswatch. Real-time information about shipping lanes and forecasts can be retrieved from this solution. For example, wave alerts can be obtained and provide a basis for the safe planning of a voyage.

Kystinfo is a service which brings together extensive maritime information. Kystinfo enables information about real-time traffic to be displayed, along with information about historical sailings, a heatmap of traffic in certain areas, and basic marine charts and statistics. The solutions also contain digital port data charts. For example, the coordinates of an anchoring point will be available for certain ports.

Kystdatahuset.no is the starting point for the Norwegian Coastal Administration's initiative to provide both internal and external users with easy and good access to maritime traffic data. Data can be retrieved in two different ways:

1. Kystdatahuset – Menu item "Figures and statistics". Contains various dashboards/queries with maritime traffic data, where it is possible to present the data in maps, figures and data tables. In the dashboards, you can filter and analyse the data. Screenshots can be saved and tables of data exported to Excel.
2. Data sharing portal – Menu item "Data and services". Portal for downloading larger data sets. Use and presentation of the data takes place in the recipient's own tools and solutions. The portal contains a selection of data sets concerning both maritime traffic and other maritime data.

Vessel Traffic Services

The Norwegian Coastal Administration is responsible for the maritime traffic control centre service in Norway (VTS). The Norwegian Coastal Administration has five maritime traffic centres which inform, organise and monitor shipping in defined service areas along the coast. The maritime traffic centres are a risk-mitigation initiative to prevent undesirable traffic situations in defined risk areas with high traffic density and where there is a high proportion of traffic carrying dangerous and/or polluting cargo. The Norwegian maritime traffic control centre service is based on national regulations, international regulations issued by the UN Maritime Organization (IMO) and standards from the International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA).

Emergency preparedness

The Norwegian Coastal Administration is responsible for coordinating central government, municipal and private emergency preparedness. The purpose of emergency preparedness with regard to acute pollution is to protect life, health, the natural environment and commercial interests at sea and on land. In principle, it is the responsible polluter who has a duty to take action in the event of acute pollution. If the responsible party is unable to or will not implement the necessary measures, the public sector, under the Norwegian Coastal Administration, will take over. In the case of incidents which entail a risk of major acute pollution, the Norwegian Coastal Administration may decide that the state should take over responsibility for handling the action. This means that the Norwegian Coastal Administration will then take over responsibility for leading the action both at sea and in the shore zone. Necessary measures will be those which prevent the risk of acute pollution from turning into actual pollution. If pollution has occurred, necessary measures will consist of stopping, removing or limiting the effects of the pollution.

All incidents involving acute pollution or a risk of acute pollution on the mainland must be reported as stipulated in the Notification Regulations (Regulations relating to notification of acute pollution) of 1993, as stipulated pursuant to Section 39 of the Pollution Control Act, the Act relating to protection against contaminants and on waste (the Pollution Control Act) [48] of 1983, and Section 70 [49] of the Svalbard Environmental Protection Act when the pollution occurs or threatens to occur in Svalbard or its surrounding waters. As a general rule, the duty of notification rests with the party that is responsible for the pollution, but anyone who detects acute pollution or a risk of acute pollution is obliged to call the fire service's emergency number (110). In the case of vessels at sea, the nearest coastal radio service or the Joint Rescue Coordination Centre (JRCC) must be notified. For more information on the reporting of incidents, see the Norwegian Coastal Administration's website or the instructions for reporting [50].

The Norwegian Coastal Administration normally receives and processes 1,000 – 1,400 alerts and reports of acute pollution or a risk of such pollution every year. These are logged in the Norwegian Coastal Administration's crisis support tool "KystCIM" and form the basis for statistics on acute pollution. The statistics cover both reported incidents that have led to acute pollution and incidents where there was a risk of acute pollution, but no discharges actually occurred. The figure shows an overview of the number of alerts and discharge volumes (m^3), broken down according to main category processed by the Norwegian Coastal Administration's emergency preparedness team in 2020.

The table shows logged incidents reported to the Norwegian Coastal Administration's emergency preparedness service (both with and without discharges) during the period 2013 - 2020, broken down into different types of incidents.

Loggførte hendelser	2013	2014	2015	2016	2017	2018	2019	2020
Akvakulturanlegg (Oppdrett)	0	0	0	0	0	0	0	3
Andre landbaserte hendelser	37	13	17	33	31	41	10	47
Anleggsarbeid med utslipp	0	5	3	7	6	1	8	8
Drikkevannskilde forurenset	3	2	1	1	0	0	0	2
Drivende gjenstand	99	118	151	175	193	171	106	7
Fartøy i brann	26	18	17	19	20	22	27	18
Fartøy i drift	164	105	101	112	109	104	107	101
Fartøyskollisjon	22	5	10	5	1	2	7	5
Forlis (uten vrakhåndtering, alle fartøygrupper)	8	19	40	34	34	43	28	29
Grunnstøting	77	74	72	65	70	58	52	65
Hydraulikklekkasje (Land)	3	2	3	17	6	49	66	49
Hydraulikklekkasje (Sjø)	8	16	8	22	17	17	29	26
Industri	67	63	72	89	76	38	45	37
Internasjonal varsling og bistand	5	1	1	2	5	3	5	2
Kontaktskade (kai, bro, etc.)	10	20	15	10	12	10	14	10
Landbruk	11	11	13	13	18	12	16	22
Landtransport	137	97	127	171	129	100	126	112
Luftfart – Overbunkring, lekkasjer og fuel drop	1	0	3	3	2	0	0	1
Lufttransport	0	0	0	2	0	0	0	2
Maskinfeil (fremdrift eller styring)	0	3	4	8	2	8	5	2
Naturhendelse	4	4	5	1	1	5	3	3
Navigasjonsinstallasjoner	23	11	5	8	3	3	3	0
Observert mulig akutt forurensning i vassdrag (ukjent kilde)	11	10	6	12	9	21	19	8
Observert mulig akutt forurensning på sjø (ukjent kilde)	220	144	97	133	120	97	90	86
Offshore	159	165	178	222	246	103	63	72
Sjøpattedyr	4	5	5	7	3	9	3	8
Tankanlegg, tank og fat - lekkasjer og overfylling	48	61	66	52	75	115	96	97
Transformator og sjøkabel	2	3	1	7	1	6	7	2
Utslipp fra fartøy til sjø	11	28	30	28	37	28	17	20
Utslipp fra land til sjø	0	1	3	6	2	1	2	1
Utslipp til luft (gass)	4	3	0	2	0	5	6	4
Utslipp til vassdrag (kilde kjent)	2	8	5	12	6	4	15	11
Utslipp ved bunkring av fartøy	11	11	7	16	18	12	20	9
Vrakhåndtering (Skip)	30	24	7	9	15	9	10	6
Øvrige skipshendelser	74	10	18	24	23	22	18	51
Totalt	**1 281**	**1 060**	**1 091**	**1 327**	**1 290**	**1 119**	**1 023**	**926**

Coastal radio stations

The coastal radio service consists of two 24-hour stations – *Kystradio Nord* and *Kystradio Sør* – and around 120 remotely operated VHF stations. Coastal radio also forms part of the rescue service in Norway and acts as a link between the vessel in distress and the Joint Rescue Coordination Centre. Coastal radio performs one of Telenor's many societal tasks and is part of the rescue service in Norway. The rescue service's needs as regards radio communication via the coastal radio stations is met by Telenor and operated in combination with the commercial part of the coastal radio service. The highest priority task within this is to act as a link between the vessel in distress and the Joint Rescue Coordination Centres.

