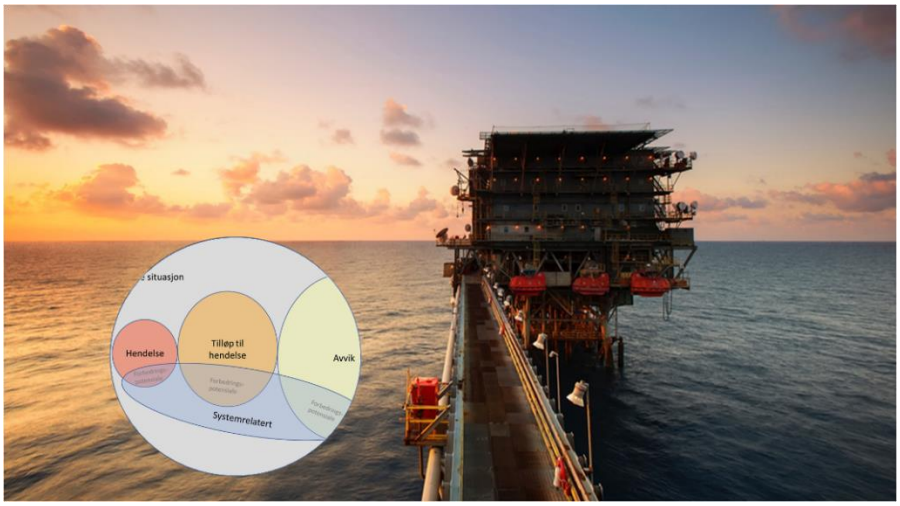


Rapport

Rapportering av hendelser i automatiserte systemer i boreoperasjoner

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

Rapportnummer:
2021:01416 - Åpen

Oppdragsgiver:
Petroleumstilsynet

SINTEF Digital
Postadresse:
Postboks 4760 Torgarden
7465 Trondheim

Sentralbord: 40005100

info@sintef.no

Foretaksregister:
NO 919 303 808 MVA

Rapport

Rapportering av hendelser i automatiserte boresystemer

EMNEORD:
Boring
OT-system
Kontrollsystem
Sikkerhet

VERSJON
Version 04

DATO
2021-12-16

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

OPPDRAGSGIVER(E)
Petroleumstilsynet

OPPDRAGSGIVERS REFERANSE
Kristian Solheim Teigen

PROSJEKTNUMMER
102025164

ANTALL SIDER OG VEDLEGG:
62+ Bilag/vedlegg

SAMMENDRAG

Dette arbeidet er en forstudie om hvordan hendelser, tilløp til hendelser og avvik innenfor automatiserte systemer detekteres, registreres og eventuelt varsles til Ptil i dag, samt ulike aktørers roller i bearbeiding av data fra slike situasjoner. Det tas utgangspunkt i en oppgave innen bore- og brønnoperasjoner, men det er også samlet inn informasjon om rapportering og håndtering av hendelser og avvik i andre relevante bransjer. Til sammen gir dette grunnlag for å foreslå hvordan man kan etablere og systematisere rapportering av hendelser og avvik i automatiserte systemer, kontrollsystemer og sammenkoblede løsninger i petroleumsvirksomheten.

UTARBEIDET AV
Maria Vatshaug Ottermo

SIGNATUR
Maria Vatshaug Ottermo
Maria Vatshaug Ottermo (16. Dec. 2021 13:51 GMT+1)

KONTROLLERT AV
Ranveig Kviseth Tinmannsvik

SIGNATUR
Ranveig Kviseth Tinmannsvik
Ranveig Kviseth Tinmannsvik (16. Dec. 2021 15:54 GMT+1)

GODKJENT AV
Anita Øren

SIGNATUR
Anita Øren
Anita Øren (17. Dec. 2021 08:59 GMT+1)

RAPPORTNUMMER	ISBN	GRADERING	GRADERING DENNE SIDE
2021:01416	978-82-14-07700-1	Åpen	Åpen

Historikk

VERSJON	DATO	Versjonsbeskrivelse
02	2021-08-24	Skisse til Ptil for kommentar
03	2021-11-19	Rapportutkast til Ptil for kommentar
04	2021-12-16	Endelig rapport

Kreditering av bilder:
Forside: Equinor
Øvrige: Pixabay

Innholdsfortegnelse

Sammendrag

Innledning

Formålet med denne rapporten har vært å gi næringen og Ptil økt innsikt i hvordan hendelser, tilløp til hendelser og avvik innenfor automatiserte systemer detekteres, registreres, klassifiseres og eventuelt videreapporteres til Ptil per i dag, samt ulike aktørers roller i bearbeiding av slike situasjoner. I rapporten er det tatt utgangspunkt i bore- og brønnoperasjoner, men det er også samlet inn informasjon om håndtering av hendelser i andre relevante bransjer. Dette er videre brukt som grunnlag for å foreslå hvordan man kan etablere og systematisere rapportering av hendelser og avvik i automatiserte systemer, kontrollsystemer og sammenkoblede løsninger i petroleumsvirksomheten.

Arbeidet er i hovedsak basert på dokumentgjennomgang, intervju og workshop samt interne arbeidsmøter.

Bakgrunn

I henhold til Ptils styringsforskrift §19 og aktivitetsforskriften § 49 skal den ansvarlige sikre at data som har betydning for helse, miljø og sikkerhet blir samlet inn og bearbeidet, samt evaluere effektiviteten av vedlikeholdet systematisk på grunnlag av registrerte data for ytelse og teknisk tilstand. Evalueringen skal brukes til kontinuerlig forbedring av vedlikeholdsprogrammet, jf. styringsforskriften § 23.

Men, i hvilken grad registreres og bearbeides tilløp til hendelser hvor det under andre omstendigheter kunne blitt en fare- og ulykkessituasjon? Hvilke data rapporteres i tilfeller hvor for eksempel personell må gripe inn og overta kontroll over de automatiserte systemene eller hvis det oppstår mindre avvik som ikke følges opp systematisk? Klarer vi å fange opp og utnytte tilgjengelige data og informasjon om disse situasjonene på en tilstrekkelig måte slik at det kan brukes til fremtidig analyse og læring? Kan erfaring fra sammenlignbare industrier utnyttes for å gi bedre rapportering av avvik og hendelser i bore- og brønnoperasjoner?

Automatiserte systemer i boring

Automatiserte boresystemer blir kun brukt på et fåtall rigger, men installeres etter hvert stadig flere steder. Automatiserte systemer benyttes for eksempel ved trykkstyring (Managed Pressure Drilling - MPD), i systemer som blir brukt for å kjøre heisverk og for kontroll av boreparametere. I rapporten gis en kort oversikt over ulike automatiserte systemer som brukes i boring. I tillegg gis en vurdering av hvilke data som kan og bør logges for disse automatiserte systemer for å sikre at man har tilstrekkelig meningsfull informasjon om avvik eller tilløp til hendelser.

Hendelseshåndtering i boring

Det er tatt utgangspunkt i en forenklet prosessflyt for håndtering av en hendelse fra den oppstår til den detekteres, registreres, klassifiseres, analyseres og følges opp. Basert på intervjuene uttrykkes det bekymring for at økt rapportering av tilløp til hendelser og avvik skal føre til større belastning på borer. En er redd for at økt rapportering av mange små avvik vil kunne stjele oppmerksomhet fra den allerede komplekse boreprosessen og i verste fall føre til manglende oppfølging av hendelser med storulykkesrisiko. Automatisert rapportering og filtrering av hendelser og avvik er derfor ønskelig. En annen viktig konklusjon fra intervju og workshop er at det mangler et standardisert system for rapportering som kan sikre deling av informasjon på tvers av selskap. Det mangler også etablerte selskapsinterne krav til hvilke hendelser og tilløp som skal rapporteres og hvordan de skal rapporteres.

Hvordan etablere og systematisere forståelse av uønskede hendelser og omsette det til læring og forbedring?

Et av målene med denne rapporten har vært å foreslå hvordan man kan etablere og systematisere bearbeiding av hendelser, tilløp til hendelser og avvik i petroleumsvirksomheten. Forslagene innbefatter

bruk av et standardisert rapporteringssystem, mer detaljerte og standardiserte taksonomier for situasjoner som muliggjør automatisk rapportering og klassifisering av avvik, samt økt deling av data på tvers av selskap. For å understøtte et slikt felles løft, kan det vurderes å etablere et felles interesseorgan/forum for aktører innen boring og brønn for erfaringsutveksling og mulige samarbeids- og forbedringsprosjekter.

Anbefalinger

Det er gitt 10 anbefalinger til tiltak for næringen, hvorav fem retter seg mot hva som rapporteres og deles, mens de resterende omhandler forhold som påvirker rapportering og oppfølging. Det er gitt 4 anbefalinger til tiltak for Petroleumstilsynet, hvorav to retter seg mot standardisert rapportering og klassifisering og de øvrige mot opplæring og borers arbeidsbelastning.

Vi ser behov for å etablere nye og standardiserte måter å samle inn, analysere og dele data og kunnskap på for å sikre interoperabilitet og fremtidig læring. I tillegg er det behov for å etablere kunnskap om hvordan man kan tilrettelegge for større grad av automatisert rapportering.

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 Innledning

1.1 Mål og hensikt

Dette arbeidet er en forstudie om hvordan hendelser, tilløp til hendelser og avvik innenfor automatiserte systemer detekteres, registreres og eventuelt varsles til Ptil i dag, samt ulike aktørers roller i bearbeiding av slike situasjoner. Med aktører menes her de ulike selskapene som er involvert i boreprosessen (for eksempel borekontraktør, boreleverandør, operatørselskap etc.). Det tas utgangspunkt i en oppgave innen bore- og brønnteknologi, men det er også samlet inn informasjon om håndtering av hendelser i andre relevante bransjer. Til sammen gir dette grunnlag for å foreslå hvordan man kan etablere og systematisere rapportering av hendelser og avvik i automatiserte systemer, kontrollsystemer og sammenkoblede løsninger i petroleumsvirksomheten.

SINTEFs delmål for oppdraget

Følgende delmål knyttet til IKT- hendelser og tilløp til hendelser er spesielt vurdert/hensyntatt i oppdraget:

1. Gi en oversikt over og vurdere hvordan IKT-hendelser og tilløp til hendelser bearbeides [1] med spesiell vekt på bore- og brønnteknologi.
2. Gi en oversikt over og vurdere hvordan IKT-hendelser og tilløp til hendelser bearbeides i andre næringer der automatisering og autonomi er i bruk eller nær kommersiell realisering.
3. Gi en oversikt over og vurder ulike aktørers rolle i bearbeiding av IKT-hendelser og tilløp til hendelser, inklusive andre aktører enn operatørselskaper som har rapporteringsplikt til Ptil.
4. Vurder i hvilken grad dagens bearbeiding av IKT-hendelser og tilløp til hendelser er tilstrekkelig for å gi meningsfull informasjon som kan brukes til læring og fremtidig risikoreduksjon.
5. Foreslå hvordan man kan etablere og systematisere bearbeiding av IKT-hendelser og tilløp til hendelser i petroleumsvirksomheten, inklusive om de kan beskrives som definert fare eller ulykkessituasjoner (DFU) eller lignende.

I det følgende vil vi bruke *industrielle IKT-systemer* som et samlebegrep for både automatiserte systemer og industrielle kontrollsystemer.

1.2 Begrensninger

Oppdraget er begrenset til IKT-systemer i bore- og brønnoperasjoner. I arbeidet med å innhente informasjon fra industrien har vi valgt å bruke en bred definisjon av begrepet IKT-hendelse. Bakgrunnen for dette var et ønske om å fange opp flest mulig eksempler på hendelser, tilløp til hendelser og avvik. Det vil si at det ikke bare er de hendelsene som typisk rapporteres til Ptil som er inkludert, men også tilløp til hendelser som kunne fått et annet utfall under andre omstendigheter. Det er derfor ikke selve brønnhendelsen som er i fokus, men først og fremst feil (og svakheter) i automatiserte systemer som utløsende eller medvirkende årsak til hendelse (for eksempel på grunn av manglende deteksjon, forvirrende informasjon til mannskap, feil respons, etc.). Tilfeller hvor programvare eller samspillet mellom programvare og bruker ikke fungerer som ønsket/forventet er også inkludert. Dette kan være alt fra konfigurasjonsfeil, sensordatafeil og brukerfeil, til programvarefeil (bugs) og cyberangrep. Oppdraget omfatter også passive automatiserte beslutningsstøttesystemer som gir råd til boreteamet under operasjoner. Systemer som er spesielt relevante i denne sammenheng er for eksempel trykkstyring under MPD og automatisert tripping, ettersom dette er sentrale operasjoner hvor det gjerne brukes systemer med høy grad av automatisering.

[1] Vi bruker *bearbeiding av IKT-hendelser i industrielle IKT-systemer* som en felles betegnelse for registrering, kvalitetssikring, analysering, rapportering, læring, samt varsling til Ptil av hendelser og tilløp til hendelser.

Et eksempel er en brønnkontrollhendelse ("Mærsk Gallant") hvor sensorfeil førte til for høy åpning av den automatisk styrte MPD-ventilen og dermed resulterte i for lavt brønntrykk inntil boreteamet forstod situasjonen riktig.

1.3 Begreper, definisjoner og forkortelser

1.3.1 Begreper og definisjoner

Definisjoner benyttes for at vi skal ha en lik forståelse av sentrale begreper, men definisjoner kan i seg selv gi en begrensning i forståelsen av et begrep, og det er ofte flere definisjoner av samme begrep.

Tabell 1 Begreper og definisjoner.

Begrep	Definisjon/beskrivelse	Referanse
24-7/ 24-timermøte	Daglige møter hvor siste 24 timer og neste 24 timer diskuteres	Denne rapporten
Avvik	Opplevd funksjon til et IKT-system er ikke i henhold til tiltenkt funksjon	Denne rapporten
Barriere	Tiltak som har til hensikt og funksjon enten å forhindre et konkret hendelsesforløp i å inntreffe, eller påvirke et hendelsesforløp i en tilsiktet retning ved å begrense skader og/eller tap. Funksjonen til disse barrierene ivaretas av tekniske, operasjonelle og organisatoriske elementer enkeltvis eller samlet	Ptil 2020 (ptil.no) [1]
Beredskap	Tekniske, operasjonelle og organisatoriske tiltak som planlegges iverksatt under ledelse av beredskapsorganisasjonen ved inntrådte fare eller ulykkessituasjoner for å beskytte mennesker, miljø og økonomiske verdier	NORSOK Z-013:2010 [2]
Cybersikkerhet	Beskyttelse av IKT-systemer mot angrep som kan ramme IKT-systemers konfidensialitet, integritet og tilgjengelighet. (Merk: I noen standarder inkluderer begrepet også utilsiktede hendelser)	IEC 62443 [3]
Definerte fare- og ulykkes-situasjoner (DFU-er)	Et representativt utvalg fare- og ulykkessituasjoner som brukes ved dimensjoneringen av beredskapen	Veiledning til AF § 73 [4]
Drillers forum	Forum der borere og andre møtes regelmessig for å dele og diskutere erfaringer.	Denne rapporten
Drilling recorder	System som logger alle tidsseriedata, kommandoer, operasjoner, skjermbilder og alarmer under boreoperasjonen.	Denne rapporten
Experience transfer system	Deling av observasjoner og erfaringer til relevante deler av intern organisasjon eller eksterne aktører	Denne rapporten
Fare	En utilsiktet uønsket hendelse	NSM 2015 [5]
Hendelse	En hendelse er enten en ulykke eller en nestenulykke/ et tilløp til hendelse.	Bridges [6]

Begrep	Definisjon/beskrivelse	Referanse
IKT	Alle systemer som utfører sin funksjon gjennom å sende, motta, lagre, prosessere og konvertere informasjon fra andre systemer	Riksrevisjonen, dokument 3:7 (2020-2021) [7]
IKT-hendelse	En hendelse som kan ramme IKT-systemers konfidensialitet, integritet og tilgjengelighet. IKT-hendelser omfatter både tilsiktede handlinger og utilsiktede hendelser	Riksrevisjonen, dokument 3:7 (2020-2021) [7]
IKT-sikkerhet	Beskyttelse av IKT-systemene, samvirket mellom systemene, tjenestene som leveres av systemene, eller informasjon som behandles i systemene. IKT-sikkerhet omfatter sikring av alt IKT-utstyr eller digitalt utstyr, inkludert driftskontrollsystemer	Riksrevisjonen, dokument 3:7 (2020-2021) [7]
Informasjonsteknologi (IT)	Teknologi som behandler informasjon	Dette prosjektet
Nestenulykke/Tilløp til hendelse	En nestenulykke er en uplanlagt sekvens av hendelser som kunne ha forårsaket skade hvis forholdene var annerledes eller hendelsen hadde fått lov til å utvikle seg, men ikke gjorde det i dette tilfellet	Bridges [6]
Nyhetsbrev/Bulletin	Kortfattet publikasjon som inneholder nyheter, analyser og kommentarer om aktuelle hendelser eller resultater	Denne rapporten
PDS forum	Faglig industriforum innen pålitelighet av instrumenterte sikkerhetssystemer i petroleumsvirksomheten	SINTEF [8]
PDS-metode	Metode for pålitelighetsanalyse av instrumenterte sikkerhetssystemer	SINTEF [9]
Risiko	Med risiko menes konsekvensene av virksomheten med tilhørende usikkerhet	Veiledning til RF § 11 [10]
Safety alert	Kortfattet informasjon om sikkerhetsobservasjon eller hendelse som spres til relevante deler av organisasjonen.	Denne rapporten
Sikkerhet	Sikkerhet innebærer beskyttelse mot farer og trusler som kan forårsake uønskede hendelser	NOU2015: 13 [11]
Stand	Et stand er normalt to eller tre borerør som er skrudd sammen. Disse står klar for bruk til uttrekking/nedkjøring (tripping) ifbm. boreoperasjoner. Ett stand er ca. 30 m.	Denne rapporten
Surge	Overtrykk i brønn, som resultat av at borestrengen senkes for fort ned i brønnen	Denne rapporten
Swab	Undertrykk i brønn, som resultat av at borestrengen løftes for fort ut av brønnen	Denne rapporten
Taksonomi	Vitenskapen om klassifisering, det vil si å dele inn ting eller begreper i klasser	Britannica [12]
Tilløp til hendelse	Se nestenulykke	Bridges [6]
Trussel	En tilsiktet uønsket handling	NSM 2015 [5]
Ulykke	En ulykke er en sekvens av uplanlagte hendelser og forhold som resulterer i skade på mennesker, miljø, prosess, produkt eller omdømme.	Bridges [6]

1.3.2 Forkortelser

Tabell 2 Forkortelser.

Forkortelse	Beskrivelse
ADC	Automated Drilling Control
AF	Aktivitetsforskriften
APOS	Automatisert prosess for oppfølging av instrumenterte sikkerhetssystemer (SINTEF prosjekt 2019-2022)
ASR	Annual Status Report
CMMS	Computerized Maintenance Management System
DBR/DDR	Daglig Borerapport/Daily Drilling Report
DBRS/DDRS	Daglig Borerapportsystem/Daily Drilling Reporting System
DFU	Definert Fare- og Ulykkessituasjon
HAZID	Hazard Identification
HMS	Helse, Miljø og Sikkerhet
HRS	Hovedredningssentralen
IACS/IAKS	Industrial Automation and Control Systems/Industrielt Automasjons- og Kontrollsystem
IEC	International Electrotechnical Commission
IF	Innretningsforskriften
IKT	Informasjons- og Kommunikasjonsteknologi
IMS	Information Management System
ISO	International Standardization Organization
IT	Informasjonsteknologi
NEK	Norsk Elektroteknisk Komite
NOG/NOROG	Norsk Olje og Gass
NORSOK	NORsk SOkkels Konkurranseposisjon
NOU	Norges Offentlige Utredninger
NS	Norsk Standard
NSM	Nasjonal Sikkerhetsmyndighet
NTSB	The National Transportation Safety Board
ODR	Organisatorisk Datarisiko
OT	Operasjonell Teknologi
Ptil/PSA	Petroleumstilsynet/Petroleum Safety Authority Norway
RF	Rammeforskriften
RNNP	Risikonivå i Norsk Petroleumsvirksomhet
ROC	Rate of Change
SAR	Search and Rescue
SAS	Safety and Automation Aystem/Sikkerhets- og Automasjonssystem
SF	Styringsforskriften
SIS	Safety Instrumented Systems/Instrumenterte Sikkerhetssystemer
SJA	Sikker Jobbanalyse

1.4 Metode og gjennomføring

Arbeidet er i hovedsak basert på dokumentgjennomgang, intervju, interne arbeidsmøter samt en halvdags workshop med industrien. Det er utført i et tverrfaglig prosjektteam med kompetanse innenfor blant annet instrumenterte sikkerhetssystemer, IKT-sikkerhet, boring og brønn, læring etter hendelser, samt petroleumsregelverk og standarder innenfor disse fagområdene.

Intervju har blitt gjennomført med oljeselskap, boreselskap og boreleverandører. Av hensyn til anonymitet oppgis ikke navnene på selskapene. Det er gjennomført ni gruppeintervju med totalt 37 informanter. Hovedtema for intervju var:

- Typer hendelser i forbindelse med automatiserte boresystemer
- Varslingssystem, innsamling og klassifisering
- Aktørbildet og rammevilkår for rapportering

En halv dags workshop har også blitt gjennomført med totalt 8 deltagere fra oljeselskap, boreselskap og boreleverandører. Tema for workshop var:

- Hvilke hendelser og tilløp til hendelser i automatiserte boresystemer bør rapporteres?
- Hvordan bør hendelser og tilløp til hendelser i automatiserte boresystemer rapporteres (aktørbilde og rammevilkår)?
- Hva er kritiske faktorer for implementering?

1.5 Rapportstruktur

Kapittel 2 oppsummerer funn fra tidligere studier angående rapportering av hendelser og tilløp til hendelser, hvilke krav som fins i Ptils regelverk, samt relevante standarder og retningslinjer.

Kapittel 3 gir en kort innsikt i automatiserte systemer i boring samt hvilke relevante data som kan/bør logges for de ulike systemene.

Kapittel 4 oppsummerer funn fra intervju og workshop med næringslivet og ser på detaljer knyttet til hvilke hendelser og tilløp til hendelser som rapporteres, hvordan de detekteres, rapporteres, klassifiseres, følges opp og analyseres.

Kapittel 5 diskuterer noen forhold som bør tas hensyn til ved videreutvikling av rapporteringssystem, samt forskjell mellom rapportering/gransking og tiltak/læring.

Kapittel 6 oppsummerer SINTEFs anbefalinger til tiltak for næringen og Ptil, samt behov for videre arbeid med kunnskapsinnhenting.

Det er 6 vedlegg (A-F). Disse vedleggene går mer i dybden på hvilke rapporteringssystem som brukes i andre bransjer enn boring, herunder luftfart, vegtransport, skipsfart, jernbane, kraftforsyning samt vann- og avløpssektoren.

I tillegg til figurer og tabeller, benytter vi faktabokser (grønne bokser til venstre på siden). Faktatabeller har også grønn farge, mens resultattabeller har blå farge.

2 Bakgrunn

I henhold til styringsforskriften § 29 Varsling og melding til tilsynsmyndighetene av fare- og ulykkessituasjoner [13] skal operatøren varsle Ptil ved fare- og ulykkessituasjoner. I veiledningen nevnes blant annet: "*b) brønnkontrollhendelser*" og "*i) situasjoner der normal drift av kontroll- eller sikkerhetssystemer blir forstyrret av arbeid som ikke er planlagt (IKT-hendelse)*". Men hva med alle situasjoner hvor det under andre omstendigheter kunne blitt en fare- og ulykkessituasjon? Klarer vi å fange opp tilgjengelig data og informasjon om slike situasjoner på en tilstrekkelig måte slik at vi kan bruke det til fremtidig analyse og læring? Figur 1 viser eksempler på ulike faktorer som kan påvirke om vi klarer å fange opp og utnytte hendelses- og avviksdata på en god måte.

Figur 1 Faktorer som kan påvirke om vi klarer å fange opp og utnytte data fra hendelser og tilløp til hendelser.

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.

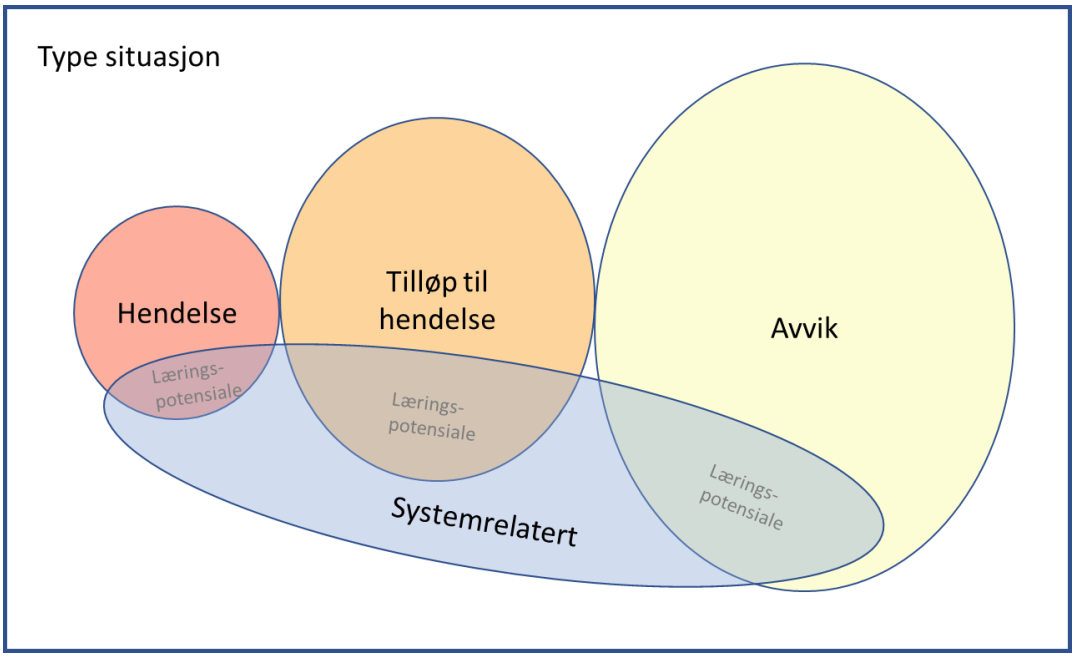
This gives a total population of roughly 10 000 errors for every accident.

Bridges 2012 [7]

Studier i flere bransjer tyder på at det er mellom 50 og 100 nestenulykker for hver ulykke [6]. I moderne og automatiserte systemer kan dette tallet være enda høyere på grunn av for eksempel bruk av beta programvare. Når slike avvik eller hendelser oppstår i autonome og automatiserte systemer er det ikke alltid de med letthet kan løses på stedet. For disse tilfellene må det være nok tilgjengelig data for å kunne analysere hendelsen i ettertid, slik at man kan være i forkant med å forhindre fremtidige uønskede hendelser. Og om de kan løses på stedet bør man uansett sikre seg nødvendig informasjon for systematisk forbedring og læring. Men hva er egentlig "nok tilgjengelige data"?

Denne rapporten skal bidra med vurderinger om *hvilke data som kan og bør logges* for sikkerhetskritiske automatiserte systemer slik at tilstrekkelig meningsfull informasjon om sikkerhetskritiske hendelser er tilgjengelig. Dette innebærer også å vurdere hvilken informasjon om hendelser og tilløp ulike brukere og roller i automatiserte systemer kan bidra med.

Figur 2 illustrerer at det kan være et uutnyttet læringspotensial både fra hendelser, tilløp til hendelser og avvik i automatiserte systemer, og det er noen av disse denne rapporten søker å avdekke. Selv små endringer i omstendighetene kan i noen tilfeller bety forskjellen mellom tilløp til hendelse og hendelse, eller mellom avvik og tilløp til hendelse. Det er derfor verdt å merke seg at et gitt læringspotensial ikke nødvendigvis er "forbeholdt" en av kategoriene.



Figur 2 Visualisering av læringspotensial knyttet til avvik, tilløp til hendelser og hendelser.

2.1 Funn fra tidligere studier

2.1.1 Automatisering og autonome systemer: Menneskesentrert design i boring og brønn

Rapporten "Automatisering og autonome systemer: Menneskesentrert design i boring og brønn" [14] ble utarbeidet på oppdrag fra Ptil i 2020. Der knyttes det usikkerhet til om dagens brukere av autonome boresystemer har nok erfaring og kjennskap til teknologien til å fastslå hvilke typer hendelser og tilløp til hendelser som bør rapporteres som bekymringsmeldinger, og om slike systemer brukes i tilstrekkelig grad. Det er heller ingen systematisk innhenting av data for mindre kritiske tilløp til hendelser fra myndighetenes side, og det er derfor usikkert om disse situasjonene fanges opp gjennom rapportering av DFU-er eller andre rapporteringspunkter til RNNP.

Det ene av fem tiltak i rapporten nevnt ovenfor peker på forhold som er spesielt relevante for denne rapporten: "Sørge for systematisk datarapportering og mulighet for analyser av drift". Dette tiltaket var basert på funn fra granskingsrapporter, workshop med deltagere fra Ptil, SINTEF og ulike bransjeeksperter samt litteraturgjennomgang. De aktuelle granskingsrapportene var knyttet til ulike bransjer, inkludert boring og brønn, ubemannet metro, autonom veitransport samt autonomi innen sjøfart og luftfart, hvor det, med enkelte unntak, ble funnet at det manglet systematisk datarapportering og dokumentasjon, spesielt for mindre hendelser. For eksempel ble det i en gransking av en ulykke knyttet til autonome biler utført av NTSB (The National Transportation Safety Board) påpekt at det var utfordrende å samle data til ulykkesanalysen. Dette medførte at en av anbefalingene fra NTSB var at datainnsamling og datarapportering fra autonome systemer bør prioriteres og være mer i fokus. I andre rapporter ble det også påpekt at det manglet taksonomier for datarapportering. Taksonomier vil bli diskutert i noe mer detalj i kapittel 2.4.7. I de tilfellene hvor systematisk datarapportering og dokumentasjon var tilgjengelig eller delvis tilgjengelig ble det konkludert med at løpende datainnsamlingen og rapporteringen fra sensorer i det autonome systemet både før og under hendelsen bidro til forståelse, læring og tiltak [14].

En av hovedkonklusjonene fra workshopen som ble gjennomført som basis for rapporten [14] var at "nesten-hendelser ikke fanges opp i tilstrekkelig grad verken hos myndigheter eller selskaper". Det er i dag

begrensede krav til hva som bør logges for hendelser og tilløp til hendelser som involverer automatiserte systemer i olje- og gassbransjen, og hvordan slike data eventuelt skal håndteres i forbindelse med rapportering og læring. Det ble derfor anbefalt at myndighetene og næringen bør samarbeide om å sette krav til hvilke data som skal logges for sikkerhetskritiske automatiserte systemer. Det ble i rapporten også påpekt at det generelt er mangelfull datainnsamling både på operatørnivå og på myndighetsnivå. Det kan tyde på at behovet for detaljert rapportering og samling av historiske data ikke er vurdert i forkant av en hendelse. Dette kan lede til manglende data og erfaringer fra nesten-hendelser som igjen fører til at man mangler en viktig basis for risikobasert tilsyn. Manglende rapportering av automatiseringsfeil kan også føre til at man ikke oppnår et riktig og hensiktsmessig nivå av tillit til de automatiserte systemene. Riktig nivå av tillit til teknologien er viktig for at sluttbruker skal kunne og adoptere den effektivt. Det vil si at det bør tilstrebes en balanse mellom tillit (tro på at teknologien fungerer slik den skal) og det å ha et kritisk blikk på teknologien [15].

I studien ble det også påpekt at den operative tidsperioden gjerne er mye kortere i boring enn for produksjonsprosesser slik at standard rapportering og oppfølging kan skje daglig eller per skift ved "Daglig borerapport" og "Daglig mudrapport". Mindre alvorlige hendelser vil rapporteres der uten å sette i gang en mer omfattende prosess, og det kan kanskje være en utfordring at de som rapporterer har lite kunnskap om de automatiserte systemene og derfor lett kan misforstå, rapportere feil eller kanskje underrapportere der mennesker tar over og berger situasjoner.

2.1.2 Bruk av modeller i boring

På oppdrag fra Ptil undersøkte SINTEF i 2020 ulike sider av temaet IKT-sikkerhet – robusthet i petroleumssektoren [16]. I det ene av totalt seks delprosjekter i dette oppdraget var formålet å diskutere utfordringer og muligheter ved bruk av modeller i boring, spesielt knyttet til hvordan modellene og data fra modellene kan brukes på en sikker måte og hvordan IKT-sikkerhet ivaretas [17]. Arbeidet var i hovedsak basert på dokumentgjennomgang, intervju og arbeidsmøter. Noen relevante funn fra dette arbeidet som peker mot viktigheten av å sette søkelys på at rapportering av hendelser for automatiserte løsninger var:

- Ved å innføre ny teknologi basert på modeller (og automatiserte løsninger) introduserer man også nye sårbarheter som må følges opp og håndteres. Samtidig skal en være bevisst på at boring med konvensjonelle løsninger, der systemene opereres opp mot toleransegrensen, ofte kan være farligere.
- For å sikre at modeller (og automatiserte løsninger) fungerer som tiltenkt må de testes, verifiseres og valideres. Det vil ofte være utfordrende å tenke gjennom alle mulige scenarioer modellene kan utsettes for. Det må dessuten logges hvilke endringer som er gjort på modellene og de automatiserte systemene, hvem som har gjort dem og når. Med en slik historikk vil det det være enklere å rette opp og identifisere både tilsiktede og ikke-tilsiktede feil som har medført hendelser.
- Det er et behov for mer kunnskap knyttet til håndtering av IKT-hendelser i forbindelse med bruk av modellkontrollerte operasjoner, og det vil være et behov for økt kompetanse hos fagpersonell og ledelse, samt å hente inn mer kunnskap om hvordan man kan øve og forberede de ansatte og organisasjonen på slike hendelser.
- Modeller som brukes for boring blir ofte så komplekse at det er vanskelig for bruker å ha full oversikt over og kontroll på alle underliggende beregninger og prosesser. Ofte gir det heller ingen merverdi for brukeren å ha denne oversikten, spesielt når modeller i større grad baseres på empiri og bruk av kunstig intelligens fremfor fysiske modeller. Likevel er det viktig at brukene ikke mister den mentale modellen av prosessen og den overordnede forståelsen for systemet som vil gjøre dem i stand til å gripe inn ved en uønsket hendelse. Det er behov for å hente inn mer erfaring og kunnskap om hvordan man kan muliggjøre slik meningsfull menneskelig kontroll i de tilfellene hvor man ikke nødvendigvis forstår de underliggende modellene.

2.2 Krav til rapportering i Ptils regelverk

I henhold til styringsforskriften §19 [13] og aktivitetsforskriften § 49 [4] skal den ansvarlige sikre at data som har betydning for helse, miljø og sikkerhet, blir samlet inn og bearbeidet, samt evaluere effektiviteten av vedlikeholdet systematisk på grunnlag av registrerte data for ytelse og teknisk tilstand. I disse paragrafene vises det til NS-EN ISO 14224 [18] og NS-EN ISO 20815 [19] (se tabeller nedenfor). En egen paragraf i styringsforskriften stiller krav til at bore- og brønnaktiviteter skal rapporteres til Petroleumstilsynets og Oljedirektoratets database.

PARAGRAF - TEMA	KRAV
Styringsforskriften [SF] (med tilhørende veiledning [13])	
§ 19 **Innsamling, bearbeiding og bruk av data**	Den ansvarlige skal sikre at data som har betydning for helse, miljø og sikkerhet, blir samlet inn, bearbeidet og brukt til å a) overvåke og kontrollere tekniske, operasjonelle og organisatoriske forhold, b) utarbeide måleparametere, indikatorer og statistikk, c) utføre og følge opp analyser i ulike faser av virksomheten, d) bygge opp generiske databaser, e) sette i verk korrigerende og forebyggende tiltak, deriblant forbedring av systemer og utstyr. Det skal settes krav til dataenes kvalitet og validitet ut fra det aktuelle bruksbehovet.
Veiledning til § 19	Denne paragrafen omfatter krav til alle typer data som har betydning for helse, miljø og sikkerhet. Spesifikke krav til data til ulike formål er gitt i andre paragrafer i denne forskriften, samt i rammeforskriften, teknisk og operasjonell forskrift og aktivitets- og innretningsforskriften. For å oppfylle kravene til data som nevnt i første ledd bokstav c og d, bør standarden ISO 14224 [18] brukes for pålitelighets- og vedlikeholdsdata til risikoanalyser på området helse, arbeidsmiljø og sikkerhet dersom innretningens posisjon gjør dette mulig. Hvis to uavhengige varslingsveier via faste samband ikke lar seg realisere, kan én av varslingsveiene erstattes med samband i den maritime mobile tjenesten.
Aktivitetsforskriften [AF] (med tilhørende veiledning [4])	
§ 49 **Vedlikeholdseffektivitet**	Effektiviteten av vedlikeholdet skal evalueres systematisk på grunnlag av registrerte data for ytelse og teknisk tilstand for innretninger eller deler av disse. Evalueringen skal brukes til kontinuerlig forbedring av vedlikeholdsprogrammet, jf. styringsforskriften § 23.
Veiledning til § 49	Med effektiviteten av vedlikeholdet som nevnt i første ledd, menes forholdet mellom de kravene som er satt til ytelse og teknisk tilstand, og de resultatene en oppnår. Ved registrering av data som nevnt i første ledd, deriblant feildata og vedlikeholdsdata, bør standardene NS-EN ISO 14224 [18] og NS-EN ISO 20815 vedlegg E [19] brukes.
Styringsforskriften [SF] (med tilhørende veiledning [13]	
§ 38 **Rapportering av bore- og brønnaktiviteter**	Operatøren skal rapportere bore- og brønnaktiviteter til Petroleumstilsynets og Oljedirektoratets database. Rapporteringen skal bruke brønn- og brønnbanebetegnelsen samt klassifiseringen som nevnt i forskrift om ressursforvaltning i petroleumsvirksomheten § 10.
Veiledning til § 38	Rapporteringen skal være i henhold til de kriteriene, tidsfristene og det formatet som er gitt i brukerveiledningen for DDRS-databasen som nevnt i første ledd.

2.3 Definerte fare- og ulykkeshendelser

Definerte fare- og ulykkessituasjoner (DFU-er) utgjør et representativt utvalg fare- og ulykkessituasjoner som brukes ved dimensjoneringen av beredskap (jf. veiledningen til aktivitetsforskriften § 73 Beredskaps-etablering [4]). Disse er innretnings- og lokasjonsspesifikke, dvs. det finnes ingen fast liste med DFU-er. Aktivitetsforskriften § 73 viser til styringsforskriften § 17 Risikoanalyser og beredskapsanalyser, og i veiledningen til styringsforskriften § 17 vises til NORSOK Z-013 [2]. I NORSOK Z-013 Annex C (informativt) er det angitt sjekklister for fareidentifikasjon (HAZID – Hazard identification) som man kan ta utgangspunkt i. Normalt vil en beredskapsplan inneholde i størrelsesorden 15-20 DFU-er (hydrokarbonlekkasjer, brann og eksplosjon, akutt forurensning, osv.), avhengig av hvor spesifikke de er. For hver DFU inneholder beredskapsplanen aksjonsplaner som angir hvem (ansvarlig) som skal gjøre hva (aksjon), og når (beredskapsfase).

Varsling utgjør den første av fem beredskapsfaser (jf. aktivitetsforskriften § 77 Håndtering av fare- og ulykkessituasjoner [4]). I mange tilfeller vil det være kritisk at varslingen blir gitt umiddelbart for å møte kravene til beredskap. Selv om behovene er noe forskjellig for de ulike DFU-ene, så vil det for de fleste DFU-er være behov for å varsle redningshelikopter, hovedredningssentralen (HRS) i nord eller sør, og 2. linje beredskapsledelse i eget selskap. Dette vil normalt utføres så raskt som mulig, gjerne angitt med tidskrav (for eksempel innen 3 minutter for SAR, og innen 10 minutter for Hovedredningssentralen (HRS) og 2. linje). Mange selskap har innleid beredskapsvakt som da utgjør 2. linje [20].

Bortfall eller tap av strømforsyning inngår ofte som en DFU blant operatørselskaper, men intervjustudien viser at hendelser innenfor automatiserte systemer ikke blir behandlet som en DFU.

2.4 Standarder og retningslinjer

I det følgende omtales noen relevante standarder og retningslinjer for rapportering av HMS-hendelser og teknisk tilstand ved automatiserte boreoperasjoner.

2.4.1 NS-EN ISO 14224

NS-EN ISO 14224 [18] gir et grunnlag for standardisert innsamling av pålitelighets- og vedlikeholdsdata for utstyr i petroleumsvirksomheten, inklusive utstyr for boreoperasjoner. Standarden definerer blant annet nedbrytning og klassifisering av utstyr, samt feilmodi, feilårsak og deteksjonsmetoder.

ISO 14224 (Appendix D-5) [18] skiller mellom følgende datakilder for etablering av pålitelighetsdata:

1. Generiske data (databaser og håndbøker) basert på driftserfaring fra lignende utstyr
2. Selskapsspesifikke data basert på driftserfaring fra eget utstyr
3. Produsentdata basert på driftserfaring fra utstyrsleverandør
4. Ekspertvurderinger basert på uttalelser fra tekniske eksperter
5. Data om menneskelige feilhandlinger (f.eks. ISO/TR 12489:2013, Annex H.2 [21])

2.4.2 IEC 615011/IEC 61508

Overordnet bruk av feildata er diskutert i IEC 61511-1 [22], Seksjon 11.9.3 og 11.9.4. Ifølge IEC 61511-1 skal pålitelighetsdata som brukes ved kvantifisering av effekten av tilfeldige feil, være troverdig, sporbar, dokumentert og begrunnet.

2.4.3 Norsk olje og gass 070

Ptil viser spesielt til retningslinjen: "070 Norwegian Oil and Gas Association Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry (Recommended SIL requirements)" [23] i sitt regelverk. Det

overordnede formålet med retningslinjen er å standardisere og forenkle anvendelsen av IEC 61508 [24] og IEC 61511 [22] i norsk petroleumsindustri.

Retningslinjen har et eget kapittel 8.5 "Requirements to Failure Data" som i stor grad viser til ISO 14224 [18].

2.4.4 SCSC-127E Data Safety Guidance

Safety-Critical Systems Club (SCSC) [25] har utgitt en veiledning for håndtering av sikkerhetsrelaterte data som vil være et nyttig underlag for utvikling av rapporteringssystem for autonome systemer.

Veiledningen representerer beste praksis for hvordan data (forskjellig fra programvare og maskinvare) skal håndteres i en sikkerhetsrelatert sammenheng. Formålet er å hjelpe organisasjoner med å identifisere, analysere, evaluere og behandle datarelaterte risikoer, og dermed redusere sannsynligheten for at datarelaterte problemer forårsaker uønskede hendelser. I veiledningen gis flere eksempler på at 1) *feil i data*, eller 2) *upassende bruk av data* i automatiserte systemer har bidratt til ulykker. Et eksempel på upassende bruk av data er et skipsnavigasjonssystems som ved bred feltvisning av kartdata, fjerner små grunne undervannsfunksjoner og dermed også fjerner viktig sikkerhetsrelatert informasjon på grunn av bildeskala.

Veiledningen identifiserer et bredt spekter av sikkerhetsrelaterte data og dataegenskaper (f.eks. nøyaktighet, tilgjengelighet) som må ivaretas for at systemet fungerer på en sikker måte (se Vedlegg B i veiledningen). Den er ikke begrenset til ytelsesdata under drift, men den omhandler spesielt hvordan data om industrielle kontrollsystemer som er lagret i IT-systemer, kan påvirke funksjonell sikkerhet av industrielle kontrollsystemer (f.eks. feil alarmgrenser registret i det industrielle kontrollsystemet).

Veiledningen inneholder et sett med spørsmål for vurdering av organisatorisk datarisiko (ODR) som inkluderer blant annet: alvorlighetsgraden av potensielle ulykker, organisatorisk modenhet, juridiske rammer, størrelse, kompleksitet og nyhetselement til system. Det resulterer i en rangering, fra ODR0 (som tilsvarer den laveste risikoen) til ODR4 (som tilsvarer til høyeste risiko) og dermed nødvendig innsats for håndteringen av datasikkerhetsrisiko. En del av prosessen er å forstå organisasjonskulturen og det er utviklet et kort spørreskjema for datasikkerhetskultur (vedlegg C i veiledningen), som kan hjelpe i dette

Dokumentet er ment å brukes som et supplement til eksisterende standarder og normer og tilpasset strukturen i ISO 31000 [26]. I likhet med IEC 61508 [24] er dokumentet skrevet for flere sektorer og må tilpasses til den enkelte sektoren. Vi er kjent med at det foreligger forslag om at IEC 61508 skal referere til denne veiledningen ved neste revisjon av standarden.

Datasikkerhet, datakilder og dataflyt i offshoreindustrien er også omhandlet i artikkelen "Data safety, sources and data flow in the offshore industry" [27].

2.4.5 NORSOK D-010:2021; Brønnintegritet i boring og brønnoperasjoner

NORSOK D-010:2021 [28] har et eget kapittel 5.10 "Experience transfer and reporting" som omhandler hvordan brønnaktiviteter og operasjoner skal dokumenteres og gjøres tilgjengelig for fremtidig bruk og kontinuerlig forbedring. Dokumentet gir kun overordnede krav til rapportering av hendelser som har betydning for helse, miljø og sikkerhet, og har derfor begrenset informasjon om hvordan man kan klassifisere hendelser eller etablere rapporteringssystem for automatiserte systemer.

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 Industrielle automasjons- og kontrollsystemer

NORSOK I-002:2021 [29] har et eget kapittel 8.2.2.2 "Data collection and storage" som stiller krav til at industrielle IKT-systemer skal være i stand til å registrere og rapportere tidsstemplede prosessverdier, hendelsesdata og beregnede data i tillegg til system- og applikasjonsdata.