The coastal radio stations provide a range of services, including:

- Watches concerning the international emergency frequencies
- Receiving messages and establishing communication with vessels in distress
- Ensuring efficient communication during search and rescue operations
- Notifying the Joint Rescue Coordination Centres
- Notifying ships and any other units which can contribute rescue resources
- Sending out messages which have safety implications for safe passage and navigation.
- Disseminating medical advice (Radio Medico)
- Managing commercial traffic

Global Maritime Distress Safety System (GMDSS)

The Global Maritime Distress Safety System (GMDSS) is a set of internationally approved procedures for safety, equipment types and communication protocols, which are intended to improve safety and make it easier to rescue vessels and aircraft in distress. Vessels over 15 m in length and all vessels operating passenger services must be fitted with GMDSS-approved equipment on board for the marine areas in which

they operate. In 2014, stricter requirements regarding GMDSS equipment were also introduced for fishing vessels under 15 m.

The applicable requirements regarding equipment depend on the areas in which the ship operates and are linked to the coverage area for different radio equipment. The areas of interest cover the four area categories:

- **A1:** Areas within range of shore-based VHF stations (20-30 nm).
- **A2:** Areas within range of shore-based MF stations (100-150 nm), with the exception of A1 areas.
- **A3:** Areas within range of Inmarsat (between ~70°N and ~70°S), with the exception of A1 and A2 areas.
- **A4:** Areas outside A1-A3, such as the High North.

The equipment requirements are formulated so that vessels must be able to transmit and receive alerts and distress signals in the areas in which they operate: a "minimum requirement" for operation in the A1 area, with additional requirements for MF/HF equipment and satellite equipment if sailing outside this area.

Equipment covered by GMDSS requirements includes:

- Radio installations – requirements depend on area. In addition to installed radio, there must also be portable transceivers on board for use in lifeboats.
- Digital Selective Calling (DSC) – A system that transmits a predefined digital message via MF, HF or VHF. Emergency messages transmitted via DSC will include the ship's MMSI and will normally also be connected to the ship's GPS, so that the ship's identity and position will automatically be included in the message. In addition to being able to rapidly transmit messages, a ship will also have equipment for receiving such messages.
- Emergency Position-Indicating Radio Beacon (EPIRB) – An emergency beacon which transmits signals which can be interpreted by COSPAS-SARSAT satellite systems.
- EGC and Navtex are not included.

C.2.4 Norwegian Maritime Authority

The Norwegian Maritime Authority is an administrative body under the Ministry of Trade, Industry and Fisheries and the Ministry of Climate and Environment. The Norwegian Maritime Authority is the administrative and supervisory authority with regard to the safety of life, health, the environment and material assets on vessels flying the Norwegian flag and foreign vessels in Norwegian waters. The authority is also responsible for ensuring legal protection for Norwegian-registered ships and their rights. The activities are determined by national and international regulations, treaties/agreements and political decisions. The main tasks of the Norwegian Maritime Authority are:

1. Safety of life and health, environment and material assets
2. Registration of vessels and rights in vessels
3. Supervision of the construction and operation of vessels flying the Norwegian flag, and their shipping companies
4. Issuing of certificates for seafarers and supervision of Norwegian educational institutions
5. Supervision of foreign vessels in Norwegian ports
6. Supervision and promotion of good working and living conditions on vessels
7. Management and development of Norwegian and international regulations
8. Promotion of Norway as a flag state
9. Administration of grant schemes on behalf of the Ministry
10. Monitoring of the risk picture

11. Preventive work aimed at reducing the number of accidents in both the recreational and commercial fleets.

Accidents and near misses must be reported. This is regulated in Lovdata, the Regulations relating to alerting and reporting obligations in the event of maritime accidents and other incidents at sea [51]. These Regulations concern the duty to alert and report in the event of:

a) maritime accidents and very serious maritime accidents; see Section 472a, fourth and fifth paragraphs of the Maritime Act [52],
b) serious accidents; see Section 472a, first paragraph of the Maritime Act,
c) occupational accidents, even if the accident is not regarded as a maritime accident; see Section 47 of the Ship Safety and Security Act [53],
d) discharges or risk of discharges of hazardous or polluting substances, even if the matter is not regarded as a maritime accident; see Section 34 of the Ship Safety and Security Act,
e) sabotage or piracy (see Sections 39 and 47 of the Ship Safety and Security Act), even if the matter is not regarded as a maritime accident,
f) occupational illness (see Section 47 of the Ship Safety and Security Act), as stipulated in the individual provision.


Rapport om sjøulykke, arbeidsulykke og nestenulykke

Del A. Generelt

Figure 20 Reporting form for Maritime accidents. Source: Norwegian Maritime Authority

The Regulations are applicable to:

a) Norwegian ships, including mobile facilities, fishing vessels and recreational craft.
b) Foreign ships:
    1. In the event of a maritime accident in Norwegian territorial waters.
    2. In the event of discharges or a risk of discharges of oil, hazardous or polluting substances in Norwegian territorial waters, including the territorial waters surrounding Svalbard and Jan Mayen and in the Norwegian Economic Zone.

As regards Ro-Ro ferries and high-speed passenger vessels sailing on scheduled services to or from a Norwegian port to or from a port in an EEA State, the provisions of the Regulations also apply when the maritime accident occurs outside Norwegian territorial waters if Norway was the last EEA State that the ship visited before the accident.

The Regulations do not apply to military vessels, with the exceptions referred to in the first paragraph (d) of the provision, or to maritime accidents which only involve military vessels.

As regards the reporting of acute pollution or a risk of acute pollution, Regulation No. 1269 of 9 July 1992 applies.