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 Retningslinje PDS-forum/APOS

Det er ofte knyttet usikkerhet til kvalitet i innsamlede vedlikeholds- og hendelsesdata. Et viktig utgangspunkt for å eliminere noe av usikkerheten er å sikre at feil registreres på en konsistent måte. Ved å definere standardiserte utstyrsgrupper med veldefinerte systemavgrensninger samt tilrettelegge for høy tillit til valg av parametere for feilregistrering (for eksempel for feilmodus og deteksjonsmetode) kan man oppnå konsistent registrering [30]. Per i dag er ISO 14224 [18] aktivt brukt for innsamling av pålitelighets- og

vedlikeholdsdata for sikkerhetsutstyr i petroleumsvirksomheten, men gjennom arbeid i regi av PDS forum[2] er det kommet frem et behov for veiledning, eksempler og forklaringer som kan forenkle dagens bruk av ISO 14224 [18]. Med støtte fra Norges forskningsråd gjennom prosjektet "Automatisert prosess for oppfølging av sikkerhetssystem" har SINTEF derfor utgitt en retningslinje for standardisert rapportering av klassifisering av feil i instrumenterte sikkerhetssystemer i petroleumsvirksomheten [30]. Denne retningslinjen vil også være relevant for feilrapportering og klassifisering av boreutstyr. SINTEFs retningslinje tar utgangspunkt i ISO 14224 [18] med sikte på ytterligere standardisering og effektivisering av prosessen for feilrapportering og klassifisering av sikkerhetsutstyr. Et hovedmål har vært å operasjonalisere og forenkle taksonomiene (klassifiseringene) og gi eksempler, beskrivelser og illustrasjoner knyttet til parametervalg:

Mer spesifikt forventes det at denne retningslinjen vil bidra til:

- Mer effektiv og forbedret rapportering av hendelsesdata ved å gi enklere og mer intuitive taksonomier.
- Mer automatisert feilregistrering, klassifisering og analyse. I denne forbindelse er felles taksonomier og rapporteringsformater avgjørende.
- Et forbedret rammeverk for feilanalyser og gjennomføring av tiltak.
- Enklere og forbedret tilrettelegging for datadeling og sammenligning, både mellom operatører, mellom operatører og leverandører og som input til Ptil (dvs. RNNP).
- Integrering og anvendelse av automatiserte feilrapporteringssystemer (IMS, ASR, tilstandsovervåkings-systemer osv.).
- Økt tillit til, og dermed forbedret utnyttelse av dataene til læring.

Standardisert feilrapportering er relevant for:

- Personell som er ansvarlig for å utvikle og konfigurere informasjons-, vedlikeholds- og rapporteringssystemer (både operatører og leverandører).
- Personell som utfører vedlikehold og skriver notifikasjoner.
- Personell som klassifiserer og/eller kvalitetssikrer hendelsesdata.
- Personell som utfører dataanalyse og videre oppfølging.

For å forenkle feilregistrering og klassifisering foreslås algoritmer som kan redusere parametervalg. Et eksempel er begrensningen av antall mulige feilmodi basert på utstyrstype, f.eks. hvis en gassdetektor er valgt, er bare feilmodi som er relevante for gassdetektorer inkludert.

I det følgende presenteres eksempler på standardiserte utstyrsgrupper samt anbefalte taksonomier for deteksjonsmetode og feilmodus.

2.4.7.1 Standardiserte utstyrsgrupper

Gruppering av sikkerhetskritisk utstyr med sammenlignbare egenskaper er viktig for å:

- Strukturere feildata; utstyrsgruppene definerer hvordan feil kan aggregeres og slås sammen med det formål å estimere feilrater for utstyr.
- Muliggjøre standardiserte (og utstyrsspesifikke) taksonomier og automatisert registrering og klassifisering av feil på utstyr i en gruppe.
- Sammenligne, slå sammen og analysere data fra ulike anlegg og/eller operatører.
- Muliggjøre effektiv og standardisert driftsoppfølging på et anlegg (og på et passende nivå).

[2] *PDS forum er et samarbeid mellom oljeselskaper, ingeniørselskaper, konsulenter, leverandører og forskere med spesiell interesse for instrumenterte sikkerhetssystemer. Det er mer enn 20 deltakende bedrifter i forumet som møtes to ganger i året for workshops, presentasjoner og tekniske diskusjoner.*

SINTEFs retningslinje [30] foreslår at utstyr grupperes hierarkisk i tre nivå (se eksempel for gassdetektorer i Figur 3). Denne strukturen er utledet fra analyser av gjeldende bransjepraksis, internasjonale standarder, ekspertvurderinger og identifiserte behov og krav til påfølgende bruk av data.

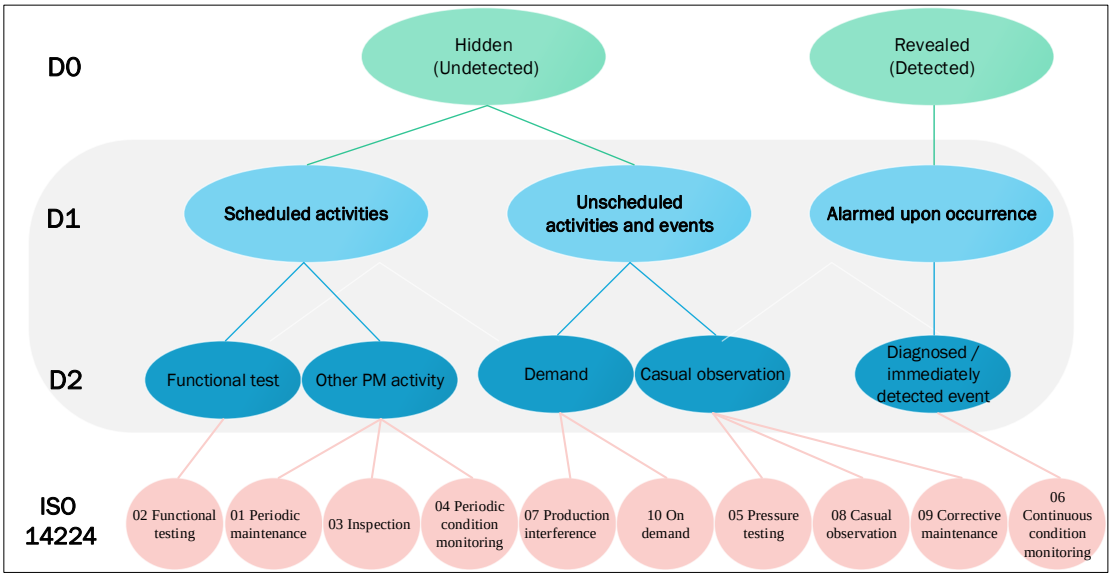
Main Equipment groups – L1	Safety Critical Elements (subgroups) – L2	Equipment attributes – L3								Equipment attribute categories and *Comments*
		Measuring principle	Design/mounting principle	Actuation principle	Medium properties	Dimension	Location/ Environment	Application	Diagnostics / Configuration	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

Figur 3 Taksonomi for utstyrsgrupper [30].

2.4.7.2 Deteksjonsmetode

Klassifiseringen av deteksjonsmetode er viktig for å kunne skille mellom feil som varsles automatisk (Detektert - "Detected") og feil som oppdages manuelt (Udetektert/latent - "Undetected") (se Figur 4). Feil som varsles ved selvtesting eller tilstandsovervåking, er mindre kritiske siden korrigerende tiltak kan iverksettes umiddelbart. Udetekterte/latente feil derimot vil kunne være kritiske og hindre tiltenkt sikkerhetsfunksjon dersom en uønsket hendelse skjer før feilen er oppdaget og korrigert. Disse feilene kan avdekkes ved både planlagt og ikke-planlagt vedlikehold.

SINTEFs retningslinje [30] foreslår en fleksibel og hierarkisk taksonomi som forener ulike selskapspraksiser og samtidig er kompatibel med ISO 14224 [18].



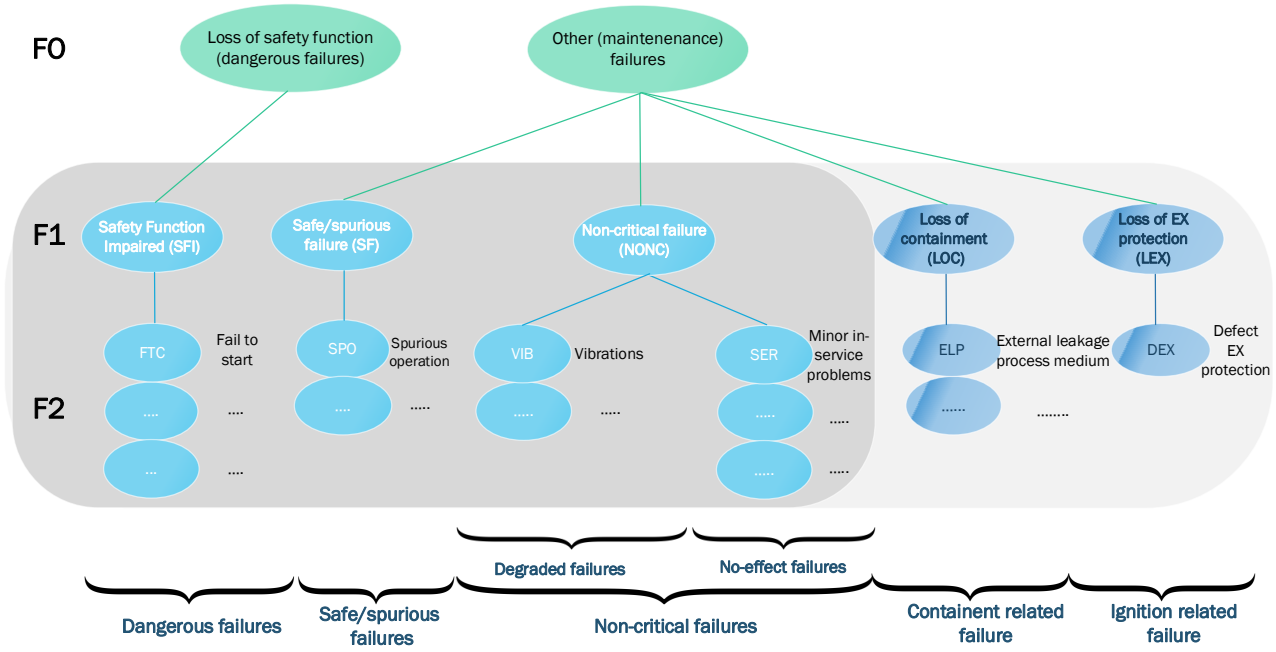
Figur 4 Taksonomi for deteksjonsmetode [30].

2.4.7.3 Feilmodi

Feilmodi beskriver hvilken effekt feil har på systemets ytelse. Viktige feilmodi for sikkerhetsutstyr er:

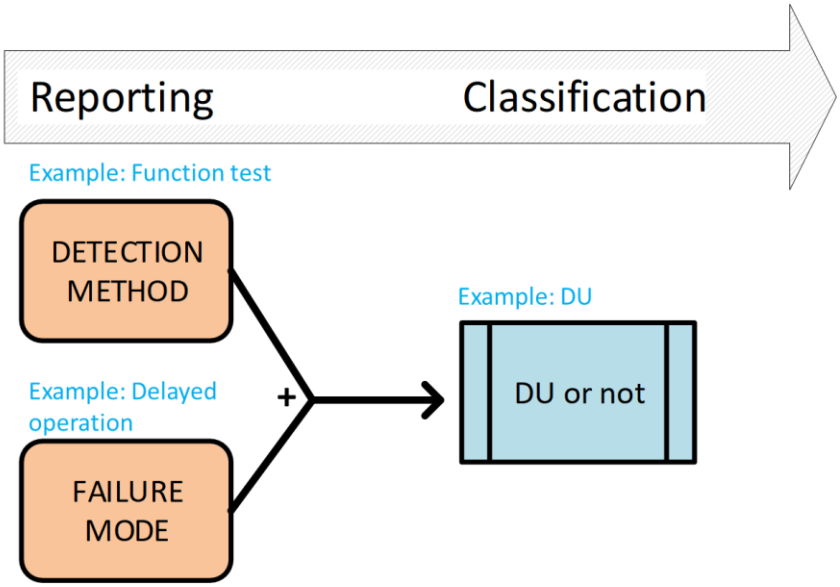
- Farlige feil ("Dangerous"): Tap av sikkerhetsfunksjon (f.eks. brannpumpe starter ikke).
- Vedlikeholdsrelaterte feil:
    - Sikre feil ("Safe/spurious"): Utilsiktet aktivering av sikkerhetsfunksjon (f.eks. falsk alarm fra gassdetektor).
    - Ikke-kritiske feil ("Non-critical"): Ingen svekket sikkerhetsfunksjon (f.eks. ventil kan stenge ved behov, men må repareres på grunn av andre forhold). Kan ofte være avgjørende for produksjonen.
    - Andre feil: For noen typer utstyr vil det være andre sikkerhetskritiske feilmodi enn den primære sikkerhetsfunksjonen (f.eks. lekkasje fra ventiler eller svikt av tennkildebeskyttelse).

SINTEF foreslår en hierarkisk utstyrsspesifikk taksonomi for feilmodi for sikkerhetsutstyr (se Figur 5). Bruken av noen få, nøye utvalgte feilmodi for hver utstyrsgruppe vil forenkle rapporteringen og dermed forbedre både mengden og kvaliteten på rapporteringen. Dvs. når man velger en feilmodus på nivå 1, vil antallet relevante feilmodi på nivå 2 være begrenset. Nivå 2-listen over feilmodi vil være fullstendig i den forstand at feilmodiene "Annet" eller "Ukjent" unngås, og at man heller prøver å fange opp alle mulige relevante feilmodi for en spesifikk utstyrstype.



Figur 5 Taksonomi for feilmodi [30].

Automatisk brukerveiledning er anbefalt for å hjelpe til med riktig valg av parametere, for eksempel ved å bruke popup-vinduer, mus-over og forhåndsutfylte valg. Slike hjelpetekster kan f.eks. komme opp i vedlikeholdssystemet der feilmeldingen er registrert eller sekundært i driftsprosedyrene som følger med feilrapportering og klassifisering. Automatisk generering av enkelte parametere er en annen foreslått forenkling. For eksempel, når du har valgt deteksjonsmetode og feilmodus, kan feilklassen bestemmes automatisk og dermed kan også vedlikeholdsprioritet (høy, middels, lav) foreslås, se eksempel i Figur 6 [31].



Figur 6 Potensiale for automatisk feilklassifisering [31].

2.4.8 Industri 4.0

På en boreinnretning er det installert store mengder utstyr som skal assistere boreprosessen og forhindre at farlige hendelser oppstår. For å sikre god oppfølging av dette utstyret, må vi samle inn data om det, og ikke minst, etablere kunnskap om hvordan man bruker og deler data og informasjon for å skape verdi Tradisjonelt har ofte bedrifts- og/eller fagspesifikke løsninger, verktøy og proprietære formater hindret deling av informasjon og data, men etter hvert som maskiner, produkter og anlegg blir stadig smartere, må de kunne kommunisere autonomt i digitale, globale nettverk [32]. Tyskland har gjennom en årrekke drevet intensiv forskning- og utvikling innenfor dette domenet og er verdensledende på området for integrering av individuelle systemløsninger gjennom deres Industri 4.0-initiativ. Det grunnleggende formålet med Industri 4.0 er å muliggjøre sømløs interoperabilitet mellom objekter i den fysiske verden, og dermed tilrettelegge for nye nivåer av automatisering og produktivitetsutbytte. De fysiske objektene må derfor være virtuelt representert og koblet sammen, og Industri 4.0 gjøres dette ved hjelp av en oversetter som ofte refereres til som "den digitale tvillingen" av det fysiske objektet. Denne digitale representasjonen av objektet er kjent som Asset Administration Shell (AAS). Noen industrier, for eksempel fabrikkvirksomhet, er kommet et stykke på vei med å definere og systematisere egenskaper og informasjon vedrørende sitt utstyr, men for petroleumsbransjen er det fortsatt et behov for å definere og utvikle åpne standarder og løsninger som tilrettelegger for et digitalt økosystem for hele verdikjeden.

3 Automatiserte systemer i boring

Automatiserte boresystemer blir fremdeles brukt på et fåtall rigger, men det brukes for eksempel ved trykkstyring i Managed Pressure Drilling (MPD), og i systemer som blir brukt for å styre heisverk (eksempelvis automatisert tripping og connection og auto driller som finnes i ulike varianter for optimalisering av selve boringen). Tabell 3 beskriver sentrale komponenter og utstyr involvert i boring og tripping, samt data som kan/bør logges for å tilrettelegge for best mulig deteksjon og læring. Tabell 4 beskriver viktige kontrollsystemfunksjoner som brukes i automatiserte operasjoner, samt hvilke data disse systemene trenger for å fungere optimalt.

Tabell 3 Oversikt over komponenter og utstyr for boring, samt relevante (sensor)data som kan/bør logges.

System/komponent	Relevante data som kan/bør logges
Borestreng: En samlebetegnelse for alt av rør og utstyr som kobles til top drive for å utføre boring. Deles gjerne inn i borekrone, nedihullsutstyr (BHA - bottom hole assembly) og borerør. Borekrona gjør selve boringen, mens borerør sørger for å bringe borekrona og BHA inn og ut av brønnen, i tillegg til å overføre rotasjonskraft fra top drive og transportere borevæske ned i brønnen. BHA er den nederste delen av borestrengen, og inneholder en rekke spesialiserte komponenter, blant annet vektrør, utstyr for å styre borekrona, samt måleutstyr og loggeutstyr. Data fra sensorene i BHA overføres enten gjennom selve brønnen og borevæsken via elektromagnetiske eller akustiske signaler, eller via en spesiell type borerør med innebygget signalkabel, såkalt wired pipe. Signaloverføring via wired pipe er vesentlig dyrere, men gjør det mulig å sende data opp til boredekk med uovertruffen båndbredde og latenstid, slik at parametere fra brønnen kan måles og logges mye mer nøyaktig og hurtig, og gi et tydeligere og riktigere bilde av forholdene i brønnen.	I et BHA er det normalt mange sensorer, og bortfall eller feil i disse målingene kan være sikkerhetskritisk ved at en får mindre eller feil informasjon om forholdene i brønnen. Eksempel kan være sensorer som måler brønntrykk eller borevæsketetthet. Mange av målingene i BHA og top side er viktige for å kunne begrense slitasje på borekrone og BHA, slik som vekt på bit, dreiemoment og vibrasjoner. Ugunstige forhold kan skade borekronen og BHA-komponenter. Dette er normalt ikke sikkerhetskritiske hendelser, men kan f.eks. medføre behov for ekstra tripping og dermed økt total risiko. Bør derfor logges for å gi det totale bildet.
Borevæske: Borevæske fungerer primært som et verktøy for brønnkontroll (ved å skape nødvendig trykk nede i brønnen for å unngå spark og utblåsning), men sørger også for å smøre og avkjøle borekrona (og strengen), samt frakte borekaks opp til overflaten gjennom ringrommet. Riktig væskestrøm og trykk oppnås ved å styre relevante pumper og ventiler, samt justere borevæskens egenvekt (tetthet).	Får å få oversikt over borevæskens egenskaper måles blant annet egenvekt (tetthet), nivå/mengde, viskositet og temperatur. Det er vanlig å måle borevæskens egenskaper ved hjelp av manuell prøvetaking, men det jobbes også en del med automatisk måling. For å få hyppigere måledata (og dermed bedre kontroll på borevæsken) er det ønskelig med automatisk måling av borevæskens egenskaper.
Foringsrør: Brønnen forsterkes seksjonsvis ved å senke ned foringsrør (også kjent som casing eller liner) og sementere disse fast. I tillegg til å unngå kollaps i brønnen, sørger foringsrør for at gass og væske ikke siver ut av eller inn i brønnen.	Få/ingen sensorer direkte knyttet til foringsrør, men andre brønnrelaterte målinger kan indirekte si noe om tilstand på utforing.
Sikkerhetsventiler/BOP: Sikkerhetsventilene utgjør en ekstra barriere mot uønskede brønnhendelser som spark og utblåsning, og fungerer ved at en eller flere ventiler kan "stenge av" brønnen dersom brønnkontroll ikke kan ivaretas av borevæsken. Dersom det er borestreng i brønnen, kan sikkerhetsventilene lukkes rundt borestrengen eller klippe den. Ved trykkbalansert boring vil sikkerhetsventilene i BOP-en overta for MPD systemet mens en vedlikeholder et høyt trykk når en har oppdaget innstrømning fra reservoaret.	På BOP er det status på ventiler og kontroll-hydraulikk samt kommunikasjon som er mest relevant. Dette gjelder spesielt for de delene av BOP som benyttes av MPD-systemet. I tillegg måles borevæsketrykk i ringrommet ved BOP

System/komponent	Relevante data som kan/bør logges
Stigerør og strekksystem: Stigerør (riser) brukes som en "forlengelse" av brønnen for å frakte borevæske og borekaks fra havbunnen og opp til overflaten. Stigerøret fungerer også som en slags "navlestreng" for sikkerhetsventilene på havbunnen, ved at dedikerte linjer og kabler for hydraulikktrykk og strøm/kommunikasjon er festet til stigerøret. Det vil være noe relativ bevegelse mellom stigerøret og boredekket, på grunn av bevegelser/krefter i sjøen og på grunn av riggbevegelser dersom det er en flytende innretning. Det er derfor nødvendig med et strekksystem (riser tensioner) som holder stigerøret stramt med tilnærmet konstant kraft for å unngå at den relative bevegelsen skaper problemer.	Viktige parametere/tilstander for stigerør og strekksystem er vinkler, krefter og diverse statussignaler. Disse dataene påvirkes først og fremst av naturkrefter og riggbevegelser, og er viktige for posisjoneringssystemer (dynamic positioning, DP) og for automatiske frakoblingssekvenser på BOP. For automatiserte systemer for boring og tripping er stigerørdata mindre relevant.
Hivkompensator: For flytende innretninger vil det være vertikal bevegelse mellom boredekket og havbunnen/brønnen, og det er nødvendig med et system som kompenserer for disse bevegelsene ved boring. Uten slik kompensering vil borekrona bli utsatt for store variasjoner i vekt på bit, eller til og med løftes opp fra og slås ned i bunnen av brønnen på grunn av innretningens vertikale bevegelser (hiv). Hivkompensering kan gjøres på flere måter, f.eks. ved å løfte kronblokka opp og ned i motfase med hivbevegelsene, eller ved å styre heisverket på en måte som kompenserer for innretningens bevegelser.	For et hivkompenserende system er det trykk/kraft samt posisjon, hastighet og akselerasjon som er de viktigste målingene. Kommando- og statussignaler er også relevante.
Heisverk: For å løfte og senke top drive og borestreng trengs et solid løftesystem dimensjonert for den aktuelle lasten. Det vanligste er å bruke heisverk, som inneholder en stor trommel som roteres for å trekke inn eller slippe ut boreline. I kombinasjon med et taljesystem bestående av kronblokk og løpeblokk, skaper heisverket den nødvendige løftekraften. Et alternativ til heisverk er å bruke hydrauliske sylindre til å løfte og senke top drive og borestreng. I slike systemer er det festet en eller flere taljer på toppen av løftesylindrene, og top drive løftes av en eller flere kabler som går fra festepunkt(er) på dekk, over taljen(e) og ned til top drive.	For heisverk er det kraft (torque, hook load, etc.), posisjon, hastighet og akselerasjon som er de viktigste parameterne. Disse måles direkte eller indirekte på ulike måter. I tillegg er det viktig å ha oversikt over temperatur, kommando og status på bremser, motorer og gir.
Top drive: En boremaskin som heises opp og ned i boretårnet, og gjør det mulig å bære lasten av borestrengen og rotere den samtidig. Top drive (og borestrengen) løftes og senkes av heisverket, og den vertikale bevegeligheten (avstanden fra nedre posisjon til øvre posisjon) avgjør hvor lange stands (rørseksjoner) som kan brukes ved boring og tripping.	Vertikal kraft (hook load), dreiemoment og rotasjonshastighet er viktige målinger. For å unngå at top drive løftes for høyt eller senkes for lavt, brukes også et sett med posisjonssensorer (i tillegg til posisjons-målinger fra heisverk og hivkompensator). Kommando- og statussignaler er også relevante.
Rørhåndteringssystem: Når borestrengen trekkes ut av brønnen er det nødvendig å lagre stands på en effektiv måte etter hvert som de brekkes ut fra borestrengen, og når strengen skal kjøres inn i brønnen må de lagrede seksjonene hentes frem og skrus på strengen. Slik rørhåndtering (pipe racking) innebærer samspill mellom flere forskjellige maskiner: • Iron roughneck: Maskin for å skru rørkoblinger sammen eller fra hverandre. • Rørstabler (pipe racker): Maskin (eller maskiner) som frakter stands fra/til brønnen og til/fra fingerbord (sted for vertikal lagring av stands)	For maskinene som er involvert i rørhåndtering er det spesielt deres respektive posisjoner og hastigheter i forhold til hverandre samt trykk/krefter som er viktig. Diverse statussignaler for sensorer, kommunikasjon og hydraulikk- og strømforsyning er også relevant, for deteksjon av problemer som kan føre til f.eks. stans eller kollisjon.

System/komponent	Relevante data som kan/bør logges
• Fingerbord: Stedet hvor stands blir lagret kalles fingerbord. Foruten å være lagringssted sørger også fingerbordet for å holde rørene på plass slik at de ikke beveger seg eller velter. I tillegg til å frakte stands mellom brønn og fingerbord, sørger rørhåndteringssystemet for å sette sammen og ta fra hverandre stands, samt frakte enkeltrør mellom rørdekk/rørlager og boredekk. Disse oppgavene innebærer enda flere maskiner, som må samhandle med hverandre og med iron roughneck og rørstabler: • Rørhåndteringskran: Kran for å frakte enkeltrør (i horisontal stilling) mellom rørlager og catwalkmaskin. • Catwalkmaskin: Frakter enkeltrør (liggende) mellom rørdekk og boredekk. • HTV-maskin: HTV står for "horizontal-to-vertical", og denne maskinen løfter enkeltrør ut/opp fra catwalkmaskinen slik at de går fra å være horisontale til å være vertikale. De vertikale enkeltrørene skrus så sammen til stands (ved hjelp av iron roughneck) og fraktes til fingerbord av rørstabler.	

Tabell 4 Sentrale kontrollsystemfunksjoner for automatisert boring og tripping.

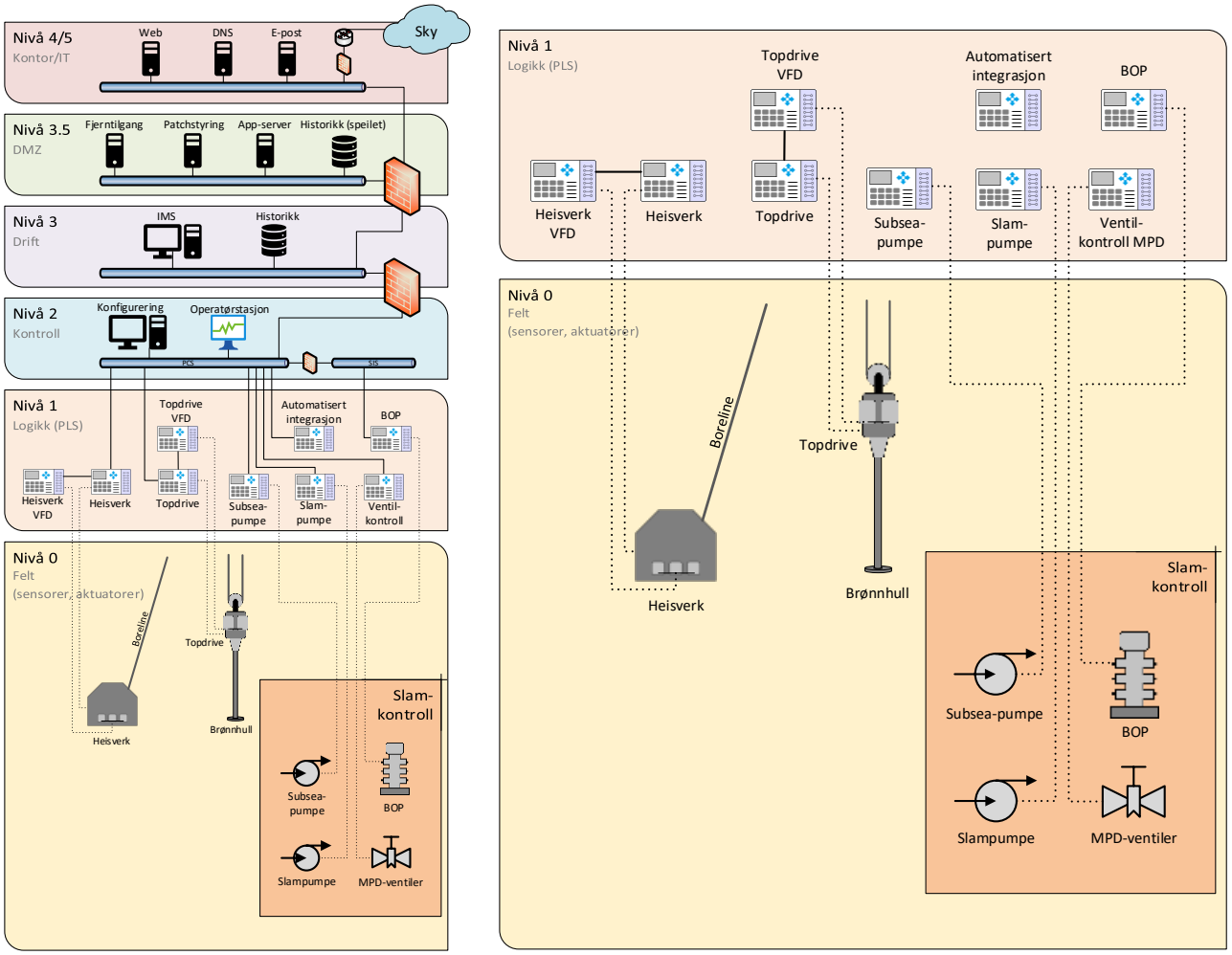
Funksjon	Viktige inputdata
Trykkbalansert boring (MPD): Det finnes forskjellige varianter/konsepter for trykkbalansert boring, og felles for alle er at de gjør det mulig å styre trykket i brønnen mye mer nøyaktig enn ved tradisjonell boring. I tradisjonell boring er det primært borevæskens egenvekt som bestemmer trykket i brønnen, mens man i MPD benytter ventiler og pumper til å justere trykket på en mer dynamisk og fleksibel måte. Dette gjør at trykkvariasjoner i brønnen kan reduseres betraktelig, slik at det blir lettere å bore i smale trykkvindu, hvor det er lite "spillerom" mellom formasjonstrykket og fraksjonstrykket. MPD medfører ekstra automatisering, maskinvare og program-vare som må fungere godt sammen med øvrig utstyr for boring. Videre er volumkontroll mer nøyaktig enn for tradisjonell boring.	Ved trykkbalansert boring er det viktig å ha oversikt over alle parametere som er relevante for brønnkontroll. I tillegg til borevæskens egenskaper er det viktig å ha oversikt over alle relevante trykkmålinger, status/posisjon på ventiler og status og væskestrøm i pumper. Brønntrykket påvirkes også av borestrengens vertikale hastighet. For rask senking av borestreng kan føre til overtrykk (surge), mens for rask heising kan føre til undertrykk (swab) fordi MPD-systemet ikke klarer å styre ventiler og væskestrøm fort og nøyaktig nok til å kompensere for borestrengens bevegelser.
Automatisert styring av heisverk: Brønn, borestreng, top drive, heisverk og evt. hivkompensator utgjør til sammen et komplekst mekanisk system, og det er ikke trivielt å ha kontroll på alle krefter og bevegelser. Ved boring ønsker man å ha stabil og riktig WOB (vekt på bit), og ved tripping er det viktig å unngå at for rask senking eller heising fører til for store surge- eller swab-trykk. Styringen av heisverk må blant annet ta hensyn til både fjæreffekter (borelina og borestrengen strekkes betydelig under last slik at lengden ikke er konstant) og dynamiske krefter (top drive og borestreng er så massive at det skal mye til å stanse dem eller sette dem i bevegelse) for å oppnå ønsket hastighet, posisjon og kraft. Interne krefter i heisverket må kompenseres for med mindre kraften på borestrengen måles mer direkte. Heisverket begrenses også av hvor mye effekt som er tilgjengelig fra	For å kunne styre heisverket optimalt behøves informasjon om blant annet: • Krefter (kraft i boreline, torque i trommel, hook load etc.) • Posisjoner (trommelvinkel, hiv, hiv-kompensator, top drive) • Hastigheter (trommel, hivbevegelse og hivkompensatorbevegelse) • Akselerasjoner (trommel, hivbevegelse og hivkompensatorbevegelse) • Strekk (hvor mye boreline spoles inn før top drivebevegelse starter) • Temperaturer (motorer, gir, bremser etc.) • Tilgjengelig effekt fra strømforsyning

Funksjon	Viktige inputdata
generatorene/strømnettet og hvor mye/kraftig bremsing som kan gjøres uten å overopphete komponenter.	• Diverse kommando- og statussignaler
Automatisert rotasjon av borestreng: På samme måte som borestrengen strekkes i lengderetning, oppfører den seg også som en lang torsjonsfjær. Det betyr at akslingen ut fra top drive må rotere et stykke før rotasjonskrafta i torsjonsfjæra blir høy nok til å overvinne friksjonen og rotere borekrona. Hvis man ikke har god kontroll på rotasjonskrafta og -hastigheten fra top drive risikerer man å få torsjonsvibrasjoner som øker slitasjen på nedihullsutstyret. Et eksempel på torsjonsvibrasjon er såkalt stick-slip, hvor nedre del av borestrengen varierer mellom å rotere "for sakte" (stick) og "for fort" (slip). I stick-fasen har borekrona liten eller ingen rotasjonshastighet, mens krafta i torsjonsfjæra bygges gradvis opp fordi top drive fortsetter å rotere. Slip-fasen begynner når den lagrede torsjonskrafta har blitt så stor at borekrona begynner å rotere fort, og rotasjonen fortsetter frem til borekrona har "gått forbi" top drive slik den bremses og ny stick-fase starter. Disse uønskede fenomenene kan i stor grad unngås med smart styring av top drive og/eller heisverk (heisverk kan påvirke friksjonen ved å justere vekt på bit). Eksempler på funksjoner for å redusere torsjonsvibrasjon er "soft torque" og stick-slip-deteksjon.	Relevante parametere/målinger for styring av borestrengrotasjon: • Kraft (torque i motorer og aksling) • Rotasjonshastighet • Rotasjonsakselerasjon • Vibrasjonsindikatorer • Vekt på bit • Borevæskestrøm • Temperaturer (motorer, gir etc) • Tilgjengelig effekt fra strømforsyning • Diverse kommando- og statussignaler • Aksielle og torsjonelle krefter og bevegelse i BHA og langs strengen (i noen tilfeller måles disse direkte på noen posisjoner, ellers må de beregnes)

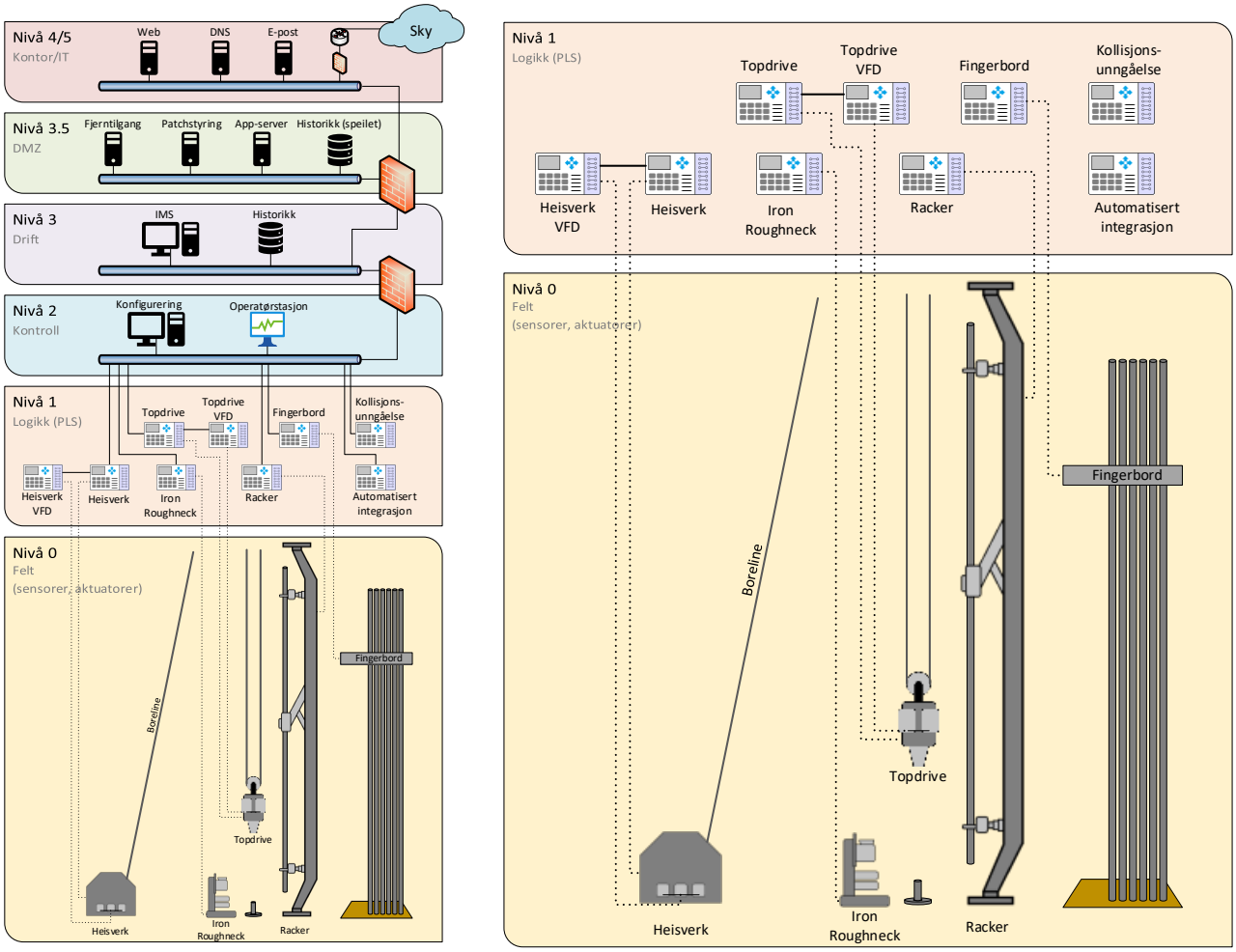
Mye av inputdataen som brukes i automatiserte systemer er "direkte" sensorverdier, men det er også en del indirekte/deriverte variabler som er viktige, f.eks. hvor mye strekk som er i borelina eller avstanden mellom borekrona og bunnen av brønnen.

Automatiserte systemer for boring og tripping vil typisk inneholde flere av funksjonene i Tabell 4, ettersom både boring og tripping innebærer koordinert styring av heisverk, top drive og borevæske for å optimalisere prosessen og samtidig ivareta brønnkontroll. Funksjonene inngår gjerne som "moduler" i et overordnet automatisert system som håndterer koordineringen mellom de involverte systemene. Felles for de automatiserte funksjonene (og det overordnede systemet) er at kontrollalgoritmene bruker modeller for å optimalisere prosessen. Noen automatiserte systemer brukes til direkte styring, mens andre kun gir beslutningsstøtte.

Sentrale komponenter fra tabell 3 er vist i Figur 7 og Figur 8, for å visualisere koblinger og interaksjoner under henholdsvis boring og tripping. I tillegg til de omtalte komponentene viser figurene også komponenter fra høyere nivåer i en overordnet nettverksarkitektur.



Figur 7 Forenklet topologifigur for å visualisere kommunikasjon og samspill mellom forskjellige komponenter under boring. Inneholder ikke nødvendigvis alle koblinger og komponenter som finnes i automatiserte systemer.



Figur 8 Forenklet topologifigur for å visualisere kommunikasjon og samspill mellom forskjellige komponenter under tripping. Inneholder ikke nødvendigvis alle koblinger og komponenter som finnes i automatiserte systemer.

4 Hendelseshåndtering i automatiserte systemer

Det er per i dag ikke tydelig verken for myndighetene eller næringen hvordan informasjon og data fra hendelser, tilløp til hendelser og avvik bør sikres for fremtidig risikoreduksjon ved bruk av automatiserte systemer. Det varierer hvilke hendelser og avvik som registreres, hvordan og av hvem eller/hvilket system hendelsene detekteres, hvilket system de registreres i, hvordan de klassifiseres og av hvem eller hvordan de følges videre opp. Figur 9 viser en forenklet prosessflyt for håndtering av en hendelse, fra den oppstår til den detekteres, registreres, klassifiseres, analyseres og følges opp. Hvert enkelt av disse punktene er omhandlet i mer detalj i de kommende underkapitlene.

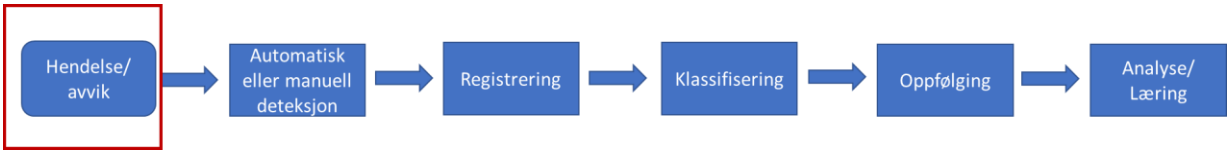
Figur 9 Forenklet prosess for hendelseshåndtering i boring.

4.1 Hvilke hendelser og avvik rapporteres?

Dette delkapitlet omhandler hvilke hendelser, tilløp til hendelser og avvik som trigger håndtering i henhold til den forenklede prosessflyten skissert i Figur 10. Ifølge informantene i intervju rapporteres det mest systematisk på nedetidshendelser og slike rapporter behandles metodisk av organisasjonen. Hva som rapporteres og prioriteres avhenger av kritikalitet. Det skilles gjerne mellom:

- Nedetid (dvs. riggen ute av drift/ikke i operasjon)
- Systemnedetid (dvs. riggen kan operere, men ett eller flere system er ute av funksjon). Eksempler kan være ting som må re-startes, bytte av harddrive etc. som ikke direkte påvirker boreoperasjonen.

Mindre hendelser og supportforespørsler som påvirker systemnedetid rapporteres også inn, men det er mindre systematikk i denne rapporteringen, for eksempel kan det sendes per epost og håndteres videre inn i organisasjonen som "lessons learned" eller tas opp som tema på daglige møter etc. På daglig basis gjøres det vurdering av de små hendelsene slik at det kan foreslås forbedring eller små justeringer. Generelt forsøker man å melde inn kun det som er kritisk for borer direkte til han/henne for å hindre unødige distraksjoner under selve boreprosessen.



I det følgende gis eksempler som selskapene selv identifiserer som på avvik, hendelser og tilløp til hendelser som per i dag typisk vil rapporteres eller registreres, og som derfor vil inngå i første del av prosessflytdiagrammet. Alle eksemplene er hentet fra intervjuene som ble gjennomført med industrien.

Manuell overstyring/kjøring i avvikssituasjoner:

- Overstyring av antikollisjonssystem grunnet feil eller bortfall av sensorer
- Overstyring av antikollisjonssystem ved for trange/strenge bevegelsesrom
- Kjøring i avvikssituasjon ved samtidig bruk av ADC (automated drilling control) og wired pipe, som ikke er kompatible med hverandre (wired pipe krever folk på dekk, mens ADC har som bruksbetingelse at det ikke er noen på dekk). Kjøring i avvikssituasjon krever SJA.
- Kjøring i avvikssituasjon i påvente av utbedring av fysisk feil eller programvarefeil. Krever SJA.

- Situasjoner der man glemmer å aktivere automatiserte systemer/funksjoner etter at de har vært deaktivert i forbindelse med f.eks. utbedring/vedlikehold. Kan skape feilaktige antakelser om at automatisert system opererer og griper inn.

Feil knyttet til deling og input av data:

- Feil konfigureringsfil
- Feil boretrykksprofil

Feil knyttet til alarmgrenser (systemet gir alarm eller systemet automatisk griper inn):

- Stopp av bevegelse på top drive ved kraftoverskridelser
- Trykkavvik (for eksempel i forbindelse med lekkasjer eller blokkering)
- Feil på høyspenttavle
- Avvik i borevæskenivå
- Avvik i væskestrøm

Feil knyttet til kommunikasjon/utfall:

- Kommunikasjonsavbrudd for programvare som brukes til å styre automatisert system
- Mistet kommunikasjon med mudpumpe
- Utfall av programvare

Feil knyttet til igangsetting/oppgraderinger

- Feil på parametersetting
- Sanntidssimulering avviker fra preliminær simulering
- Avvikende pre-simuleringer fra ulike leverandører
- Små programvaredeler som må oppdateres etc.
- Manglende erfaring med nytt system

Annet

- Feil i deteksjon av dårlig hullrensing
- Feil ved nedstengning av mudpumper
- Heisverk stoppet på grunn av feil i tilknyttet automatisert styringssystem
- Programvarefeil

4.1.1 Hvilke hendelser og avvik rapporteres ikke?

I intervjuene ble det også etterspurt eksempler på hendelser, tilløp til hendelser og avvik som sjelden eller aldri rapporteres. Typiske eksempler som ble nevnt var:

- Feil grunnet forveksling av desimaltegn og tusenskilletegn
- Feil grunnet forveksling av enheter
- Feil ved inntasting av verdier
- Feil parametere/grenseverdier mottatt av tredjepart
- Enkelte avvik fra forventede verdier rapporteres via telefon og løses på stedet uten at de blir systematisk registrert.
- Bortfall av kommunikasjon med støttetjenester på land. Fører ikke til nedetid, men gjør ofte at man velger å deaktivere funksjoner som påvirkes av bortfallet (systemnedetid).
- Dynamisk variasjon i hook load ved trekking ut av hull fordi automatisert system innfører hastighetsbegrensning for å unngå for lavt trykk i brønn. Hastighetsbegrensningen påføres og opphører periodisk slik at det kan oppfattes som at det "napper" i strengen. Noen operatører synes dette er helt greit, mens andre foretrekker å ha full kontroll selv.