On the basis of reported incidents, the Norwegian Maritime Authority regularly disseminates information concerning "learning from incidents" based on accidents and incidents. For example, the Norwegian Maritime Authority has had a number of accident reports submitted with the cause stated as being "falling asleep on duty". The crew on board have usually fared well, but some vessels have sunk, run aground or

suffered major damage, and some accidents have also led to discharges into the environment. Some sample excerpts from the reports are as follows:

> ***What happened?***
> "The captain fell asleep...." "...the mate fell asleep on duty..." "... fell asleep at the helm..." "... the crew member fell asleep at the helm..." "... the boat's captain fell asleep on his way to an assignment..." "... the autopilot was on and I fell asleep..." "... grounded due to the captain falling asleep on duty and the lookout had gone down from the bridge to clean the mess/galley..." "... the helmsman fell asleep..." "... the officer fell asleep..." "... fell asleep before arriving at the locality and was woken up as a result of running aground..." and "... one person on the bridge and that person fell asleep."

This list was taken from a sample of accident reports which were submitted during the past year and gave the reason why the vessel ran aground. In cases where we receive reports with the cause "fell asleep on duty", the crew on board has usually fared well, but some vessels have sunk, run aground or suffered major damage, while some accidents have led to discharges into the environment.

Causes

Some crew members fell asleep after a long voyage and duty, often at the end of the shift, while others had only recently started their shift. Being sufficiently rested often depends on what the crew members spent their rest time doing, and whether or not the quality of the rest time was good. Rest time and duties which are affected by noise, vibration, lack of sleep or disturbances can make a bridge shift challenging. The time of day and the right bridge crew are also important factors.
Decreasing daylight, monotonous tasks and little happening, poor air quality on the bridge, long shifts, or improper use of technical aids with a redundancy function (e.g. bridge duty alarm) are other possible causes. The list of direct and underlying causes could have been longer; the outcome is "fell asleep on duty".

Measures

Various measures are required by law, or require an assessment to be carried out by the company and the crew on board. Possible measures include a bridge duty alarm, bridge duties in accordance with the Rules of the Road (RoR), and the Watchkeeping Regulations, appropriate crewing, etc. There is a long list of measures which are aimed at preventing something going wrong and crew members falling asleep on duty. Irrespective of laws and regulations, individual crew members serving on board must also ensure that the quality of their rest time is good before they start their next shift. Good planning of work and rest time means safer shifts, and better rest and essential sleep.

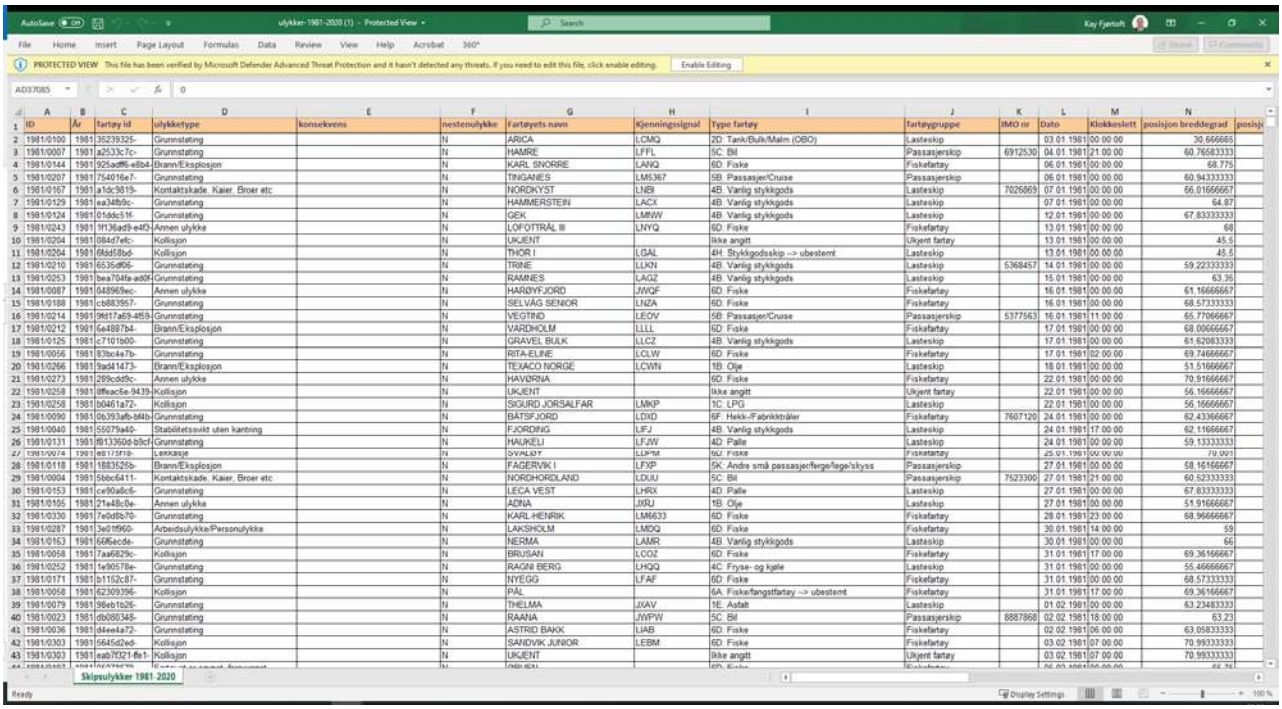
More information about learning from events can be found here:

- https://www.sdir.no/sjofart/ulykker-og-sikkerhet/undersokelse-av-ulykker/laring-av-hendelser/

Together with the Norwegian Coastal Administration, the Norwegian Maritime Authority has drawn up proposals for a maritime strategy relating to digital safety. The agencies present a number of specific recommendations, including the establishment of a national response centre. A link to more information about this can be found here. One of the reports noted is SINTEF's threat assessment in connection with the strategy for maritime digital safety:

- https://www.sdir.no/aktuelt/nyheter/anbefaler-nasjonalt-responssenter-for-maritim-digital-sikkerhet/

The Norwegian Maritime Authority uses data from reported accidents to produce accident statistics. These are often published after six months and at the year-end. There are also accident statistics for recreational craft.



ID	År	Fartøy id	ulykketype	konsekvens	nestenulykke	Fartøyets navn	Kjenningssignal	Type fartøy	Fartøygruppe	IMO nr	Dato	Klokkeslett	posisjon breddegrad
1981/0100	1981	36239325-	Grunnstøting		N	ARICA	LCMQ	2D Tank/Bulk/Malm (OBO)	Lasteskip		03.01.1981	00:00:00	30.666665
1981/0007	1981	a2533c7c-	Grunnstøting		N	HAMRE	LFTL	5C Bil	Passasjerskip	6912530	04.01.1981	21:00:00	60.76583333
1981/0144	1981	925adff6-e8b4-	Brann/Eksplosjon		N	KARL SNORRE	LANQ	6D Fiske	Fiskefartøy		06.01.1981	00:00:00	68.775
1981/0207	1981	754016e7-	Grunnstøting		N	TINGANES	LM5367	5B Passasjer/Cruise	Passasjerskip		06.01.1981	00:00:00	60.94333333
1981/0167	1981	a1dc3819-	Kontaktskade. Kaier. Broer etc		N	NORDKYST	LNBI	4B Vanlig stykkgods	Lasteskip	7026869	07.01.1981	00:00:00	66.01666667
1981/0129	1981	ea34fb9c-	Grunnstøting		N	HAMMERSTEIN	LACX	4B Vanlig stykkgods	Lasteskip		07.01.1981	00:00:00	64.87
1981/0124	1981	01ddc51f-	Grunnstøting		N	GEK	LMNW	4B Vanlig stykkgods	Lasteskip		12.01.1981	00:00:00	67.83333333
1981/0243	1981	1f136ad9-e4f0-	Annen ulykke		N	LOFOTTRÅL III	LNYQ	6D Fiske	Fiskefartøy		13.01.1981	00:00:00	68
1981/0204	1981	084d7efc-	Kollisjon		N	UKJENT		Ikke angitt	Ukjent fartøy		13.01.1981	00:00:00	45.5
1981/0204	1981	68dd58b6-	Kollisjon		N	THOR I	LGAL	4H Stykkgodsskip -> ubestemt	Lasteskip		13.01.1981	00:00:00	45.5
1981/0210	1981	6535df06-	Grunnstøting		N	TRINE	LLKN	4B Vanlig stykkgods	Lasteskip	5368457	14.01.1981	00:00:00	59.22333333
1981/0253	1981	bea704fa-ad0f-	Grunnstøting		N	RAMNES	LAGZ	4B Vanlig stykkgods	Lasteskip		15.01.1981	00:00:00	63.35
1981/0087	1981	048969ec-	Annen ulykke		N	HARØYFJORD	JWQF	6D Fiske	Fiskefartøy		16.01.1981	00:00:00	61.16666667
1981/0188	1981	cb883957-	Grunnstøting		N	SELVÅG SENIOR	LNZA	6D Fiske	Fiskefartøy		16.01.1981	00:00:00	68.57333333
1981/0214	1981	9fd17a69-4f59-	Grunnstøting		N	VEGTIND	LEOV	5B Passasjer/Cruise	Passasjerskip	5377563	16.01.1981	11:00:00	65.77066667
1981/0212	1981	6e4887b4-	Brann/Eksplosjon		N	VARDHOLM	LLLL	6D Fiske	Fiskefartøy		17.01.1981	00:00:00	68.00666667
1981/0125	1981	c7101b00-	Grunnstøting		N	GRAVEL BULK	LLCZ	4B Vanlig stykkgods	Lasteskip		17.01.1981	00:00:00	61.62083333
1981/0056	1981	83bc4e7b-	Grunnstøting		N	RITA-ELINE	LCLW	6D Fiske	Fiskefartøy		17.01.1981	02:00:00	69.74666667
1981/0266	1981	9ad41473-	Brann/Eksplosjon		N	TEXACO NORGE	LCWN	1B Olje	Lasteskip		18.01.1981	00:00:00	51.51666667
1981/0273	1981	269cdd9c-	Annen ulykke		N	HAVØRNA		6D Fiske	Fiskefartøy		22.01.1981	00:00:00	70.91666667
1981/0258	1981	8feac6e-9439-	Kollisjon		N	UKJENT		Ikke angitt	Ukjent fartøy		22.01.1981	00:00:00	56.16666667
1981/0258	1981	b0461a72-	Kollisjon		N	SIGURD JORSALFAR	LMKP	1C LPG	Lasteskip		22.01.1981	00:00:00	56.16666667
1981/0090	1981	0b393afb-bf4b-	Grunnstøting		N	BÅTSFJORD	LDXD	6F Hekk-/Fabrikktråler	Fiskefartøy	7607120	24.01.1981	00:00:00	62.43666667
1981/0040	1981	55079a40-	Stabilitetssvikt uten kantring		N	FJORDING	LIFJ	4B Vanlig stykkgods	Lasteskip		24.01.1981	17:00:00	62.11666667
1981/0131	1981	f813360d-b9cf-	Grunnstøting		N	HAUKELI	LFJW	4D Palle	Lasteskip		24.01.1981	00:00:00	59.13333333
1981/0074	1981	e81758f8-	Lekkasje		N	SVALØY	LDPM	6D Fiske	Fiskefartøy		25.01.1981	00:00:00	70.091
1981/0118	1981	1883526b-	Brann/Eksplosjon		N	FAGERVIK I	LFXP	5K Andre små passasjer/ferge/lege/skyss	Passasjerskip		27.01.1981	00:00:00	58.16166667
1981/0004	1981	5bbc6411-	Kontaktskade. Kaier. Broer etc		N	NORDHORDLAND	LDUU	5C Bil	Passasjerskip	7523300	27.01.1981	21:00:00	60.52333333
1981/0153	1981	ce90a8c6-	Grunnstøting		N	LECA VEST	LHRX	4D Palle	Lasteskip		27.01.1981	00:00:00	67.83333333
1981/0155	1981	21e48c0e-	Annen ulykke		N	ADNA	JXRJ	1B Olje	Lasteskip		27.01.1981	00:00:00	51.91666667
1981/0336	1981	7e0d8b76-	Grunnstøting		N	KARL-HENRIK	LM6633	6D Fiske	Fiskefartøy		28.01.1981	23:00:00	68.96666667
1981/0287	1981	3e01f960-	Arbeidsulykke/Personulykke		N	LAKSHOLM	LMDQ	6D Fiske	Fiskefartøy		30.01.1981	14:00:00	59
1981/0163	1981	60f6acde-	Grunnstøting		N	NERMA	LAMR	4B Vanlig stykkgods	Lasteskip		30.01.1981	00:00:00	66
1981/0058	1981	7aa6829c-	Kollisjon		N	BRUSAN	LCOZ	6D Fiske	Fiskefartøy		31.01.1981	17:00:00	69.36166667
1981/0252	1981	1e90578e-	Grunnstøting		N	RAGNI BERG	LHQQ	4C Fryse- og kjøle	Lasteskip		31.01.1981	00:00:00	55.46666667
1981/0171	1981	b1152c87-	Grunnstøting		N	NYEGG	LFAF	6D Fiske	Fiskefartøy		31.01.1981	00:00:00	68.57333333
1981/0058	1981	62309396-	Kollisjon		N	PÅL		6A Fiske/fangstfartøy -> ubestemt	Fiskefartøy		31.01.1981	17:00:00	69.36166667
1981/0079	1981	96eb1b26-	Grunnstøting		N	THELMA	JXAV	1E Asfalt	Lasteskip		01.02.1981	00:00:00	63.23483333
1981/0023	1981	db080348-	Grunnstøting		N	RAANA	JWPW	5C Bil	Passasjerskip	8887866	02.02.1981	18:00:00	63.23
1981/0036	1981	d4ee4a72-	Grunnstøting		N	ASTRID BAKK	LIAB	6D Fiske	Fiskefartøy		02.02.1981	06:00:00	63.05833333
1981/0303	1981	56456ce8-	Kollisjon		N	SANDVIK JUNIOR	LEBM	6D Fiske	Fiskefartøy		03.02.1981	07:00:00	70.99333333
1981/0303	1981	eab7f321-ffe1-	Kollisjon		N	UKJENT		Ikke angitt	Ukjent fartøy		03.02.1981	07:00:00	70.99333333

Figure 21 Accident statistics. Source: Norwegian Maritime Authority.