- Ustrakt bruk av "override" eller at mannskap velger å ikke bruke enkelte funksjoner fordi de pleier å føre til stans og feilmeldinger. Dette er eksempler som ofte blir sett på som feil bruk, og som i noen tilfeller kan føre til at barrierer som er innebygd i programvare blir fjernet

Det er verdt å merke seg at få eller ingen cyberhendelser eller -angrep er registrert, men at industrien setter spørsmålstegn ved om dette kan stemme.

4.1.2 Funn relatert til hvilke hendelser og avvik som rapporteres

Resultatetabellene med funn i de kommende underkapitlene oppsummer innspill fra næringen og gjengir hvordan noen informanter opplever status og utfordringer med rapportering av hendelser i automatiserte systemer. I siste kolonne har vi tatt med SINTEFs overordnede kommentarer knyttet til utsagn fra informantene. SINTEFs vurderinger og videre anbefalinger som i stor grad er basert på funn fra disse tabellene er oppsummert i Kapittel 6. Begrepet "hendelser" er i noen steder i tabellene brukt som et samlebegrep for avvik, tilløp til hendelser og hendelser i automatiske systemer.

Tabell 5 Innspill fra næringen relatert til hvilke hendelser og avvik som rapporteres

	Input fra intervju/workshop	SINTEF kommentar
1.	Svært få (ingen) cyberhendelser registrert. Det settes spørsmålstegn ved om dette kan stemme.	• Trengs det strengere/tydeligere krav til rapportering av slike hendelser? • Det mangler en kategori for IKT-hendelser (havner det under "annet"?). • Kan rapporteringsverktøyene for HMS utvides/tilpasses til å også håndtere IKT-hendelser, for å utnytte personellets evne og motivasjon til å bruke disse verktøyene?
2.	God kultur og lav terskel for rapportering av avvik. Terskelen for å rapportere er blitt blir lavere.	Hva kan være årsaken til det? • Fokus på rapportering gjennom observasjonskort ufarliggjør rapportering? • Enklere rapporteringssystemer? • Rapporterer på det automatiserte systemet, ikke menneskelige feil (føler seg ikke direkte ansvarlig)? • Kan økt automasjonsgrad føre til både til lavere rapporteringsterskel og færre hendelser, eller kan det skyldes underrapportering?
3.	Ønsker mer kontinuerlig og detaljert registrering av operasjonelle data og automatisk rapportering av avvik, f.eks. • Automatisk registrering av endringer i viktige input-parametere som f.eks. diametere som påvirker beregning av maksimal hastighet ved tripping. • Registrere antall ganger personell har korrigert manuelt før avvik fanges opp. I dag er man i enkelte selskaper avhengig av at man overfører slike meldinger muntlig, uten mulighet til å kjenne til videre oppfølging.	Hva vil være konsekvensen av automatisert rapportering? • Det vil være mange positive effekter, men det kan kanskje også føre til degradert systemforståelse eller for stor tillit til systemene? • Hvem tar over rapporteringen hvis systemet er nede? • Kan det gi unødig støy (fanger opp for mye)?
4.	Hvilke hendelser som rapporteres er i dag personavhengig. Tilbakemeldinger blir mange ganger så subjektive at de blir	Skyldes dette manglende forståelse av systemer, uklare kriterier, kultur, annet?

	Input fra intervju/workshop	SINTEF kommentar
	vanskelige å tolke. Etterlyser krav og rammeverk for å si hva som må rapporteres og hvem det må rapporteres til.	• Kan man finne kriterier som gjør det mer entydig hva som skal rapporteres? • Har man tydelige kriterier hos operatør, både for hendelser som skal rapporteres til myndigheter og andre typer avvik?
5.	Manglende prosessforståelse kan være et hinder for god rapportering. Kanskje mer enn manglende systemforståelse. Borer har stort sett bra forståelse av selve systemet, men det er likevel viktig at han eller hun forstår begrensningene i systemene.	• Kan dette føre til underrapportering? • I et fremtidsscenario hvor systemene gjør vesentlig mer og operatøren gjør vesentlig mindre enn i dag, kan det tenkes at borer forstår for lite til å kunne rapportere godt, men i et slikt scenario trenger man kanskje ikke boreoperatøren i det hele tatt?
6.	Utfordringer knyttet til kvalitet på programvare og data kan føre til misforståelser og feilrapportering.	Følges det en beste praksis for hvordan data og programvare skal håndteres i en sikkerhetsrelatert sammenheng?
7.	Stort fokus på rapportering av hendelser som medfører nedetid og hvilken og leverandør/hvilket system nedetiden kan knyttes til.	• Dette kan gå på bekostning av sikkerhet (dersom rapportering påvirkes av ansvars- og kostnadsfordeling). • Trenger bransjen en mer uavhengig vurdering av hendelser?
8.	Bevisstgjøring rundt avvik og hendelser knyttet til effektivitet. Lett å mobilisere ved nedetid, men kanskje må man bli bedre på å fange opp mer av det som går på effektivitet også?	• Manglende forståelse for hvilken innvirkning redusert effektivitet har på prosessen? • Hvor mye må effektiviteten reduseres for at det skal være meningsfullt å rapportere (og hvordan skal man kunne forutse dette)?
9.	Det er generelt vanskelig å forutse hva konsekvensene av et avvik kan være under andre omstendigheter (worst case), slik at det ofte kun er hendelser med betydelige konsekvenser som rapporteres. Ved tripping har man for eksempel hatt anledning til å legge for mye last på heisverk i forhold til det resten av systemet kan håndtere. Ser da ikke nødvendigvis rekkevidden av at man kan forårsake power black out. ROC-filter (rate of change) for å eliminere denne muligheten lagt inn.	• Kan det hjelpe å inkludere flere avviksscenarioer i treningssimulatorer?

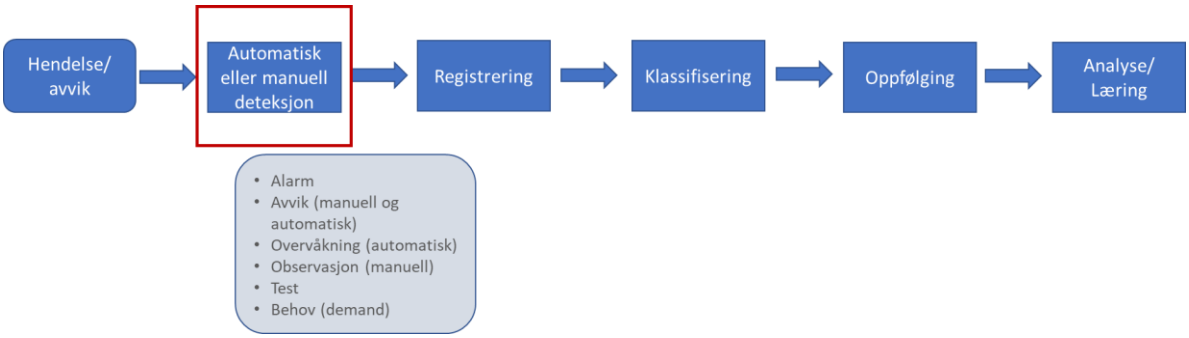
4.2 Hvordan detekteres hendelser og avvik?

Dette delkapitlet omhandler funn relatert til hvordan hendelser og avvik detekteres. En hendelse eller et avvik oppdages enten ved automatisk eller manuell deteksjon. Ulike manuelle og automatiske deteksjonsmetoder er listet i figuren under, men noen konkrete eksempler på hvordan avvik og hendelser detekteres kan være:

- Dersom systemet opererer utenfor grenseverdier eller avvik fra forventet respons oppstår kan dette detekteres både automatisk og manuelt, dvs. man kan få varsel via alarm/annet varsel eller for eksempel visuell deteksjon.
- Avvik fra forventet respons kan detekteres både automatisk og manuelt, f.eks. ved at gamle og nye system kjøres i parallell og at man observerer (visuelt) eller får alarm om avvikende respons der det

egentlig forventes at systemene skal være like. For slike situasjoner blir det viktig å definere hva som defineres som et avvik slik at det kan fanges opp både manuelt og automatisk. Det samme gjelder for avvik mellom ulike simuleringer og mellom simulering og operasjon.

- Hendelser og avvik kan også detekteres under testing og i drift (demand) eller basert på tilbakemeldinger fra underleverandører som har overvåkningsfunksjon.



Tekniske ressurser som brukes for deteksjon av hendelser kan være f.eks.:

- Selvdiagnostikk og tilstandsovervåkning
- IMS (Information management system)
- Alarmsystemer
- Safety and Automation System
- Simuleringer
- Drilling recorder

Eksempler på organisatoriske og operasjonelle ressurser som er relevant for deteksjon av hendelser:

- Vedlikeholdsprogram
- Vedlikeholds-/teknisk personell
- Inspeksjonsprogram
- Inspeksjonspersonell
- Daglig drift og tilfeldig observasjon
- Kontrollromsoperatører (både onshore og offshore)
- Ekspertovervåkning (fra systemleverandør)
- Feltoperatører
- Opplæringsprogram

4.2.1 Funn relatert til hvordan hendelser og avvik detekteres

Tabell 6 Innspill fra næringen relatert til hvordan hendelser og avvik detekteres

	Input fra intervju/workshop	SINTEF kommentar
1.	I drilling recorder har boreren en "Knapp" som trykkes dersom borer føler at noe ikke er helt som forventet. Følges som regel opp i ettertid, men det er ingen formelle krav til oppfølging.	• Blir potensialet utnyttet fullt ut så lenge det ikke fins krav eller systematikk rundt oppfølging av slike avvik?
2.	Stor alarmtetthet og "unødvendige" alarmer er en utfordring og alarmhåndtering og prioritering blir viktig for å unngå overbelastning av operatør i slike sammenhenger. Alarmtekster kan ikke heller ikke være for like (en eller flere nesten like alarmer med ulik betydning) eller vanskelige å forstå.	• Hvordan sørge for å samle inn data knyttet til de mindre viktige alarmene uten å skape støy?

	Input fra intervju/workshop	SINTEF kommentar
		• Hvordan skille mellom alarmer til borepersonell og såkalte system-alarmer for vedlikehold? • Hvordan få til balanse mellom det som oppleves som "støy" og viktige meldinger? • Tilpasse alarmer til brukerprofil?

4.3 Hvordan rapporteres/registreres hendelser og avvik

Dette delkapitlet omhandler hvordan hendelser og avvik detekteres og rapporteres. Rapportering/registrering av en hendelse eller feil avhenger av type hendelse, kritikaliteten på hendelsen og hvem (eller hva) som detekterer hendelsen. For de fleste selskapene er det et skille mellom rapporterte hendelser og tilløp til hendelser knyttet til henholdsvis HMS og kvalitet, og de har ulike systemer for å håndtere disse. Noen har også ulike rapporteringsveier for prosessrelaterte hendelser (rapporteres til ledelse) og programvare/teknisk feil (rapporteres til utviklingsteam eller teknisk personell). Leverandørene som mottar nedetidsrapporter fra sine kunder opplever at det varierer hvor informative og strukturerte de ulike kundenes beskrivelser er. Noen rapporter er detaljerte og ryddige (hva har skjedd, under hvilken operasjon, etc.), mens andre rapporter forteller lite utover at "noe har skjedd". Eksempler på mulig rapporterings-/registreringsmåter er listet i figuren nedenfor. Under figuren er det også listet tekniske, organisatoriske og operasjonelle ressurser som er relevant for rapportering av hendelser og avvik.

Tekniske ressurser som brukes for registrering av hendelser kan, i tillegg til rapporteringssystemene beskrevet i kapittel 4.3.1, være for eksempel:

- Nettbrett
- Arbeidsstasjoner

Organisatoriske og operasjonelle ressurser som er relevant for registrering av hendelser kan være f.eks.:

- Rammeverk/taksonomi for rapportering
- Retningslinjer for rapportering
- Systemer/algoritmer for automatisk feilregistrering
- Personell
- Trenings-/motivasjonsprogram og kompetanse

4.3.1 Rapporteringssystem og metoder

I det følgende gis en kort beskrivelse av ulike rapporteringssystem. Det er valgt å skille mellom to hovedgrupper av rapporteringssystem: HMS&K og vedlikehold. Imidlertid er det noen av rapporteringsmåtene som kan omfatte både HMS&K og vedlikehold, som for eksempel observasjonskort.

I mange tilfeller, som også er illustrert i eksempelscenarioet i kapittel 4.3.3 vil den første meldingen om at en hendelse eller situasjon er oppstått komme per telefon, personlig beskjed eller epost. I intervjuene ble det trukket frem at fordelen med telefon eller personlig beskjed er at man kan være mer detaljert i beskrivelse av hendelsen. Ulempen kan være at det ikke blir registrert på en systematisk måte, noe som kan medføre underrapportering og redusert mulighet til fremtidig læring. En epost vil gi skriftlig dokumentasjon, men ikke systematisk lagring og oppfølging. Det er også en fare at viktige beskjeder ikke når frem til mottaker og dermed aldri vil bli fulgt opp.

4.3.1.1 HMS og kvalitetssystem

SYNERGI Life ol.

Hendelser som omhandler HMS&K rapporteres typisk i programmer som Synergi Life og Tracker. Begge programmene er kjente HMS&K-rapporteringssystem som er i allmenn benyttelse i ulike virksomheter/bransjer. Registrering av hendelser gjøres typisk ved innlogging på PC, men det er ofte også mulig å rapportere på smarttelefon. Ved innmelding av hendelse/avvik registreres som regel tid og sted samt en beskrivelse av hendelsen. Det vil også være mulighet for å legge ved bilder og andre vedlegg.

Både kvalitets- og sikkerhetshendelser registreres i slike programmer. Dette inkluderer også nedetid. Det skilles dessuten ofte mellom administrative og prosessrelaterte hendelser. Ikke alle hendelser ligger åpent for alle. Noen hendelser må man ha spesiell tillatelse eller tilhøre en spesifikk del av organisasjonen for å se. Ifølge noen av informantene er de viktigste HMS-relaterte hendelsene åpne, og det fins mekanismer for deling med riggselskaper som har kontrakt for operatørselskapet, men det knyttes usikkerhet til om dette er gjeldende for bransjen som helhet.

I Synergi registreres også potensiell og faktisk konsekvens av en hendelse, f.eks. personskade, fraværsskade, brann, utslipp til miljø, økonomisk tap etc.

Observasjonskort

Observasjonskort er en fellesbetegnelse på kort som brukes til rapportering av atferd eller usikre tilstander på arbeidsplassen. I selskapene kan disse ha ulike navn som for eksempel ”Stopp-kort”, "Safe kort" eller ”Obs-kort. Virksomhetene bruker gjerne observasjonskort som en del av forbedringsprosessen og som et virkemiddel for å skape økt fokus blant de ansatte på helse, miljø- og sikkerhet (HMS). Ofte er det et ønske om å holde rapporteringsfrekvensen høy, og det har vært ulike kampanjer i flere av de intervjuede virksomhetene knyttet til dette. Det som rapporteres på observasjonskort er ofte mindre observasjoner og hendelser som ikke krever umiddelbare tiltak. Et viktig mål med observasjonskort er å gjøre rapporteringsterskelen så lav som mulig og å gjøre brukerne kjent med systemet slik at det blir lettere å rapportere de mer alvorlige hendelsene.

Daglige borerapporter ("Daily drilling reports")

Alle operatører for boring på norsk kontinentalsokkel er pålagt å rapportere daglig fra boreaktiviteten til Ptil. Rapporten gir en oversikt over fremdriften i boreoperasjoner og viser blant annet tidsforbruk for enkeltoperasjoner med egne koder for hver fase.

Rapporten har en egen seksjon for rapportering av uønskede hendelser. Et eksempel på slik rapportering av en hendelse i daglig borerapport til Ptil er vist nedenfor (viser kun tekst). Borerapporten refererer direkte til eventuelle hendelser registrert i 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 controlleddisconnect 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 theROV panel. Operation of the ROV valve 'ADS reset isolation' did not give any indication of pressure on subsea gauge 'ADS resetpressure'. 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

Figur 10 Eksempel på utdrag fra daglig borerapport.

En ny standard ble tatt i bruk i 2008 basert på et samarbeid mellom norske og utenlandske oljeselskap. Formatet er XML-basert og bygger på WITSML. Tre alternativer er tilgjengelige for overføring av XML-filen fra operatøren til Ptil: 1) Webskjema for manuell opplasting av XML, 2) Webtjeneste for automatisert overføringsprosess og 3) EPIM Reporting Hub (ERH). Alle alternativene vil sørge for sikker datakommunikasjon.

Daglige borevæskerapporter (Daily Mud Report)

Borevæskeselskapet skriver en daglig borevæskerapport (mudrapport). Rapporten fokuserer på væsker brukt i boreoperasjonen og tilsetningsstoffer, både egenskaper og logistikken knyttet til håndteringen av dette. Denne kan i enkelte tilfeller komplettere informasjonen gitt i daglig borerapport. Etter hvert som også væske- og kjemikaliehåndtering automatiseres, kan denne bli mer relevant for rapportering av avvik, tilløp til hendelser og hendelser.

4.3.1.2 Vedlikeholdssystem

Informasjons- og styringssystem for vedlikehold (Computerized Maintenance Management System – CMMS)

Operatørselskaper rapporterer, klassifiserer og dokumenterer tilstand og feil på utstyr som oppdages under drift, testing og vedlikehold, i et databasert informasjons- og styringssystem. Typisk eksempel på norsk sokkel er SAP vedlikeholdssystem. Hver observasjon lagres typisk som en notifikasjon knyttet opp mot et utstyrs-tag som er en unik fysisk identifikasjons-tag montert på utstyret.

Tilstandsovervåkningssystem

Systemer for tilstandsovervåkning samler inn kontinuerlig data om tilstand på utstyr så som vibrasjon og temperatur. Disse data gir alarmer ved degradert tilstand av utstyr og underlag for beslutninger om nødvendig vedlikehold av utstyr. Rigsentry er et eksempel på et slikt tilstandsovervåkningsystem.

Drilling recorders

Noen leverandører tilbyr løsninger som logger alle tidsseriedata, kommandoer, operasjoner, skjermbilder og alarmer under boreoperasjonen. Alle operasjoner nummereres da med et tag. Vet å logge alt fra operatørinput til operasjonelle karakteristikker, kan hele boreprosessen lagres og gjenskapes i etterkant. Enkelte systemer har også mulighet for å merke spesifikke av tidsstempel underveis i prosessen (ved å trykke på en knapp), slik at det er enkelt å finne tilbake til rett informasjon i ettertid. Når denne knappen trykkes, får man også mulighet til å legge inn en kort beskrivelse av problemet ved gitte tidspunkt. Det er verdt å merke seg at det ikke fins noe systematisk oppfølging av hendelser som registreres i Drilling recorder. Det vil sendes en epost til ansvarlig personell hver gang knappen trykkes, men det er ingen formelle krav til oppfølging av denne.

Data fra drilling recorder brukes aktivt i granskninger samt mindre forbedringer og optimalisering. Et eksempel som ble tatt fram i intervju, var en situasjon med en mud bucket som ikke oppførte seg som forventet, og da kunne det avdekkes ved hjelp av drilling recorder at det i dette tilfellet var en funksjon som var aktivert som ikke skulle vært det. Det ble påpekt at systemet ikke brukes for å fordele skyld, men for aktiv forbedring og optimalisering, samt årsaksanalyse.

Operasjoner som tripping og boring logges kontinuerlig, vanligvis av flere leverandører, og en følger med på om det skjer endringer i operasjonen. Dette brukes også for optimalisering, men det et overordnet inntrykk at er det fins ytterligere potensiale for å utnytte dette datamaterialet på en mer systematisk måte.

Oppdateringsforespørsel

Leverandører av automatiserte boresystemer gjør kontinuerlig oppdateringer og forbedringer av sine systemer. Behov for oppgradering og feilretting rapporteres inn via ulike systemer hos de ulike selskapene. Vurdering av kritikalitet og prioritering av oppgaver gjøres fortløpende av leverandøren (eventuelt i samråd med operatørselskap eller andre). Leverandørene har et register for revisjonskontroll av program- og fastvare, men det er varierende praksis for risikovurdering av selve programvaren før den endres/oppdateres.

Intervensjonsstatistikk

Noen leverandører informerte om at de fører såkalte intervensjonsstatistikker. Her logges tilfeller hvor et automatisert system har grepet inn eller utført en aksjon som har forhindret en hendelse eller avvikssituasjon. Disse intervensjonene meldes daglig inn til det ansvarlige operatørselskapet. En av leverandørene opplyste om at de hadde opp mot 300 registrerte intervensjoner i perioden januar til april 2021.

4.3.2 Hvem rapporterer hendelser og avvik

Ifølge informantene anses det å være et kollektivt ansvar å rapportere hendelser og avvik i selskapenes interne rapporteringssystem, det vil si at det forventes at ansatte både hos operatørselskap, leverandører og serviceselskap rapporterer hendelser fortløpende i sine respektive rapporteringssystem. Enkelte ganger rapporteres samme hendelse i mer enn ett system. Da refererer hendelsene noen ganger til hverandre, men det kan oppstå duplikater og mulige misforståelser. Det er en forventning om at operatørselskapet skal sitte med totaloversikten og håndtere videre rapporteringsplikt til Ptil.

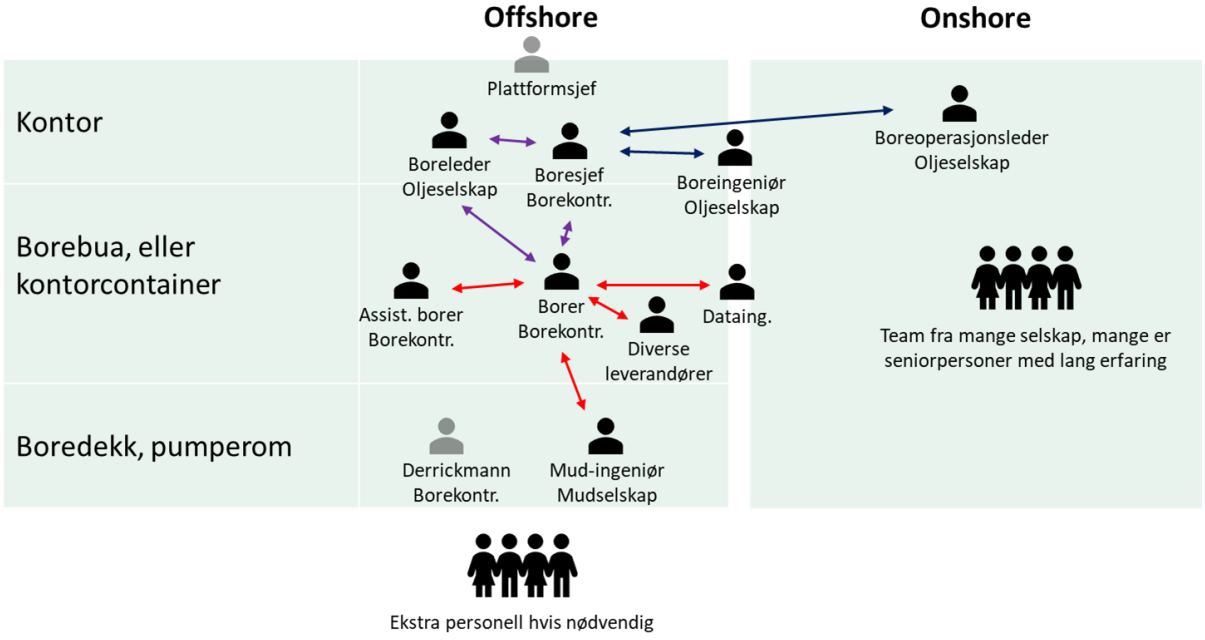
Operatørselskap og underleverandører er på lag når det gjelder å ha lav terskel for å si fra. Noen av informantene mente at hvis det blir rapportert ting som like gjerne kunne vært forbigått, så er det et godt tegn som vitner om en god kultur for varsling. Det legges generelt stor vekt på opplæring i de ulike rapporteringssystemene, og noen selskap har også kampanjer hvor beste innspill til forbedring premieres.

Det er viktig å merke seg at for teknologisk komplekse systemer kan de aktørene som forstår kritikalitet og omfang av et avvik best, være andre enn de som faktisk operer systemene. I slike tilfeller kan det tenkes at ting som burde vært rapportert ikke fanges opp på grunn av manglende forståelse eller kompetanse. I det følgende presenteres to eksempelscenario for håndtering av hendelse og tilløp til hendelse i boring. Ulike roller i håndtering av hendelsen og rapporteringen er også belyst gjennom disse eksemplene. Disse eksemplene er ikke basert på intervju, men på tidligere erfaringer, og er laget for å illustrere hvordan kommunikasjon *kan* foregå mellom ulike aktører.

4.3.3 Eksempelscenarioer

Eksempelscenario 1 (Figur 11):

1. Dataingeniør ser en uventet økning i aktivt volum
2. Dataingeniør snakker med borer på radio
3. Borer ringer til mud-ingeniør for å høre om de har sett noe på retur eller i pumperom og/eller andre
4. Borer ringer til boreleder og sier fra
5. Boreleder ser på endringen, diskuterer kanskje med boresjef eller boreingeniør
6. Avhengig av konklusjon:
    A. Temperatur-effekt: Fortsett operasjonen. *Rapporteres ikke.*
    B. Feil i sensor som vurderes ikke kritisk, operasjonen fortsetter. *Rapporteres i DBR/DDRS?*
    C. Mulig innstrømning fra formasjonen. Stopp operasjonen, steng inn brønnen og overvåk trykket. Involvering av folk på land. *Dette blir med i daglig borerapport. Kanskje Synergi.*

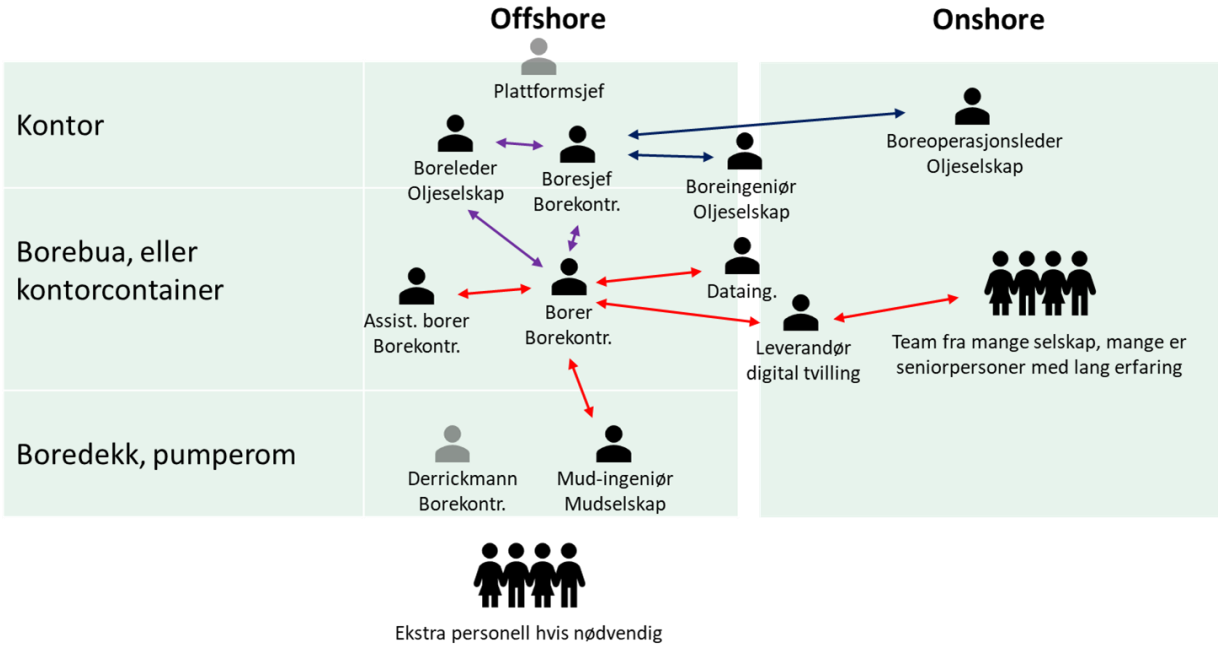


Figur 11 Eksempelscenario 1 for håndtering av hendelse og tilløp til hendelse i boring.

Eksempelscenario 2 (Figur 12):

1. Dataingeniør ser en uventet økning i *differansen* mellom målt aktivt volum og beregnet aktivt volum i den digitale tvillingen
2. Dataingeniør snakker med borer på radio
3. Borer ringer til mud-ingeniør for å høre om de har sett noe på retur eller i pumperom og/eller andre
4. Borer ringer til boreleder og formidler den informasjonen han har

5. Hvis det bare er liten eller ingen økning i *målt* aktivt volum slik at avviket skyldes reduksjon i *beregnet* aktivt volum, vil leverandøren av den digitale tvillingen involveres og bes om å vurdere situasjonen. En mulighet er at avviket skyldes unøyaktig modell eller inputdata til modellen. Hvis dette kan utelukkes, og hvis også sensorfeil kan elimineres, kan det se ut som en situasjon der økning i aktivt volum maskeres av en annen fysisk effekt, f.eks. en temperatureffekt. Dvs. at situasjonen kan være alvorlig selv om sensorene alene ikke viste noen tegn av betydning.
6. Boreleder vurderer informasjonen og diskuterer kanskje med boresjef eller boreingeniør
7. Avhengig av konklusjon:
    A. Det er overveiende sannsynlig at unøyaktighet i modell eller inputdata er årsaken til avviket: Fortsett operasjonen og overvåk nøye videre. *Rapporteres trolig ikke.*
    B. Feil i sensor som vurderes som ikke kritisk: Operasjonen fortsetter. *Rapporteres i DBR/DDRS?*
    C. Mulig innstrømning fra formasjonen. Stopp operasjonen, steng inn brønnen og overvåk trykket. Involvering av folk på land. *Dette blir med i daglig borerapport.*



Figur 12 Eksempelscenario 2 for håndtering av hendelse og tilløp til hendelse i boring.

4.3.4 Transaksjonsfeil

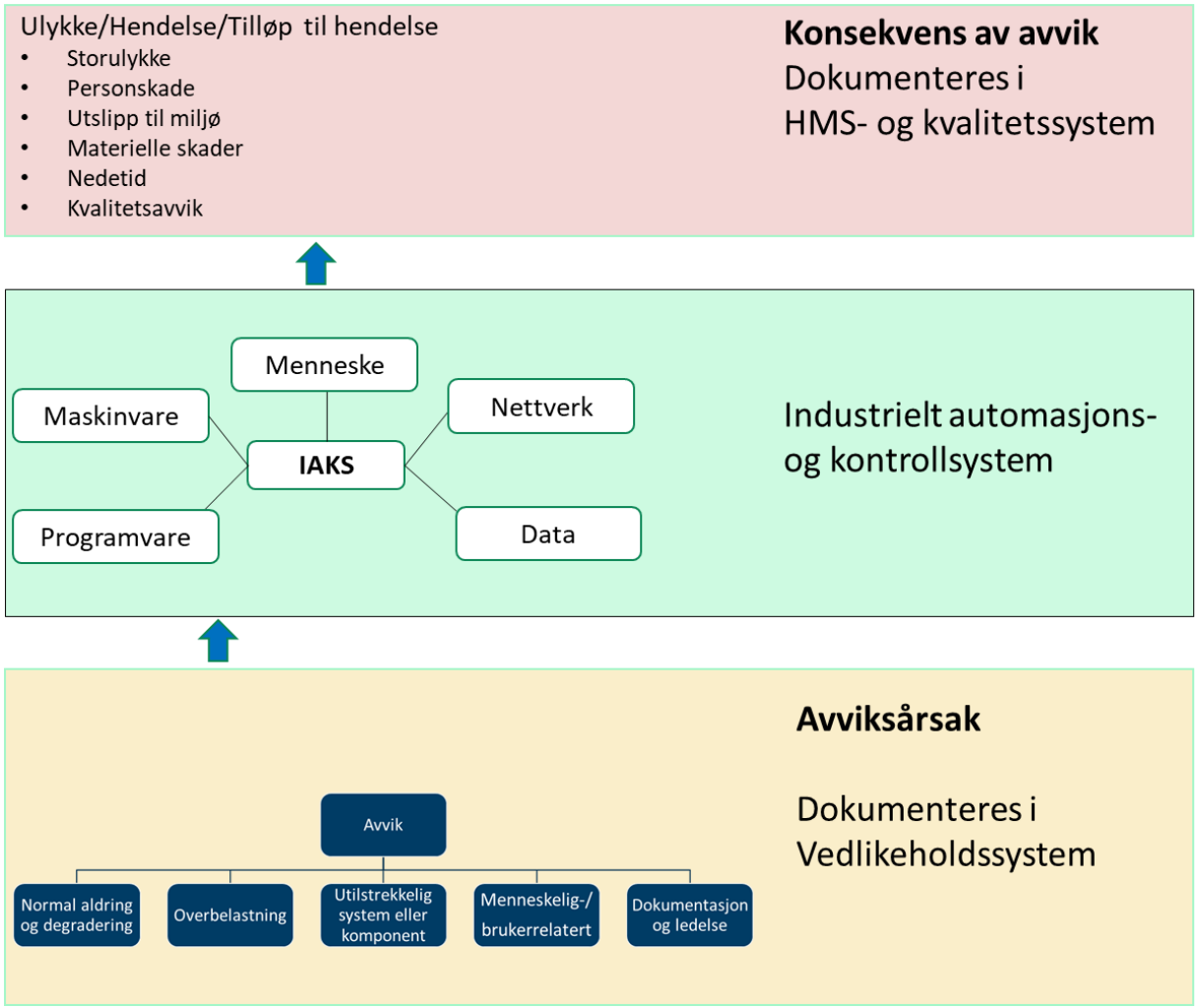
Som eksempelscenarioene viser, kan det være mange ledd og kommunikasjonskanaler involvert i overføring av informasjon. Dette gir samtidig mange muligheter for at det kan oppstå ulike sviktmoduser. I intervjuene ble det for eksempel gitt eksempler på at hendelser/avvik varsles via epost eller andre kanaler hvor det ikke bekreftes at meldingen er mottatt. I Tabell 6, som er basert på Salmon, Waler og Stanton [33], gis det eksempler på transaksjonsfeil i forbindelse med overføring av informasjon, og eksemplet med epost vil tilhøre kategorien "Fraværende transaksjon". Det vil også være en mulighet at informasjon som ble overført var feil (for eksempel ved manuell inntasting av verdier). Et annet eksempel er Pkt. 4 i Eksempelscenario 2: "Borer ringer til boreleder og formidler den informasjonen han har". Dette vil fungere så lenge boreleder har all informasjon tilgjengelig og samtidig formidler dette, men ikke hvis transaksjonen er ufullstendig. På samme måte kan mottaker på sin side tolke informasjonen på feil måte (misforstått transaksjon).

Tabell 7 Eksempler på transaksjonsfeil [33]

Type feil	Forklaring
Fraværende transaksjon	Det var behov for overføring av informasjon mellom aktørene, men dette skjedde ikke. Inkluderer tilfeller der slik overføring ikke er en del av normal operasjon (beskrevne prosedyrer, hjelpemidler i bruk, organisasjon og ledelse).
Feil transaksjon	Overføring av informasjon blir iverksatt, men informasjonen er feil. Inkluderer både feil faktainformasjon og feil individuell situasjonsforståelse foretatt av avsender.
Ufullstendig transaksjon	Ikke all informasjon mottaker hadde behov for blir overført.
Misforstått transaksjon	Riktig informasjon og individuell situasjonsforståelse blir overført, men mottakeren misforstår.

4.3.5 Funn relatert til hvordan hendelser og avvik rapporteres

Basert på intervju og tidligere studier fra prosessindustri angående håndtering av hendelser og avvik, kan man se at avvik på system- eller komponentnivå gjerne knyttes til en avviksårsak som normal degradering, overbelastning, brukerfeil, designfeil osv. og disse registreres i vedlikeholdssystemet for oppfølging og feilretting. Ulykker, hendelser og tilløp til hendelser knyttes i større grad mot konsekvens av avvik, som for eksempel personskade, materiell skade etc., og disse registreres i HMS og kvalitetssystemet.



Figur 13 Avviksårsak registrert i vedlikeholdssystem versus konsekvens av avvik registrert i HMS- og kvalitetssystem.

I tabellen under er funn fra intervju og workshop relatert til hvordan hendelser og avvik rapporteres oppsummert.

Tabell 8 Innspill fra næringen relatert til hvordan hendelser og avvik rapporteres

	Input fra intervju/workshop	SINTEF kommentar
1.	Personer som ringer og melder fra om avvik vil kunne få frem flere nyanser enn automatisert rapportering. Fortsatt person som har størst troverdighet.	• Betyr dette at rapporteringen ikke er detaljert eller god nok? • Hva betyr dette for mulighetene for automatisert rapportering?
2.	Brukervennlighet ved rapportering er viktig. Hvorfor må man ha opplæring? F.eks. mobilbank og vipps er verktøy som er lett å bruke uten opplæring. Bedre brukervennlighet vil kunne bidra til mer treffsikker rapportering) og gi mindre rom for feiltolking.	Hvorfor må vi ha opplæring? • Trenger vi bedre opplæring eller bare bedre systemer? • Har vi designet systemene feil eller er det motivasjon og eierskap som mangler? • Chatbot kan kanskje være nyttig?
3.	Savner bedre tilbakemelding (feedback-sløyfe) for de som rapporterer. Spesielt nevnt av leverandører.	Se punkt 4.
4.	Mange ulike rapporteringssystem både internt i selskap og for ulike aktører. Det brukes mye tid på å registrere samme hendelse i flere ulike system. Bør gjøre dette på en smartere måte, f.eks. felles eller standardisert system både for rapportering og opplæring. Vil også legge til rette for erfaringsdeling og læring. Initiativ må komme fra operatør.	Hva vil være begrensningene for å få gjennomført et slikt prosjekt?
5.	Noen hendelser/avvik varsles via epost eller andre kanaler hvor det ikke bekreftes at meldingen er mottatt. Dette medfører risiko for at beskjeder ikke kommer frem eller at de kommer frem for sent. Eksempelvis kan man oppleve at epost filtreres ut som søppelpost.	• Kan et standardisert rapporteringssystem være nyttig også her? • Kan i tillegg til "fravær av transaksjon", også være muligheter for andre transaksjonsfeil, ref. Tabell 6, spesielt når mange aktører er involvert?

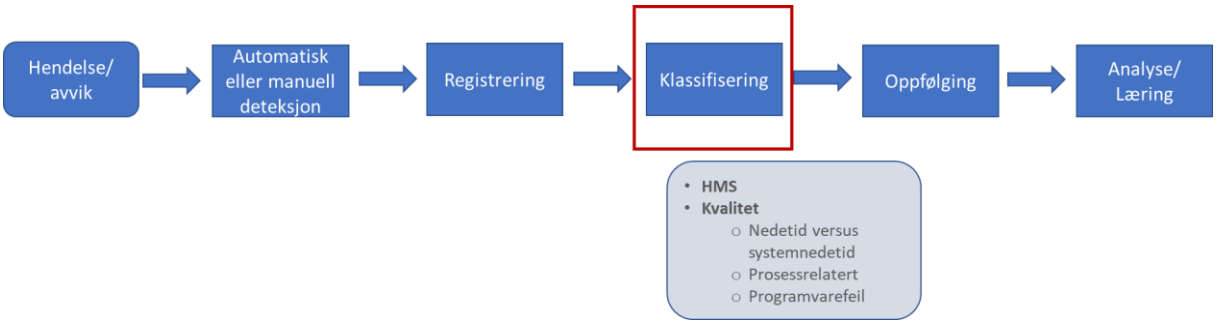
4.4 Hvordan klassifiseres hendelser og avvik?

Dette delkapitlet omhandler hvordan hendelser og avvik klassifiseres. Som påpekt i kapittel 2.4.7 er klassifisering av hendelser og avvik viktig både fordi det kan bidra til å si noe om alvorlighetsgraden av hendelsen og fordi det vil gjøre det enklere å sammenligne data om tilsvarende avvik eller hendelser.

I intervjuene ble det ikke nevnt spesifikke standarder for klassifisering av hendelser og det synes i hovedsak å være selskapsspesifikke praksiser. Det ble imidlertid nevnt noen ulike klassifiseringsmåter:

- HMS versus kvalitet
- Nedetid (knyttet mot utstyrsgruppe)
- Systemnedetid (laveste nivå), nedetid, sikkerhet
- For operasjonell hendelsesrapportering hadde ett av selskapene ulike kategorier for å klassifisere hendelser, eksempler på kategorier: Brønnkontrollhendelse, Prosedyrefeil, Forsinkelser grunnet kunde, Forsinkelser grunnet værforhold, Utstyrsfeil, Korrektivt vedlikehold etc.

Noen tekniske og organisatoriske ressurser som kan være relevant for klassifisering av hendelser er listet under figuren.



Tekniske ressurser som er relevant for klassifisering av hendelser kan, være f.eks.:

- Vedlikeholdssystem
- Tekniske hjelpemidler som nettbrett, arbeidsstasjoner etc.
- Drilling recorder

Organisatoriske og operasjonelle ressurser som er relevant for klassifisering av hendelser kan være f.eks.:

- Rammeverk/taksonomi for klassifisering
- Retningslinjer for klassifisering
- Systemer/algoritmer for automatisk feilklassifisering
- Personell
- Trenings-/motivasjonsprogram og kompetanse
- Det er vanlig at hver rigg har en onshore HMS&K rådgiver, her får man også en ekstra kontroll på klassifisering av hendelser

Et hovedinntrykk fra intervjuene er at det generelt er stort fokus på nedetid og hvilket utstyr og leverandør nedetiden kan knyttes til.

Et av operatørselskapene hadde en egen veileder i styringssystemet for klassifisering og behandling av IKT-hendelser, men dette var ukjent for de fleste leverandører. Når det gjelder klassifisering av vedlikeholdsfeil fortalte informantene at de benyttet internasjonale standarder, men ingen spesifikke standarder ble videre diskutert i intervjuene.

Det var få som mente det var et problem at det manglet en detaljert retningslinje for klassifisering, men flere syns det ville være en god idé med et felles, standardisert rammeverk. Flere så også at det kunne være et problem at klassifiseringen ofte vil bli personavhengig, og at det i så måte vil være vanskeligere å etablere konsistente og sammenlignbare data for læring. Spørsmålet er derfor om man kan komme noe bort fra personavhengighet i forhold til rapportering med klarere retningslinjer og enklere klassifiseringsmåter.

Noen av informantene hadde sett at kategoriene "annet" eller "ukjent" ofte ble brukt ved knytting av nedetid mot utstyrstype, men det ble ikke sett på som en stor utfordring i oppfølging av systemene. For oppfølging av sikkerhetskritisk utstyr for petroleumsvirksomheten ser man imidlertid at utstrakt bruk at disse kategoriene kan føre til at man må lete i for eksempel fritekstfelt for å kunne finne den relevante informasjonen man trenger. En intern studie nylig utført over en seks måneders periode for et norsk offshoreanlegg viste at for mer enn 50% av notifikasjonen ble feilmodusen klassifisert som enten "annet" eller "ukjent".

4.4.1 Definerte fare- og ulykkeshendelser

Det var generelt lite kunnskap blant intervjuobjektene om DFU-er og de fleste visste ikke hva det var. Imidlertid var det noen som hadde god oversikt over DFU-er for IT (hacking, malware, social engineering/phishing, misuse, error).

- Flere mente at DFU relatert til boring er tilstrekkelig
- Det er ingen DFU knyttet til automatisert rørhåndtering
- Det blir ansett som krevende prosess å definere nye DFU-er, fordi det vil komplisere analyser og standarder
- Cyber security er et område hvor det vurderes å innføre ny DFU.

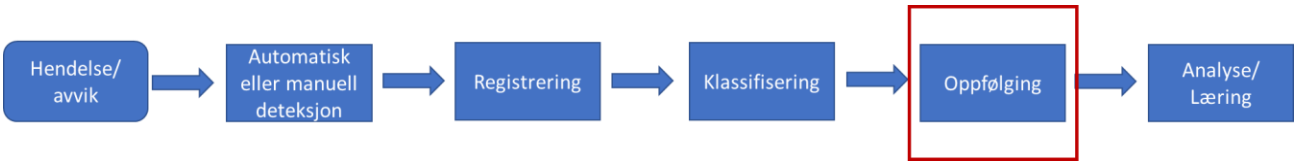
4.4.2 Funn relatert til hvordan hendelser og avvik klassifiseres

Tabell 9 Innspill fra næringen relatert til hvordan hendelser og avvik klassifiseres

	Input fra intervju/workshop	SINTEF kommentar
1.	Savner en rapportering som er mer systematisk og lettere å måle på. Tilbakemeldinger blir mange ganger så subjektive at det blir vanskelig å tolke. Eksempel på klassifisering av hendelser: service interrupt, non-productive time, sikkerhet (safety).	• Kan denne inndeling standardiseres? • Er disse eksemplene på inndeling for grove til å gi meningsfulle data og tilbakemeldinger?
2.	Ofte komplekse system, noen har måttet sette på flere personer for å sikre god nok totaloversikt. Krevende å forstå hvordan de fungerer og dermed rapportere riktig. Stort fokus på sparing kan føre til mangelfull kursing.	• Hvem er det som gjør slike vurderinger om utvidet bemanning, og fanges det opp i tilstrekkelig grad? • Manglende forståelse for/fokus på læring etter tilløp til hendelser?
3.	Motstridende interesser hos ulike aktører: Selv om det fortelles om et ønske og en intensjon om at operatørselskap, boreselskap, leverandører og serviceselskap skal fungere som et helhetlig team med felles interesser, blir det også nevnt at noe rapportering kan påvirkes av internt og/eller eksternt press for å forskyve ansvar og kostnad. Hvordan en hendelse kategoriseres kan f.eks. påvirke hvem som har ansvar for oppfølging og utbedring.	Fordeling av skyld kan gå på bekostning av sikkerhet. • Kan en mer entydig klassifisering og terskel for hva som skal rapporteres hjelpe? • Trenger bransjen en mer uavhengig vurdering av hendelser?