C.2.5 European Maritime Safety Agency

The task of the European Maritime Safety Agency (EMSA) is to serve the EU's maritime interests in a safe, secure, green and competitive maritime sector, and to act as a reliable and respected reference point in the maritime sector, both in Europe and around the world.

The EMSA's remit covers maritime security, safety, climate, environment and single market issues and tasks, primarily as a service provider to Member States and the Commission, but also as an innovative and reliable partner and knowledge hub for the European maritime cluster and potentially in addition a reference on the international stage.

The EMSA was established through Article 1 of Regulation (EC) No 1406/2002, which states that the purpose of the agency is to ensure a high, uniform and effective level of maritime safety and security, to prevent and respond to pollution caused by ships, and to respond marine pollution caused by oil and gas installations, and, where appropriate, to contribute to the overall efficiency of maritime traffic and transport with a view to establishing a European maritime transport space without barriers.

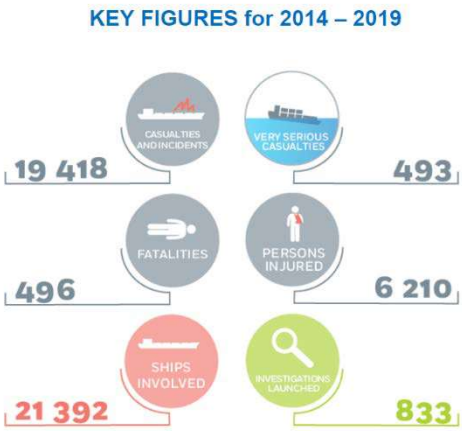


Figure 22 EMSA main statistics concerning accidents for the period 2014-19. Source EMSA

2019 was a positive year as regards improving or stabilising some indicators, such as the number of ships lost, fatalities and casualties. A total of 3,062 incidents were reported in 2019. A reduction of 200 fatalities was recorded compared with 2018. The total number of incidents stored in the EMCIP database grew to 19,500 during the period 2014-2019. This represents an average of 3,236 marine losses or incidents per year over the period.

A total of 106 very serious losses were reported in 2018, which corresponded to an increase of 68% compared with 2017, while the total number fell back to 63 in 2019. A similar trend regarding the number of ships lost was observed: after a peak in 2018, a decrease in 2019 was recorded, with 21 ships being lost.

During the period 2014-2019, 320 accidents resulted in a total of 496 lives being lost. After a steady and important decline from 2015 through to 2017, a limited increase was recorded for the years 2018 and 2019. 88.3% of the victims were crew members. Fatalities primarily occurred during collisions. When the event is limited to people, falls were the main cause of loss of life. The main events that resulted in fatalities were collisions as regards ships and falls as regards people. During the period 2014-2019, a total of 6,210 injuries were registered, corresponding to 5,424 accidents. Crew members are the main category for persons injured at sea, accounting for 79.3% of the victims.

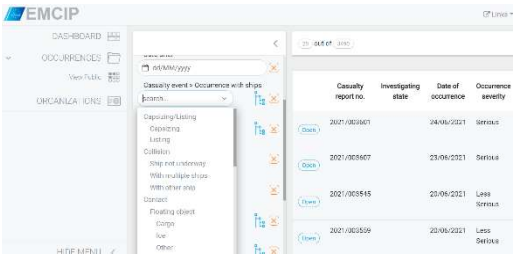


Figure 23 EMCIP database. Source EMSA

EMCIP stands for 'European Marine Casualty Information Platform', and is a centralised database for EU Member States for storing and analysing information about accidents and incidents at sea. EMCIP is filled with data by competent national authorities. It is this data that forms the basis for the annual overview of maritime accidents and incidents. Searching the database also gives access to the incident reports. The link to the database is:
https://portal.emsa.europa.eu/emcip-public/#/dashboard

C.3 Reporting for autonomous vessels

C.3.1 Information flow for autonomous vessels

Figure 24 shows who needs information from an autonomous vessel. On the right of the figure, we have a control centre which is responsible both for the ship and for exchanging information with other control centres, with VTS's, and with other traffic which impacts on a sailing. A vessel must either directly, or indirectly via the control centre, exchange the information with ports and authorities who need this information both to ensure safety and to direct traffic into port. Under the MASS vessel, some sensors are shown which are necessary in order for an autonomous vessel to be able to sail safely. For example, navigation sensors will be crucial. These could be sensors located along the shipping lanes, as well as sensors which meet the ship when it docks. It could also be weather reports which are used to determine the vessel's capabilities. Communication is essential in order for data to be transmitted between vessel and shore, as well as for collecting data for navigation purposes, and in particular if the vessel is to be controlled from a control centre.

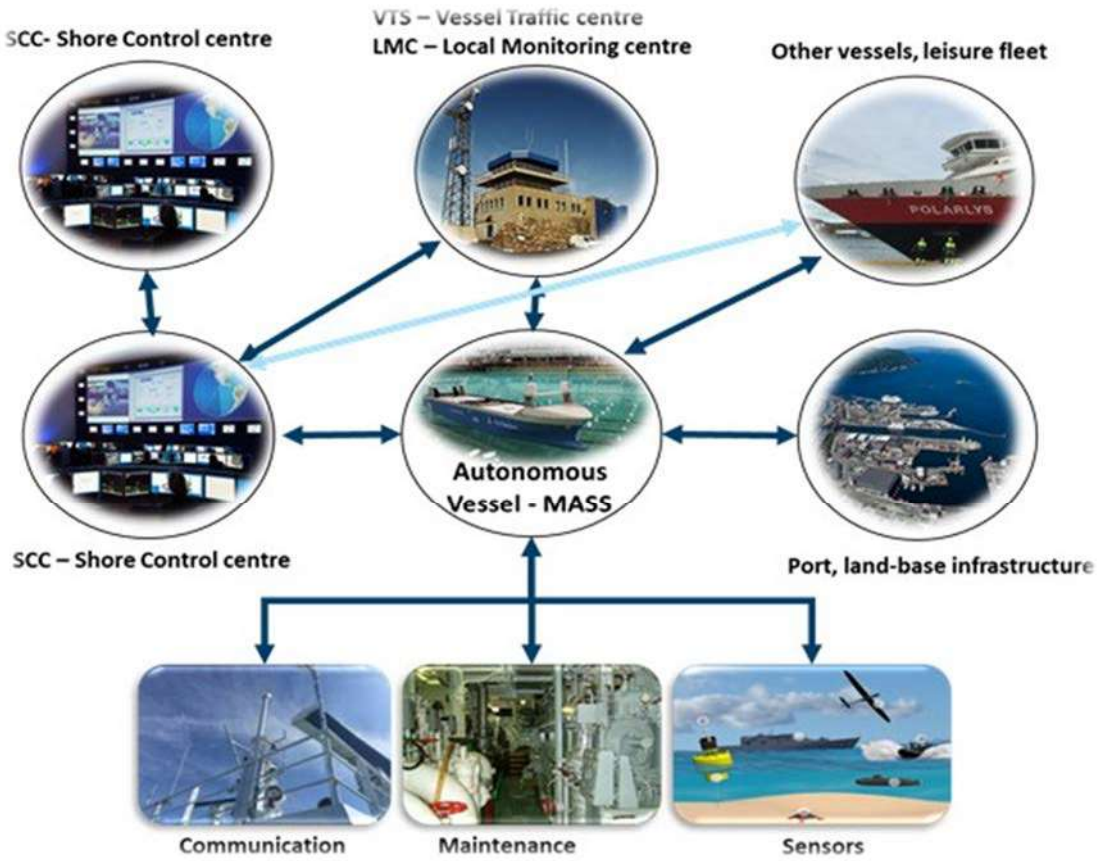


Figure 24 A maritime autonomous value chain. Source SINTEF.

C.3.2 Recent developments within autonomy

Figure 25 shows the anticipated development in the introduction of autonomy in maritime shipping. On the far left, the red circle indicates that we anticipate new incidents as a result of the introduction of autonomy. The types of incidents and consequences are still largely unknown, as we only have limited background data as present. The orange circle represents accidents which currently occur involving conventional shipping, while the black circle indicates the expected reduction as a result of the introduction of autonomy. On the far right, the red circle indicates the number of accidents which are currently being prevented due to the presence of the crew, while the black circle is what we expect the automation itself to be able to prevent in the context of today's events which are averted by the crew on board.

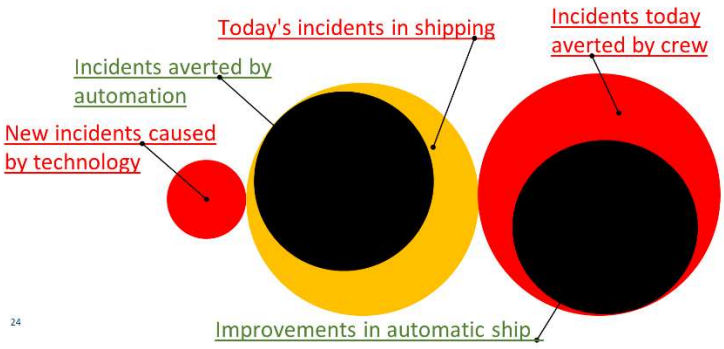


Figure 25 Accident types, autonomy. Source SINTEF

Experience from accident scenarios with conventional shipping shows that equipment failures account for almost a quarter of the accident figures. Furthermore, the figures show that a high proportion of accidents are caused by human factors.

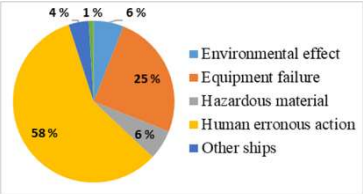


Figure 26 EMPIC (EMSA 2018). Source EMSA

We have also carried out studies on these figures, where we assessed different degrees of autonomy and set this up against some selected impacts. Our comparison highlighted the degrees of autonomy "fully autonomous" and "partially autonomous", the importance of control rooms, the importance of a high degree of technical resilience, as well as the importance of having more quality in the plans associated with a sailing. We have indicated what autonomy will mean in the form of new accidents which may occur due to autonomy, comparing the picture with the current accident picture, as well as which accidents could be prevented with a higher degree of autonomy. The colour codes indicate the following: green=better, red=expected negative effect.

As a further explanation, the introduction of full autonomy, for example, could have the following significant impacts:

- More demanding requirements regarding the use of sensors, automation and shore-based control mean that the operators at a control centre may lose some of their situational awareness as regards the environment, ships and technical performance of systems on board the vessels.
- Much lower exposure to danger for the crew.
- A vessel without any crew would make it difficult to inspect equipment or systems which report faults or problems.
- Removing vulnerable technology will reduce the risk of fire, e.g. due to the reduction in technology associated with crew comfort, such as the galley, laundry and waste systems. This is equipment which is associated with a relatively high risk of fire on manned ships.

	Main differentiating factors	Brief description of effects	New	Today's	Averted
	Fully unmanned				
1	Higher demand on sensors, automation and shore control as one lack some of the "personal touch", both on environment, ship and technical systems' performance.	More technology means more complexity and possibility for technological failure, but will also improve on some of today's operators errors (human error).	R	G	Y
2	Less exposure to danger for the crew.	40% of deaths at sea are occupational hazards.	Y	G	G
3	May be unable to inspect equipment or systems that report errors or problems.	This may cause problems, especially if sufficient back-up systems are not in place.	R	Y	Y
4	Slightly lower risk of fires in accommodation, galleys, laundry and waste systems.	Improvement on today's accident events, but more difficult fire handling and control.	R	G	Y
	Constrained autonomy				
5	More limited, but also more deterministic response from sensors and automation.	Better HAI, due to time to get situational awareness before action.	Y	G	Y
6	Dependence on shore control operators' performance and situational awareness.	Always rested, but not directly in the loop.	R	Y	Y
7	Dependence on communication link to shore.	Loss of communication may cause new accident types, but high integrity req. and clear operational design domains will help.	R	Y	Y
8	Dependence on high quality implementation of fallback solutions and definition of minimum risk conditions for the ship.	More conservative and hence safer operational procedures.	Y	G	G
	Shore control center				
9	Dependence on good cooperation in the shore control center.	Training and resource management is critical.	Y	G	R
10	Intervention crew do not have to worry about personal risk and adverse conditions on board.	May be likely to find solutions to critical problems that would otherwise be lost.	Y	G	Y
	Higher technical resilience				
11	More technical barriers against technical faults.	In case of trouble, backup systems shall be in place.	Y	G	Y
12	Much improved technical systems with built in predictive maintenance functionality.	Less chance of trouble	Y	G	Y
13	Dependent on maintenance at shore.	Something may be forgotten	R	G	Y
	Improved voyage planning				
14	Less chance of surprises during voyage.	Better planned voyage	Y	G	G
15	More support from other functions on shore	Improved traffic regulation	Y	G	G

Figure 27 Effects on type of limitations. Source SINTEF.