4.5 Hvordan følges hendelser og avvik opp?

Dette delkapitlet omhandler hvordan hendelser og avvik følges opp, ref. prosessflytdiagram under. Etter rapportering av hendelser tas det videre inn i selskapets styringssystem. Avhengig av type hendelse fylles det ut et første varsel til ledelse/disiplinansvarlige osv. Der vil det også angis om hendelsen skal granskes og på hvilket nivå. Inntrykket er at flere leverandører av avanserte delsystemer praktiserer detaljert logging og rapportering internt for feilsøking og forbedring. Samtidig antas det at ansvaret for overordnet og ekstern rapportering ligger hos andre selskaper. Rapportering av hendelser til Ptil er det operatørselskap som håndterer. Noen hendelser og feil rapporteres også videre til DNV (f.eks. tekniske effekter som omhandler klasser etc. og dette vil som regel føre til pålegg om utbedringsdato).



Tekniske ressurser som er relevant for oppfølging av hendelser kan, være f.eks.:

- Vedlikeholdssystem
- Drilling recorder

Organisatoriske og operasjonelle ressurser som er relevant for oppfølging av hendelser kan være f.eks.:

- Arbeidsprosesser for håndtering av hendelser og notifikasjoner
- Drift- og vedlikeholdsledere
- Arbeidsordre
- 24-timersmøte
- Drillers forum/kranforum/webinar
- Månedlige møter med sikkerhetsansvarlige
- Opplæring og kompetanse

Det er ikke samme grad av systematikk for håndtering av tilløp til hendelser. Et godt eksempel er "knappen" som borer har tilgjengelig under boreoperasjon (ved bruk av drilling recorder), hvor borer enkelt kan registrere at noe unormalt skjer på et gitt tidspunkt. Her er det ikke mulig å registrere hva som skjedde, men bare at noe har skjedd. Det er heller ingen krav til oppfølging av en slik registrering selv om den i de fleste tilfeller vil bli behandlet i etterkant av boreoperasjonen.

RACI (Responsible, Accountable, Consult, Inform) ble nevnt i noen av intervjuene som et verktøy for oppfølging av hendelser og avvik. RACI er typisk en matrise eller lineært ansvarsdiagram som beskriver deltakelsen av ulike roller i å følge opp oppgaver eller leveranser for et prosjekt eller en forretningsprosess.

4.5.1 Funn relatert til hvordan hendelser og avvik følges opp

Tabell 10 Innspill fra næringen relatert til hvordan hendelser og avvik følges opp

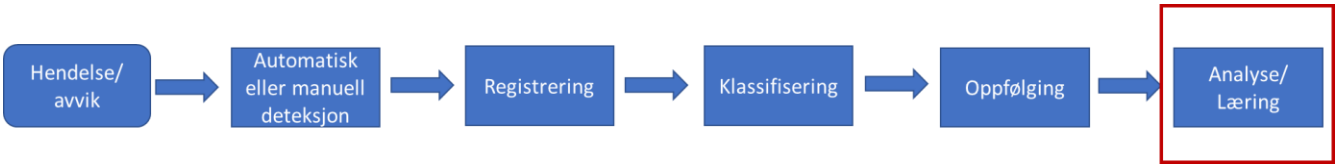
	Input fra intervju/workshop	SINTEF kommentar
1.	Leverandør får av og til informasjon om at en hendelse eller et tilløp til hendelses har skjedd, uten at de blir involvert i rotårsaksanalyse.	Komplisert aktørbilde: • Hvordan klare å skape en felles informasjonsdelings- og læringsarena?
2.	Uklar ansvarsfordeling for å respondere og aksjonere på en hendelse, som i verste fall fører til at hendelsen ikke følges opp. Man må rapportere til den som kan gjøre noe med saken (eller lære noe av rapporteringen).	• Hvordan kan ansvarsområdene kommuniseres på en enkel måte for å sørge for at rett informasjon havner på riktig sted? • Mer aktiv og standardisert bruk av RACI (Responsible, Accountable, Consult, Inform)?
3.	Noen selskaper har en egen Cyber/IT-sikringskontakt som kan kontaktes ved IKT-hendelser.	Dette gjelder kun et fåtall av selskapene. • Burde det være et krav? • Vet aktører om denne kontaktpersonen?
4.	Samspill menneske-maskin viktigere enn å følge opp på utstyrsnivå.	Kanskje stemmer dette bare for dagens situasjon? • Vil menneske-maskin grensesnitt bli viktigere ved økt bruk av

	Input fra intervju/workshop	SINTEF kommentar
		automatiserte systemer (sikre god forståelse for inngrep av personell ved avvik i automatiske systemer)? • Vil det bli viktigere å følge opp tekniske feil ved økt bruk av automatiserte systemer?

4.6 Hvordan analyseres hendelser og avvik?

Dette delkapitlet omhandler hvordan hendelser og avvik analyseres og deles. De fleste selskapene synes å ha gode løsninger for informasjonsdeling, spesielt internt i selskapene. For deling av informasjon etter hendelser sier flere informanter at "experience transfer"-systemet brukes. Dette brukes både internt og eksternt, avhengig av type hendelse og relevans for de ulike aktørene. Det kan deles både bilder og tekst, gjerne i form av nyhetsbrev. Boreselskapene arrangerer dessuten "drillers forum" hvor typiske hendelser på boredekk presenteres for å dele kompetanse på tvers av rigger. Det fins også egne kranforum for deling av kompetanse knyttet til kranhåndtering. I tillegg til deling av hendelser er det aktiv deling av både tekniske og operasjonelle forbedringer som gjøres i hvert selskap. Dette vil ofte kunngjøres via en "bulletin" eller i mer kritiske tilfeller som en "safety alert".

En oppsummering av tekniske, organisatoriske og operasjonelle ressurser som er relevant for informasjonsdeling og læring er listet under figuren.



Tekniske ressurser som er relevant for informasjonsdeling og læring av hendelser kan, være f.eks.:

- Vedlikeholdssystem
- Hendelsesdatabaser
- Safety bulletins/newsletters/experience transfer system
- Maskinlæring

Organisatoriske og operasjonelle ressurser som er relevant for informasjonsdeling og læring av hendelser kan være f.eks.:

- Gjennomgang av hendelsesdata
- Dataprosesseringspersonell
- Rammeverk og taksonomier for oppfølging
- Opplæring og kompetanse
- 24-7 møter
- Ukentlige/månedlige møter mellom rigger/leverandører etc.

Det er flere forhold som påvirker og kan hindre deling av både tekniske, operasjonelle og hendelsesdata. Det ene er kontraktsforhold. Noen kontrakter tilrettelegger for mer åpenhet, mens andre krever at kortene holdes tettere mot brystet. Ifølge informantene er deling ofte enklere når oljeselskapet har direkteavtaler med de involverte aktørene, mens det er vanskeligere hvis brønnen leveres av en én totalansvarlig (med totalansvarlig menes at ett selskap har totalansvar for brønnen overfor operatørselskapet, slik at underleverandører har kontrakt med dette selskapet i stedet for å ha kontrakt direkte med

operatørselskapet). Kommersielle forhold spiller også inn. For eksempel kan det være vanskelig å dele tekniske data dersom disse er relatert til nyvinninger som forventes å gi kommersielle fordeler for en leverandør. Dette varierer likevel mellom selskap, noen vil gjerne ha mange innspill og større åpenhet, mens andre ikke ønsker det. Kulturforskjeller ble også nevnt som en viktig faktor som påvirker åpenhet. En generell oppfatning er at det er stor villighet til deling blant aktørene på norsk sokkel, mens det kan være noe vanskeligere internasjonalt. Grad av automatisering påvirker også deling av teknisk informasjon. Ikke alle innretninger har utstyr som er relevant for deling av hendelsesdata knyttet til automatiserte system, og da blir det heller ikke like naturlig å dele. Til slutt kan et sterkt ønske om å komme videre i operasjonen komme i konflikt med oppfølging av tilløp til hendelser. Det er derfor viktig at operasjonen ikke forsinkes unødvendig av slik oppfølging, også fordi en forsinkelse av operasjonen kan gi økt risiko for hendelser. Det bør heller tilrettelegges for en parallell håndtering av tilløp med tanke på senere forbedringer og læring.

Til tross for at det er flere arenaer for deling av informasjon, er det ikke gitt at det vil føre til forbedringer eller læring. Dette er kort omhandlet i kapittel 5.

4.6.1 Funn relatert til hvordan hendelser og avvik analyseres og deles

Tabell 11 Innspill fra næringen relatert til hvordan hendelser og avvik analyseres og deles.

	Input fra intervju/workshop	SINTEF kommentar
1.	Utfordrende å spre erfaring effektivt på grunn av mange involverte aktører.	Kan en tydeligere og mer detaljert klassifisering av hendelser i forhold til aktørbildet gi mer målrettet informasjonsdeling?
2.	Noen leverandører får tilbakemelding ved problemer, men savner av og til tilbakemeldinger om normal drift. For eksempel skulle noen leverandører gjerne hatt innsyn i daglig borerapport og mudrapport (og helst digital deling av parametere). Større åpenhet og deling av viktig konfigurasjonsinformasjon kunne hindret en del trøbbel. Åpenhet om og deling av ting som normalt rapporteres internt i hvert selskap vil bidra til økt læring.	Mer avanserte verktøy/systemer kombinert med samarbeid mellom flere forskjellige aktører gjør at åpenhet/gjennomsiktighet blir stadig viktigere. Kanskje trengs det et samlet initiativ fra de store aktørene slik at informasjon kan deles tvers av selskap, både om hendelser, tilløp til hendelser og intervensjoner og deling av teknisk informasjon?
3.	Økt involvering av sluttbruker gjør det lettere å utnytte læringspotensialet og forbedre systemene. Dette forutsetter fleksibilitet hos leverandør og at operatør og boreselskap legger til rette for slike initiativer.	• Hvordan involvere sluttbrukere i leverandørenes forbedringsprosesser? • Hvordan involvere leverandørene i forbedring av sluttbrukernes kompetanse?
4.	Automatisering bidrar til kortere forbedringssløyfe (slipper å fikse feil ved å "oppdatere" alle brukere, trenger bare oppdatere systemet).	Likevel viktig å ha brukergrensesnitt som sørger for at operatørene har tilstrekkelig innsikt i og forståelse for prosessen?

4.7 Andre tilbakemeldinger fra næringen

I det følgende er det oppsummert funn fra intervju og workshop som ikke er direkte relevant for oppdraget, men som likevel kan være av interesse i forbindelse med tilløp til hendelser og hendelser i automatiserte systemer.

Tabell 12 Andre innspill fra næringen.

	Input fra intervju/workshop	SINTEF kommentar
1.	Krevende for personell å forholde seg til flere og flere funksjoner som gir beslutningsstøtte, for eksempel anbefaling om å kjøre tre ganger fortere.	• Hvem tar denne beslutningen og hvem har ansvaret? • Kan det påvirke andre systemer? • Hvordan vurdere (kvantifisere) redusert/økt risiko i slike sammenhenger?
2.	Viktig å ha gode brukergrensesnitt. God presentasjon (HMI) er avgjørende for å sikre at operatør ikke misforstår situasjonen og gjør beslutninger på feil grunnlag.	• Hvordan sikre tilstrekkelig brukerinvolvering?
3.	Forebyggende vedlikehold og overvåkningsfunksjoner fungerer stort sett godt på norsk sokkel og bidrar til færre hendelser. En ser likevel at oppetid ofte får høyere prioritet enn vedlikehold (sett fra et leverandørs ståsted). Spesielt når investeringsviljen er lav, oppstår etter hvert problemer knyttet til gammelt eller dårlig vedlikeholdt utstyr.	Kan man få til en god balanse mellom å løse utfordringer på kort sikt kontra en helehetstankegang på lengre sikt.
4.	Det handler mye om eierskap og vilje til å ta i bruk nye ting. Nye løsninger vil kanskje være bedre tilpasset kompetansen hos den nye generasjon som skal ta disse i bruk.	Hvordan kan vi sikre eierskap i alle ledd?
5.	Mangler krav til opplæring i det automatiserte systemene. Kan føre til en degradert situasjonsforståelse.	En standardisering av opplæring kan bidra til bedre systemforståelse blant borere og annet teknisk personell?
6.	Tar i bruk nye system gang på gang og det gir mye rapportering fordi systemene ikke er gjennomtestet på forhånd og dette kunne vært bedre – bransjeproblem er at kvaliteten på det som blir tatt i bruk ikke er god nok.	• Er det et godt nok system for krav til testing på forhånd? • Eller er hovedutfordringen at det er vanskelig å forutse situasjoner man må teste for?
7.	Det er få formelle krav til borer utover brønnsertifikat. Næringen ser at det er behov for mer opplæring og trening i bruk av automatiserte systemer, kanskje også leverandørspesifikke systemer, da det oppleves at ulike system som utfører tilsvarende funksjon har svært ulike brukergrensesnitt?	• Revurdere formelle krav til kompetanse for borer utover brønnsertifikat.

4.8 Hvilke rapporteringssystemer brukes i andre bransjer enn boring

Som del av studien er det gjennomført en overordnet kartlegging av systemer for rapportering av hendelser i automatiserte systemer i følgende bransjer:

- Luftfart
- Vegtransport
- Maritim skipsfart
- Jernbane
- Kraftforsyning

Kartleggingen som er gjennomført av SINTEF-forskere med spesiell kompetanse innenfor de enkelte bransjene, er dokumentert i Vedlegg A-F.

Tabell 13 gir en samlet oversikt og oppsummering av resultatene fra denne kartleggingen.

Tabell 13 Rapportering av hendelser i andre sektorer.

Sektor	Hvordan detekteres?	Hvordan rapporteres?	Hva rapporteres/ hvordan klassifiseres (kritikalitet)?	Hvordan følges opp?
Luftfart	Flyets Flight Data Monitoring (FDM) system registrerer operasjonelle data under flygning. Eksternt analyseselskap varsler avvik i operasjonell data til flyselskap etter hver flygning. I tillegg - manuell deteksjon fra piloter.	Hendelser rapporteres til myndigheter gjennom Altinn.	Operasjonelle FDM-data inndeles i tre nivåer.	"Småting" i FDM data følges opp med f.eks. automatisk epost til pilot. Ved alvorlige avvik vil representanter fra flyselskapet involveres i videre oppfølging av hendelser. Eksternt analyseselskap sender oppsummeringsrapporter til flyselskap i henhold til individuelle avtaler.
Vegtransport	Moderne biler registrerer operasjonelle data som sendes "Over the air" til fabrikant. Moderne biler varsler automatisk ulykker til nærmeste 110-sentral vha. eCall som er et felles europeisk nødmeldingssystem. Trafikant kan varsle vha en "SOS-knapp". I USA kan trafikanter bruke en "hotline" for rapportering av sikkerhetsproblem.	FOR-2005-06-30-793 [34]: "Forskrift om offentlige undersøkelser og om varsling av trafikkulykker mv." inneholder flere krav til dette. Ingen automatisk rapportering til myndigheter fra trafikant. Politiet og Statens vegvesen varsler og rapporterer til Statens Havarikommisjon om alvorlige trafikkulykker og/eller alvorlige trafikkuhell	Fabrikanter klassifiserer og rapporterer tekniske feil i sine vedlikeholdssystem.	Fabrikanter lagrer operasjonelle data som gjennomgås av fabrikantens analyseteam. Kun fabrikanter følger opp operasjonelle data og myndigheter har ikke tilgang.
Maritim skipsfart	Liten grad av automatisk deteksjon	Selskap varsler umiddelbart muntlig, og skriftlig innen 72 timer, om sjøulykker til Hovedredningssentral, Sjøfartsdirektorat og Kystverket ut fra type hendelse og alvorlighetsgrad. Tekniske feil rapporteres til myndigheter kun dersom dette er viktig ulykkesårsak.	Selskap klassifiserer og rapporterer tekniske feil i sine vedlikeholdssystem. Selskap klassifiserer og rapporterer ulykker og ulykkeshendelser i henhold til en rekke kjennetegn (f.eks. ulykkestype: Brann, Grunnstøting, Tap av fremdrift etc.).	Oppfølging av tekniske hendelser blir håndtert internt i selskapene. Ulykker går inn i offentlige statistikker. Klasseselskapene følger opp tekniske hendelser på fartøyer. I hendelser som leder til granskingsrapport, blir tekniske funn en del av rapporten.

Sektor	Hvordan detekteres?	Hvordan rapporteres?	Hva rapporteres/ hvordan klassifiseres (kritikalitet)?	Hvordan følges opp?
Jernbane	European Rail Traffic Management System (ERTMS) samler kontinuerlig data om signalering og togets hastighet. Krav til ombordsystem for kontinuerlig innsamling, lagring og bruk av audiovisuell informasjon (lyd- og videoopptak) fra førerhuset ved kjøring av tog (jfr. IEC 62625-1,-2 og 3) [35].	Manuell rapportering av hendelser hos jernbaneforetak og trafikksentraler. HMS&K hendelser og tilløp rapporteres i Synergi Forsinkelser/innstillinger rapporteres i Trafikk- og oppfølgingssystem (TIOS) Feil på infrastruktur rapporteres som AT-melding. Varslingskanal i Bane NOR for varsling av bl.a. kritikkverdige forhold som innebærer fare for liv og helse.	Synergi og TIOS bruker årsakskoder. Varslingskanal hos Bane NOR krever beskrivelse av forholdet, tidspunkt for hendelsen, kilde for mer informasjon, evt. annet nyttig.	Automatisk håndtering av avvik i ERTMS.
Kraftforsyning	Utstyr i OT-nettverkene gir automatisk liste over aktiva, programvareversjon etc. Feil- og avbruddsstatistikk i totalnettet registreres. Utplasserte inntrengnings-deteksjonssensorer (VDI) detekterer angrepsforsøk fra internett automatisk. Internt i kraftsystemer har man i varierende grad Inntrengings-deteksjonssystemer (IDS). Mange hendelser oppdages manuelt.	VDI-varsler sendes automatisk. Nettselskap melder om hendelser manuelt til KraftCERT	"Advanced Persistent Threat" (APT) skal rapporteres til NSM. Iht. Kraftberedskaps-forskriften skal enheter i Kraftforsyningens beredskapsorganisasjon (KBO) varsle [KraftCERT] om en rekke feil, herunder forsøk på innbrudd i driftskontrollsystemet og avbrudd på distribusjon. Strømbrudd klassifiseres på tid (etter to timer), men ingen klassifisering av datainnbrudd.	Oppfølging i VDI er ikke offentlig kjent.

Tabellen viser at flere bransjer har utviklet systemer og prosesser som gir automatisk rapportering og lagring av hendelser i kontrollsystemer.

Selv om dagens Industrielle automasjons- og kontrollsystemer i boreoperasjoner er i stand til å registrere og rapportere tidsstemplede prosessverdier, hendelsesdata og beregnede data i tillegg til system- og applikasjonsdata (ref. krav i NORSOK I-002:2021 [33], er det andre bransjer som er kommet lengre med automatisk rapportering og analyse av data.

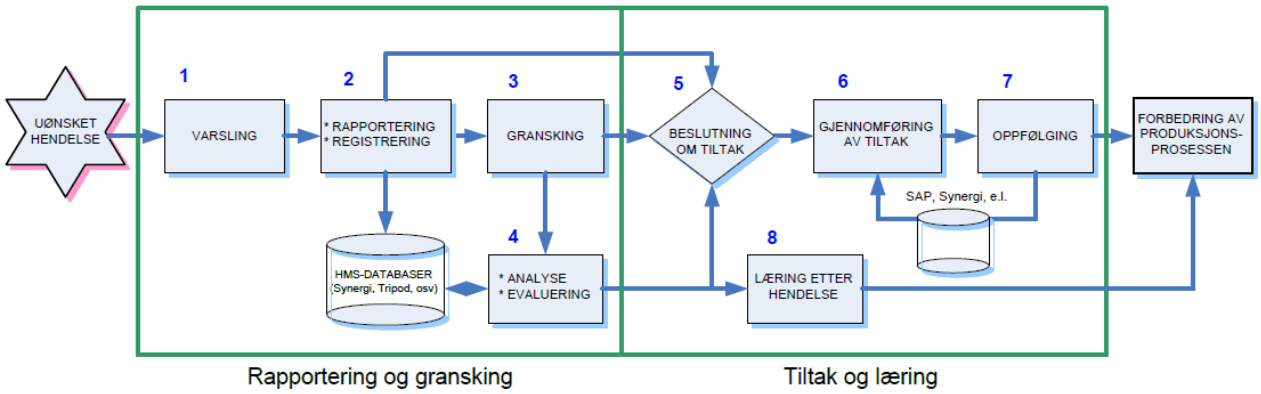
Noen læringspunker basert på gjennomgang av rapporteringssystemer på både produksjonsinnretninger og i andre bransjer enn petroleum, er:

- Bruk av mer detaljerte og standardiserte taksonomier for hendelser som muliggjør automatisk rapportering og klassifisering av avvik (ref. PDS forum/APOS, kapittel 2.4.7). Felles utstyrskategorier og taksonomier, inklusive deteksjonsmetode og feilmodi, er spesielt viktig for læring på tvers av selskaper.
- Tilrettelegge for automatisk oppfølging og håndtering av avvik (ref. jernbane, vedlegg D)
- Gi leverandører økt tilgang til operasjonelle data for gjennomgang av leverandørers analyseteam (ref. vegtransport, vedlegg B).
- Gi eksternt analyseselskap tilgang til operasjonelle data (ref. luftfart, vedlegg A). Analyseselskap vil kunne varsle avvik og følge opp med f.eks. automatisk epost til involvert personell, samt utarbeide oppsummeringsrapporter til fastsatte intervall.
- Ta i bruk system for kontinuerlig innsamling, lagring og bruk av audiovisuell informasjon (ref. jernbane, vedlegg D). Lyd- og videoopptak vil være nyttig for årsaksanalyse av inntrufne hendelser.

5 Hvordan etablere og systematisere forståelse av uønskede hendelser og omsette det til læring og forbedring?

Et av målene med denne rapporten har vært å foreslå hvordan man kan etablere og systematisere rapportering av IKT-hendelser og tilløp til hendelser i petroleumsvirksomheten. I dette kapitlet omhandles andre forslag til hvordan man kan jobbe for å etablere og systematisere forståelse av uønskede hendelser og omsette det til læring og forbedring.

Figur 14 viser ulike aktiviteter som inngår i en læringsprosess etter uønskede hendelser, fra rapportering og gransking, til videre oppfølging og læring i de involverte virksomhetene. For automatiserte systemer i boring kan det, basert på resultater i denne forstudien, tyde på at det er potensial for forbedring både med hensyn til rapportering/gransking av hendelser og tiltak/læring.



Figur 14 Flytskjema for hendelsesoppfølging [36].