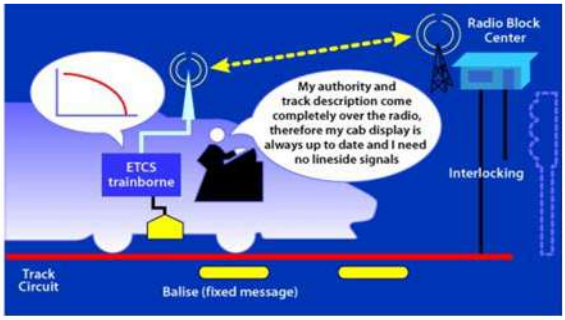
D Rail

D.1 European Rail Traffic Management System (ERTMS)

A programme to replace and modernise the signalling systems on the Norwegian rail network is currently underway. The current signalling technology will be replaced by the European Rail Traffic Management System (ERTMS), a digitalised signalling system which will become common to the whole of Europe and ensure interoperability. ERTMS is based on technological solutions which facilitate greater automation and provide a foundation for autonomous trains in the future. The system will immediately help to improve train performance and increase the capacity of the rail network through better utilisation of track access. At the same time, safety considerations are addressed through continuous speed monitoring. Existing signalling and control systems consist of ATC (Automatic Train Control) combined with lineside colour light signals which provide information to train drivers. With ERTMS, information for the train driver and movement authority will be sent directly to a computer on the driver's panel (ETCS) through the railway's own mobile network (GSM-R). The train driver is still in control, but if he or she drives too fast or starts braking too late, the train's computer will take over and decelerate the train to the correct speed or to a complete stop. The automation, and the more integrated solution in the train which ERTMS entails, therefore reduces the possibility of human error. At the same time, the consequences of human error will be reduced through the fact that the automatic equipment (speed monitoring) takes over.

ERTMS as a system consists of the following:

- ETCS (European Train Control System - speed monitoring and signalling)
- GSM-R (for communication between trains and signalling systems)
- Pan-European traffic rules



ETCS datamaskin i tog

ETCS førerpanel i tog

Figure 28 The principle of ERTMS

As a result of the implementation of ERTMS in Norway and elsewhere in the Nordic countries, ETCS will replace the current ATC system. However, both systems will be operational during a transitional phase. When a train equipped with ETCS is also to operate on sections of line equipped with ATC for a certain period of time, it must be equipped with what is known as a Specific Transmission Module (STM). This device translates information from the ATC system into a language which the new ETCS system can understand. This enables ETCS to be implemented gradually.

Upon transition from the existing ATC system to ERTMS (with ETCS and GSM-R), the traffic rules must also be adjusted somewhat due to the different characteristics of ERTMS, especially in case of non-conformant situations. The biggest difference in connection with the transition to ERTMS is that both the signalling system and the train will adopt the same operational states.

The most common operational states in ERTMS are:

- Full Supervision (FS): Movement authorisation with the maximum permissible speed in the section
- On-Sight (OS): Movement authorisation with speed limit
- Shunting (SH): Movement authorisation for “shunting” with speed limit
- Staff responsible (SR): Movement authorisation with speed limit when movement authorisation in FS/OS cannot be granted due to a fault on the train or in the infrastructure.

D.2 Reporting systems, collection and classification

Section 7-2 of the Regulations relating to safety management for railway enterprises [54] requires, inter alia, that the enterprise *shall have a system for the internal reporting, registration, investigation and analysis of railway accidents, serious railway incidents and railway incidents*.

Manual reporting of incidents and near misses on the railway currently takes place in various systems. Relevant systems in this context are "Synergi", "TIOS" and "AT-melding". These are records of deviation- and safety-related incidents in Bane NOR. Synergi is a well-known HSE&Q reporting system which is in widespread use amongst businesses/industries. TIOS (“Traffic Information and Follow-Up System”) stores planned and actual train times, as well as causes of delays/cancellations. The causes of delays/cancellations are reported to this system, broken down into different categories/codes of causes subdivided according to type of actor/circumstances. Some relevant codes relating to train movements and signalling can be found in the table below (see Bane NOR: Track access agreement AST, Appendix 4). These codes are used by infrastructure owners and railway undertakings.

Table 17 Reason codes in TIOS.

Code no. and name	Explanations
Code 2 – Safety system, signalling system and remote control	"Rail traffic controller cannot set a signal". Fault in line block, bulb check, signal box/remote control system, ATC balise, road protection system, landslide warning system. Switch not in control. Unintentional passing of signal at danger due to technical fault ("SPAD"). Track section coating, incl. salt coating. Fault in emergency power system.
Code 4 - Telecommunication and transmission failure	Telecommunication and transmission errors which result in operational disruption. Fault in GSM-R system. Fault in public address system/announcer. Error in FIDO communication.
Code 6 - Rolling stock with incorrect barriers, track/block section	Used for delays which occur because one train catches up with another; collision between one train and another with a fault blocking the line. Also used if single-track operation needs to be implemented as a result of this. Must be used even if the failed train/train with faulty vehicle has started moving again. When the line is clear for traffic, but the train dispatcher chooses to hold back a train travelling in the opposite direction in anticipation of crossing, this train should have Code 7 (Traffic management). The failed train/train with fault should have Code 81 (Fault on vehicle).
Code 7 - Traffic management	Overall assessments made by train controllers regarding the order/selection of crossing point, construction/system errors in the timetable. Reasons in relation to traffic management: Signal is set too late, cannot report train to served station, queuing, congested line section, fault in auxiliary system FJS (Automatic/ATL/TLS). Bane NOR's personnel use the FIDO system incorrectly.
Code 81 - Fault on vehicle	All faults on vehicles which result in stoppage or reduced speed. Load shifting on freight trains. Fault on onboard equipment for FIDO or in the event of a fault in onboard ERTMS equipment.

An “AT-melding” is used by Bane NOR when there are "*Faults in infrastructure which affect more than one train*" and when "*Stopping trains affect other trains*". In other words, these are also messages of relevance

to traffic management, and the system helps to convey information more rapidly to the train companies parallel to the traffic control centre. When the situation has been normalised and the operational disruption has ceased, a new “AT-melding” will be sent stating that the problem has been resolved. This will be displayed on a screen for 20 minutes before it is removed. In addition to the aforementioned systems, Bane NOR has a whistleblowing channel for reporting censurable circumstances. Via this channel, employees of the railway undertaking, vendors, customers and partners can report, inter alia, circumstances which entail a risk to life and health.

Whether there is a need for new systems for recording (safety-related) incidents linked to automated systems such as ERTMS, or whether such systems already exist or are being planned, is unclear at present. The following is stated on Bane NOR's website: "*Amongst other things, ERTMS gives us enhanced safety through technical barriers and continuous monitoring of all trains, improved punctuality due to fewer errors and automatic handling of deviations. Over time, the system will offer increased capacity with the automatic operation of trains, as well as dynamic spacing between trains.* "

Alongside the implementation of ERTMS, work is under way on procedures and instructions within Bane NOR and the train operators in order to implement the systems. Here, it is possible that new procedures are being planned for the detection and registration of incidents from the digital systems.

A series of IEC standards set out requirements regarding onboard systems for the continuous collection, storage and use of audiovisual information (audio and video recordings) from the driver’s cab when a train is being driven. This is referred to as the On-board Driving Data Recording System (ODDRS). IEC 62625-1:2013 [35] and IEC 62625-2:2016 [55] deal with system specifications and requirements for the compliance testing of such systems which may be referred to in the regulations. IEC TC-9 now has IEC NP 62625-3 under way to complement parts 1 and 2 of IEC 62625. Here, additional requirements are stipulated for audio and video recordings which can be used not only in connection with the investigation of actual commands issued within the driver’s cab during an incident or accident, but also for observation of the driver when this is required in other contexts. Such audio and video recordings should be able to reproduce the following:

- What the train driver said
- What train driver should have heard
- What the train driver could have seen, and
- What actions the train driver took in the given situation

The new IEC 62625 standard will stipulate requirements for the collection, storage and display of such audio and video recordings from the cab, as well as video recordings of the view from the driver’s cab. The following recordings are relevant:

- Calls that train driver has via (wired) intercommunication
- Video recording of the railway track seen looking forward from the cab
- Ambient sounds and voices elsewhere in the cab
- Video of the train driver's control panel(s)
- Video with an overview of the cab otherwise

IEC 62625-3 will take into account the fact that: 1) national requirements or regional regulations, employment agreements, etc. may limit the type of audio-visual recordings that are permitted, and that 2) it is not a requirement to record all audio-visual observations.

Note: In connection with the investigation of incidents, IEC 62625-1 [35] requires ODDRS to continuously record information on a *secured* storage medium with a minimum capacity of 24 hours of recording. For

observation/auditing of the driver over time, the requirement is to record incidents continuously on an *ordinary* storage medium with a minimum capacity of eight days of recording.

D.3 Actors and framework conditions for reporting

It is the persons responsible within the railway undertakings themselves, together with vendors and traffic control centres, which report incidents relating to signalling and train operation. The traffic control centres will have a complete overview of traffic management, while the HSE and quality managers amongst the undertakings will have an overview of safety-related incidents amongst the individual players.

It will probably also be part of the training in connection with the implementation of ERTMS to be given an introduction to applicable procedures and routines for the detection and registration of incidents/errors for the digital systems that are being implemented.

E Power supply

E.1 Delivery reliability

The Norwegian Water Resources and Energy Directorate (NVE) and the system administrator stipulate numerous requirements regarding the registration and reporting of errors and interruptions (see FASIT | Statnett.

Using FASIT software, error and interruption statistics in the overall network can be recorded.

The purpose of FASIT is to provide information on the reliability of supply in the Norwegian power system, including both information on the historical reliability of supplies and information for use in estimating the future expected reliability of supplies.

In FASIT, information is recorded about:

- operational interruptions (automatic disconnection, forced disconnection and unintentional disconnection)
- planned disconnections which have resulted in interruptions (both planned announced disconnections and planned, unannounced disconnections)

Operational disruption (what the fault is, where the fault is, and why there is a fault) covers a component and system focus, while interruptions for reporting points (including interrupted power, interruption duration, undelivered energy (ILE) and quality-adjusted revenue framework for undelivered energy (KILE)) cover an end-user focus.

The faults which are entered in FASIT are those which caused or extended an operational disruption. This means that some "trivial" errors are recorded because they (arbitrarily) caused an operational disruption, while some "serious" errors are not recorded because they were detected and dealt with before the fault resulted in an operational disruption.

It is assumed that, regardless of the cause or consequences, all faults are handled in other systems used by the licensees, e.g. a maintenance system.

E.2 ICT security

The Norwegian Water Resources and Energy Directorate (NVE) was originally designated as a sectoral response environment for the power sector, but they have delegated this task to KraftCERT since 2018.

In its report on NVE's work relating to ICT security in the power supply sector, the Office of the Auditor General points out that there are "weaknesses in the ability of the companies to detect ICT incidents and under-reporting" [7].

KraftCERT has confirmed that it shares information about incidents with its customers/members, both in the form of Structured Threat Information eXpression (STIX) via Trusted Automated eXchange of Indicator Information (TAXII) , as well as on encrypted Internet Relay Chat (IRC). However, relatively little information flows to KraftCERT from members/customers, as the majority of the information flow concerning attacks and indicators of compromise is one-way from KraftCERT.

A number of alternative tools for information sharing are available, including MISP and HIVE, but the biggest problem is that the industry has so far been unable to agree on a standard. Information about incidents, etc. is currently just as often shared in the form of PDF documents.

There is much evidence to suggest that many of the players in the power industry participate in NSM's Reporting System for Digital Infrastructure (VDI), but there is no publicly available information on this. Based on what is known, it can be concluded that NSM has deployed intrusion detection sensors amongst the actors, so that attempted attacks can be automatically reported back to NSM. However, we can assume that VDI is not concerned with everyday events, but rather focuses on more fundamental aspects, such as advanced persistent threats (APT).

The automation of notification is also a major issue for KraftCERT, which is currently working on a specific sensor project for its members. The vendors Claroty, Nozomi Networks and the former CyberX (now Azure Defender for IoT) have equipment which sits inside the OT networks and is updated automatically via feeds from vendors like ABB, Siemens (and many others). It is therefore possible to obtain an automatic list of assets, software versions, etc.

In addition to reporting to the sectoral response environment, there is also a European Information Sharing & Analysis Centre (ISAC) for the energy industry, the European Energy ISAC (EE-ISAC), which conducts proactive information sharing concerning indicators of compromise, etc., and contributes to the analysis of incidents retrospectively. KraftCERT is registered as a partner of EE-ISAC. There is also an American sister organisation, E-ISAC.

F Water and wastewater sector

The water and wastewater sector is not generally covered by the NIS Directive [56]; only water and wastewater works of a certain size (i.e. which cover a certain number of inhabitants) are included. In Norway, only the City of Oslo's Agency for Water and Wastewater Services (Oslo VAV) is covered by the NIS directive.

Oslo VAV is a member of KraftCERT but does not generally send notifications of incidents to them. The Norwegian Food Safety Authority is the supervisory authority for water and wastewater works, but at present only incidents relating to water quality are being reported to them.