På rapporteringssiden er mye data tilgjengelig, men det mangler i en del tilfeller systematikk og retningslinjer for hvilke data som bør logges, hva terskelen og kriteriene for rapportering skal være, hvordan og hvor rapporteringen skal gjøres. Dette gjelder spesielt for avvik og tilløp til hendelser, men i noe grad også for hendelser. I kapittel 2.4.7 ble for en retningslinje [30] for standardisert rapportering av klassifisering av feil i instrumenterte sikkerhetssystemer i petroleumsvirksomheten beskrevet, og det synes å være behov for en lignende retningslinje for automatiserte systemer i boring. Her kan det dessuten tas utgangpunkt i Tabell 3 for å etablere en forståelse for hvilke data som kan eller bør logges for å tilrettelegge for best mulig deteksjon og læring. Det er et ønske fra næringen at rapporteringen i større grad skjer automatisk. Retningslinjen [30] nevnt over inkluderer også forslag til hvordan man kan oppnå mer automatisert rapportering. I tillegg kan man ta i bruk erfaring med bruk av drilling recorder for å vurdere hvordan data fra dette systemet kan utnyttes og følges opp på en enda mer systematisk måte enn det gjøres i dag (ref. krav i revidert NORSOK I-002) [29]. Her er det også mulighet for å hente innspill fra for eksempel luftfart og erfaring med bruk av Flight Data Monitoring (Vedlegg A.1).

For å få til et standardisert rapporteringssystem er det mange brikker som må på plass, og da spesielt at aktørene selv tar eierskap til etablering og bruk av systemet. Det er viktig at systemet er enkelt å bruke, men dette kan være en utfordring dersom ett system skal fange opp alle typer avvik, tilløp til hendelser og hendelser for alle involverte aktører. Innen luftfart har NASA utviklet et frivillig rapporteringssystem som personell blant ulike aktører kan anvende og her kan man få en indikasjon på hvordan rapportering på tvers av aktører fungerer, se Vedlegg A.3.

For å muliggjøre utvikling av både en standardisert retningslinje for rapportering for automatiserte systemer i boring samt tilrettelegge for erfaringsdeling på tvers av aktører, kan det vurderes etablering av et felles

interesseorgan for aktører innen boring og brønn. PDS forum, som er omtalt i kapittel 2.4.7 er et eksempel på et slikt samarbeid. Hovedmålet med PDS Forum er å opprettholde en profesjonell møteplass for erfaringsutveksling mellom leverandører og brukere av kontroll- og sikkerhetssystemer. Dette har resultert i en rekke samarbeids- og forbedringsprosjekter opp gjennom årene, blant annet det pågående APOS-prosjektet (se kapittel 2.4.7).

"Læring betyr at noe endres, for eksempel at en arbeidsoppgave gjennomføres på en annen måte enn tidligere."

Sikkerhetsforum, 2019 [37]

En sentral utfordring i arbeidet med læring etter hendelser og tilløp til hendelser er overgangen mellom rapportering og gransking på den ene siden, og tiltak og læring på den andre.

"Læring betyr at noe endres, for eksempel at en arbeidsoppgave gjennomføres på en annen måte enn tidligere. Deling av informasjon og andre former for erfaringsoverføring er viktige skritt på veien mot læring, men er ikke læring i seg selv. Det er først når noe endres at en har lært" [37].

I kapittel 4.6 ble det presentert funn knyttet til hvordan hendelser og avvik analyseres. De fleste funnene omhandlet arenaer for erfaringsdeling, mens det i mindre grad ble fokusert på forbedring og læring. Læring kan skje på ulike nivåer. For eksempel handler avvikshåndtering om å oppdage, melde, rette opp og forbygge avvik og hendelser, mens læring på et mer overordnet nivå kan handle om:

- Hvorvidt man har det riktige utstyret.
- Hvorvidt samhandlingen mellom aktører på land og offshore er god nok.
- Hvorvidt man har riktig opplæring/kompetanse.

6 Anbefalinger

I dette kapitlet oppsummeres SINTEFs anbefalinger til tiltak for næringen og Ptil samt behov for videre arbeid med kunnskapsinnhenting. Anbefalingene er hovedsakelig hentet fra funn i kapittel 4 og 5.

6.1 Anbefalinger til næringen

Anbefalinger til tiltak for næringen er gitt i Tabell 14.

Tabell 14 Oppsummering av SINTEFs anbefalte tiltak for næringen

Nr.	Utfordring	Anbefaling	Ref.
Hva rapporteres/deles			
1.	Få rapporterte hendelser begrenser mulighet for systematisk forbedring og læring.	Utvikle og ta i bruk metoder og systemer for automatisk registrering og oppfølging av hendelser basert på blant annet erfaring fra produksjonsinstallasjoner, samt andre bransjer som luftfart, vegtrafikk og jernbane. Se også punkt 4 angående etablering av felles interesseforum for næringen for å sikre erfaringsutveksling på tvers av selskaper.	4.6/4.8
2.	Ingen entydig spesifikasjon for hvilke hendelser og avvik (tydelig avgrensning) som skal rapporteres og hvordan de rapporterte hendelsene og avvikene skal klassifiseres.	Etablere en felles retningslinje for næringen for hvilke hendelser og avvik som skal rapporteres og hvordan disse skal klassifiseres for å: a) Sikre rapportering på riktig nivå (unngå både over- og underrapportering) b) Hindre dupliseringer og ekstraarbeid c) Gi kompetanseheving på tvers av selskap d) Hindre at terskel for rapportering og videre klassifisering blir personavhengig e) Legge til rette for sammenlignbare data på tvers av selskap for å bedre sikkerhet, læring og utvikling f) Sikre tydelig rolleforståelse For at en slik retningslinje skal være hensiktsmessig må den etableres av næringen selv. Operatørselskapene som gjerne har flere leverandører i sin portefølje, kan i særskilt grad bidra til å initiere et slikt arbeid.	4.4/5
3.	Mangler kategori for klassifisering av IKT-hendelser.	Innføre en egen kategori for rapportering og klassifisering av IKT-hendelser, se for øvrig punkt 2 over.	4.1.2
4.	Manglende deling av informasjon og kompetanse	Dele informasjon på tvers av selskap, både om hendelser, tilløp til hendelser og intervensjoner. Deling av teknisk informasjon anbefales for kompetanseheving. Legge til rette for erfaringsutveksling gjennom etablering av et felles interesseforum for boring og brønn (ref. PDS forum).	4.6.1/5
5.	Mye tilgjengelige data, men ikke alltid de utnyttes til læring eller forbedring.	Bruke intervensjonsstatistikk mer aktivt for læring. Trekke ut mer informasjon og statistikk om hendelser og tilløp til hendelser i ettertid (f.eks. ved driftsgjennomgang), for eksempel årlig og bruke dette til læring. Etablere flere rutiner for å benytte avvik- og hendelsesdata til læring og forbedring, ikke bare til erfaringsdeling.	4.6.1/5

Nr.	Utfordring	Anbefaling	Ref.
Forhold som påvirker rapportering og oppfølging			
6.	Manglende tillit til de automatiserte systemene påvirker bruken av dem og gir "unødvendige" brukerfeil.	Arbeide aktivt med prosesser for å skape tillit til de automatiserte systemene. Økt involvering av sluttbruker i systemutvikling.	4.7
7.	Nye rapporteringsoppgaver kan stjele verdifull tid/oppmerksomhet fra teknisk personell/borer.	Tilrettelegge for automatisert rapportering, analyse og deling av hendelser basert blant annet på erfaring fra andre bransjer (se anbefaling nr.1).	4.1/4.3.5
8.	Manglende systemforståelse, vanskelig å forstå eller forutse mulige konsekvenser av et avvik under andre omstendigheter.	Mer simulatortrening (med feilscenarier) kan øke forståelse og evne til å rapportere. a) Bør rapportering få mer oppmerksomhet i forbindelse med trening? b) Standardisering av opplæring kan bidra til bedre systemforståelse blant borer og annet teknisk personell (se anbefaling nr. 3 til Ptil)	4.1.2
9.	Ved manuell rapportering kan det ofte være for omfattende å fylle inn skjema.	Lage enkle, gjenkjennbare rapporteringssystemer med gode brukergrensesnitt. Bruke samme system for alle hendelser og avvik og på tvers av selskap. Operatørselskapene kan i særskilt grad bidra til etablering av et standardisert system for hele næringen.	4.3.5
10.	Borers oppgaver er i stadig endring.	Borers oppgaver må endres og tilpasses høyere grad av automatisering etter hvert som flere deler av prosessen automatiseres.	4.1.2

6.2 Anbefalinger til Ptil

Anbefalinger til tiltak for Petroleumstilsynet er gitt i Tabell 15.
Dette er foreløpige anbefalinger som SINTEF vil arbeide videre med og oppdatere i endelig rapport.

Tabell 15 Oppsummering av SINTEFs anbefalte tiltak for Ptil.

	Utfordring	Anbefaling	Ref
1.	Stor variasjon i næringen i registrering og rapportering av IKT-hendelser.	Være pådriver for at næringen etablerer felles retningslinjer for hvilke IKT-hendelser og tilløp til hendelser som skal rapporteres og hvordan disse skal klassifiseres for å sikre fremtidig oppfølging og læring. Forsterke oppfølging rettet mot ulike aktørers rolle i bearbeiding av IKT-hendelser og tilløp til hendelser, inklusive andre aktører enn operatørselskaper som har rapporteringsplikt til Ptil.	4.1.2/4.4/5
2.	Det er få formelle krav til borer.	Vurder om Ptils regelverk bør tydeliggjøre behovet for formelle krav til kompetanse for borer utover brønnsertifikat. Kanskje bør det også være krav til opplæring knyttet direkte mot leverandørspesifikke automatiserte system (f.eks. to system som utfører tilsvarende funksjon, men som har svært ulike brukergrensesnitt)?	4.7

	Utfordring	Anbefaling	Ref
		Være pådriver for at næringen definerer felles krav til opplæring for å unngå at forskjellige operatørselskap har forskjellige krav. Forsterke Ptils rolle i deling av kunnskap og erfaring om sikker design og drift av automatiske systemer i boring.	
3.	Nye rapporteringsoppgaver om IKT-hendelser kan stjele verdifull tid/oppmerksomhet fra borer.	Være pådriver for at næringen tilrettelegger for økt grad av automatisk registrering av avvik i automatiske boresystemer. Vurder henvisning til revidert NORSOK I-002 i veiledning til SF § 19 Innsamling, bearbeiding og bruk av data.	4.1/4.3.5
4.	Dagens rapportering av IKT-hendelser og tilløp til hendelser er for overordnet til å gi et godt grunnlag for læring og fremtidig risikoreduksjon.	Være pådriver for at næringen arbeider mer systematisk med rapportering og bearbeiding av IKT-hendelser for egen læring og fremtidig risikoreduksjon.	4.4/5

6.3 Behov for kunnskapsinnhenting

Formålet med denne rapporten har vært å gi næringen og Ptil økt innsikt i hvordan hendelser, tilløp til hendelser og avvik innenfor automatiserte systemer registreres, bearbeides, rapporteres og eventuelt varsles til Ptil i dag, inklusive ulike aktørers roller i bearbeiding av slike situasjoner. Det er også samlet inn informasjon om håndtering av hendelser og avvik i andre relevante bransjer, som grunnlag for å foreslå hvordan man kan etablere og systematisere rapportering av hendelser og avvik i automatiserte systemer, kontrollsystemer og sammenkoblede løsninger i petroleumsvirksomheten. Resultatene er basert på dokumentgjennomgang, innspill fra intervju og workshop samt interne arbeidsmøter.

Vi opplever av de største utfordringene er at det ikke fins noe klare retningslinjer for hvilke avvik, tilløp til hendelser og hendelser som bør rapporteres, hva terskelen og kriteriene for rapportering skal være, hvordan og hvor rapporteringen skal gjøres samt hvordan de skal analyseres og følges opp for videre læring. Det er derfor et behov for å etablere en slik retningslinje.

Videre er det viktig å sørge for at belastningen på borer ikke blir for stor, både når det gjelder krav til rapportering og i bruk av de nye automatiserte systemene. Det er derfor et ønske fra næringen om å få til større grad av automatisert rapportering. For å muliggjøre dette anbefaler vi å gjennomføre en studie for å se spesifikt på hvilke systemer og prosesser som må på plass for å legge til rette for større grad av automatisert rapportering:

- Hvilke taksonomier og selskapsinterne krav til rapportering må på plass for å muliggjøre automatisert rapportering av avvik og tilløpshendelser, inklusive hendelser på grunn av signalfeil (falske positive) og tilsiktede hendelser så som cyberangrep?
- Hva kan rapporteres automatisk allerede nå (F.eks. anomalitetsdeteksjon, utstyrsfeil etc.)?
- Hvilke muligheter for automatisert rapportering ser en for seg innenfor en kort tidshorisont på 1-5 år og på lengre sikt (5-10 år)?

Samtidig tror vi dette bør sees i sammenheng med å se på hvordan man kan komme videre med automatisering for å gjøre boreprosessen mer autonom og ergo mindre avhengig av borer og annet personell. Imidlertid vil et viktig steg på veien være å se på hvordan systemene kan forbedres for å hjelpe borere, servicepersonell, ingeniører osv. i det daglige arbeidet. For begge disse perspektivene vil det kreve at man finner nye og standardiserte måter å dele data og kunnskap på, og da vil de være behov for å definere og utvikle åpne standarder og løsninger som tilrettelegger for et digitalt deling og informasjonsutveksling for alle aktører gjennom hele verdikjeden. En slik interoperabilitet kan for eksempel oppnås gjennom implementering av Industri 4.0 (se kapittel 2.4.8) eller lignende konsept.

Referanser

[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/.

Vedlegg - Hvilke rapporteringssystem brukes i andre bransjer enn boring?

A Luftfart

A.1 Flight Data Monitoring (FDM)

Flight Data Monitoring (FDM) er et sensorbasert system innenfor luftfart hvor det samles inn en stor mengde ulike sensordata fra luftfartøy under flygninger, opptil flere hundre sensorer avhengig av flytype. Nærmere bestemt handler FDM om å identifisere, kvantifisere og vurdere risiko knyttet til gjennomføring av flygninger på bakgrunn av avvik mellom praksis og standardiserte operasjonsprosedyrer.

FDM er statistikkbasert og innsamlede data lagres kontinuerlig i databaser og analyseres i etterkant av flygninger for å identifisere konkrete hendelser hvor luftfartøyet er fløyet på en måte som overskrider bestemte verdier, samt også avdekke eventuelle uheldige trender i måten det flys på. Hvis FDM – parametere overskrider på forhånd definerte verdier vil det føre til en eller annen form for oppfølging fra analyseorganisasjonen, og eller flyselskap, avhengig av alvorlighetsgraden. Utgangspunktet for analysen av FDM er tre nivåer som er definert på forhånd av flyselskapene. Nivåene og verdiene som settes vil kunne variere fra selskap til selskap, men nivå tre er alltid en alvorlig hendelse, noe som innebærer brudd på en eller flere prosedyrer. Nivå en kan for eksempel være bevegelse på bakken som er noe høyere enn ønsket.

Gjennom helikoptersikkerhetsstudiene som SINTEF utfører for Norsk Olje og Gass er analyse av FDM-data relatert til helikoptersikkerheten offshore tema. Et eksempel herfra og nivå en er identifisering av en uønsket trend i et av selskapene for helikoptrene under avgang, nærmere bestemt en uønsket lav nesestilling for som innebar avganger med en neseposisjon 20 grader under horisonten. Dette var en uønsket trend som ble tatt tak i før den fikk lov til å eventuelt eskalere. Helikopteroperatørene poengterer at FDM er et veldig nyttig verktøy for å være i stand til å stoppe negative trender på et tidlig tidspunkt.

Selve analysen av og organiseringen av hvordan FDM analyser følges opp internt varierer noe fra selskap til selskap, men det er slik at det er strenge regler og prosedyrer involvert når piloter involveres direkte, som oftest knyttet til nivå tre hendelser. Dette handler om sensitivt materiale og personvern, noe som også involverer arbeidstakerrepresentanter. FDM data skal heller ikke anvendes til å straffe enkeltpiloter i ettertid eller overlates til andre aktører. Oppfølginger basert på analyse av FDM data skal kun gjøres i læringsøyemed.

Samtidig er det slik at innenfor forskningslitteraturen er det lite forskning knyttet til eksempelvis hvordan FDM-data proaktivt kan benyttes til bedre å forstå hendelser og sammenhenger hvor menneskelig yteevne og menneske-automatiseringsteknologi har betydning. I en slik sammenheng vil FDM data potensielt kunne anvendes til å undersøke hvordan ulike faktorer som påvirker menneskelig yteevne synliggjøres gjennom variasjon i ulike FDM parametere. Yan (2014) [38] poengterer i den sammenheng hvordan FDM har potensiale til å bedre forstå risiko knyttet til f.eks. manglende etterfølgelse av regler, manglende situasjonsforståelse samt høy arbeidsmengde. Yan (2014) [38] identifiserer derav syv flyparametere, samt hvordan FDM data kan anvendes for å overvåke risiko knyttet til menneskelige faktorer, eksempelvis hvordan FDM data kan benyttes til å overvåke ”automation confusion” [38].

Anvendelsen av FDM-data i luftfart er i utgangspunktet en reaktiv tilnærming til sikkerhet gjennom å identifisere og følge opp ovenfor besetningsmedlemmer uønskede hendelser hvor det er registrert et betydelig avvikt fra nevnte forhåndsdefinerte sensorverdier. Samtidig innebærer analyse av FDM data også en proaktiv tilnærming til flysikkerheten gjennom å innføre tiltak ved uønskede trender hvor fokus er å lære fra hendelsene, noe som innebærer å ikke peke på enkeltindivider per se og fordele skyld.

A.2 Rapportering av hendelser og ulykker til myndighetene

Regelverk

Utgangspunktet for rapportering av hendelser og ulykker er knyttet til Europaparlaments rådsforordning 376/2014 som omhandler rapportering og undersøkelse av ulykker og hendelser innen luftfart - forordningen trådte i kraft i Norge 1. juli 2016. Dette har medført at nasjonale bestemmelser, BSL A 1-3 er blitt erstattet av et felleseuropeisk regelverk gjennom Kommisjonsforordning (EU) 2015/1018 hvor bestemmelser til forordning 376/2104 er gitt [39].

Regelverket innbefatter alle luftfartsorganisasjoner med egne ansatte eller innleid personell. Organisasjonen skal kunne rapportere luftfartshendelser gjennom egne interne system herunder mottak av rapporter, analyse samt oppfølging. Risiko – og kvalitetsstyringen skal være forankret i selskapsspesifikke sikkerhetsstyringssystem.

Hva rapporteres

I luftfart skal alle hendelser og ulykker rapporteres inn til luftfartsmyndighetene, nærmere bestemt luftfartstilsynet. Luftfartstilsynet definerer en hendelse innen luftfart som enten et driftsavbrudd, feil eller en eller annen form for uregelmessighet knyttet til operasjoner som har innvirkning på flysikkerheten [39]. Det er satt en tidsfrist på 72 timer etter en ulykke eller hendelse til å rapportere, alternativt 72 timer etter at organisasjonen blir klar over hva som har hendt. Rapporteringen foregår gjennom Altinn.

Eksempler på hva som er rapporteringspliktig kan være at besetningen feiltolker en automatiseringsmodus eller annen informasjon som mottas i cockpit, som igjen kan føre til fare for luftfartøy eller personer. Tap av situasjonsforståelse er også nevnt herunder at man mister oversikt over miljøet man operer innenfor, noe som relateres til romlig desorientering og manglende opplevelse av tid. Annet eksempel er teknisk tap av redundans i et system, eksempelvis funksjonssvikt eller at en indikator feiler som igjen fører til at misvisende informasjon gis besetningen.

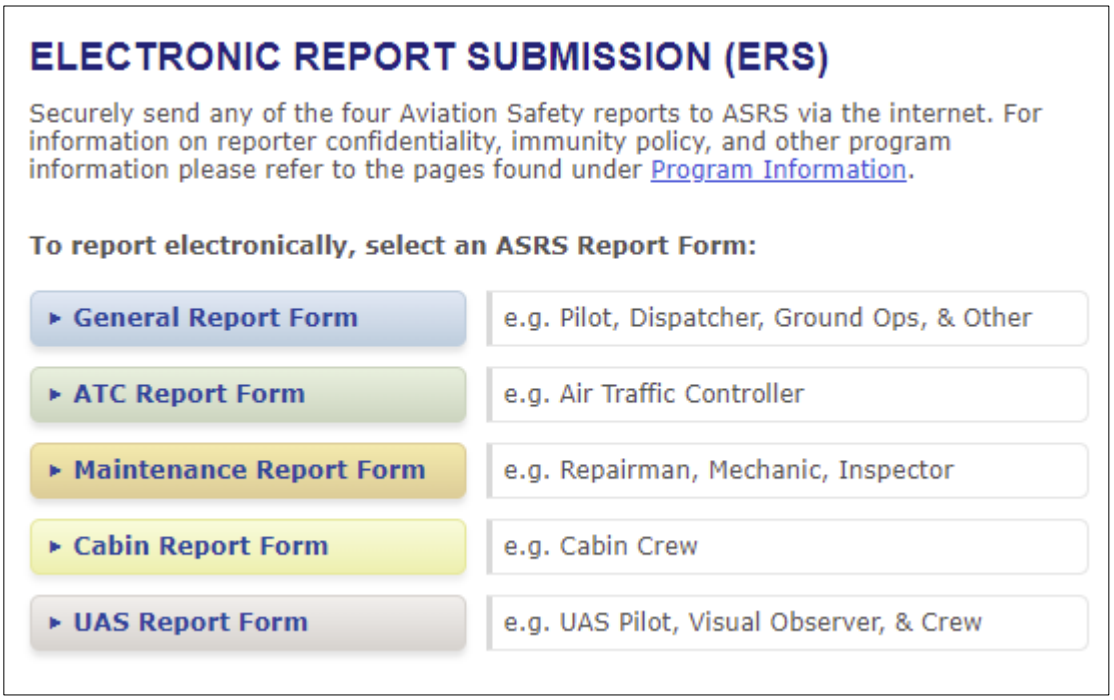
Hvem er ansvarlig

Dette knyttes til hvem som har rapporteringsplikt, noe som sees i sammenheng med flere ulike roller. Det kan være fartøysjefen om bord, alternativt andre besetningsmedlemmer hvis fartøysjefen ikke er i stand til å rapportere selv. Rapporteringsansvarlig er også personer som arbeider med design, konstruksjon, luftdyktighet eller kontinuerlig vedlikehold av luftfartøy. Tilsvarende de personer som eksempelvis utfører ulike former for inspeksjon av luftdyktigheten til et luftfartøy. Videre har man rapporteringsansvar som yter av lufttrafikktjenester herunder eksempelvis flygekontrolltjeneste. Personer som utfører bakketjenester (drivstoffylling, lastedokumentasjon) i og rundt et luftfartøy har også rapporteringsansvar.

Luftfartstilsynet poengterer at rapporteringsplikten og utøvelsen av denne alltid må sees i sammenheng med etterlevelse av prinsippet om just culture innenfor luftfartsbransjen.

A.3 Frivillig rapportering av hendelser

I USA har NASA har utviklet et frivillig rapporteringssystem som forskjellige aktører innen luftfart kan anvende (Se figur nedenfor) [40].



Figur 15 Frivillig rapporteringssystem for luftfart utviklet av NASA.

B Vegtransport

B.1 Innledning

Norge var en av de første landene som utarbeidet en egen lov i 2017 for "Utprøving av selvkjørende kjøretøy" [41]. Ved tillatelse av utprøving av autonome kjøretøy så baserer Vegvesenet seg på gjeldene norske lov med tilhørende forskrift.

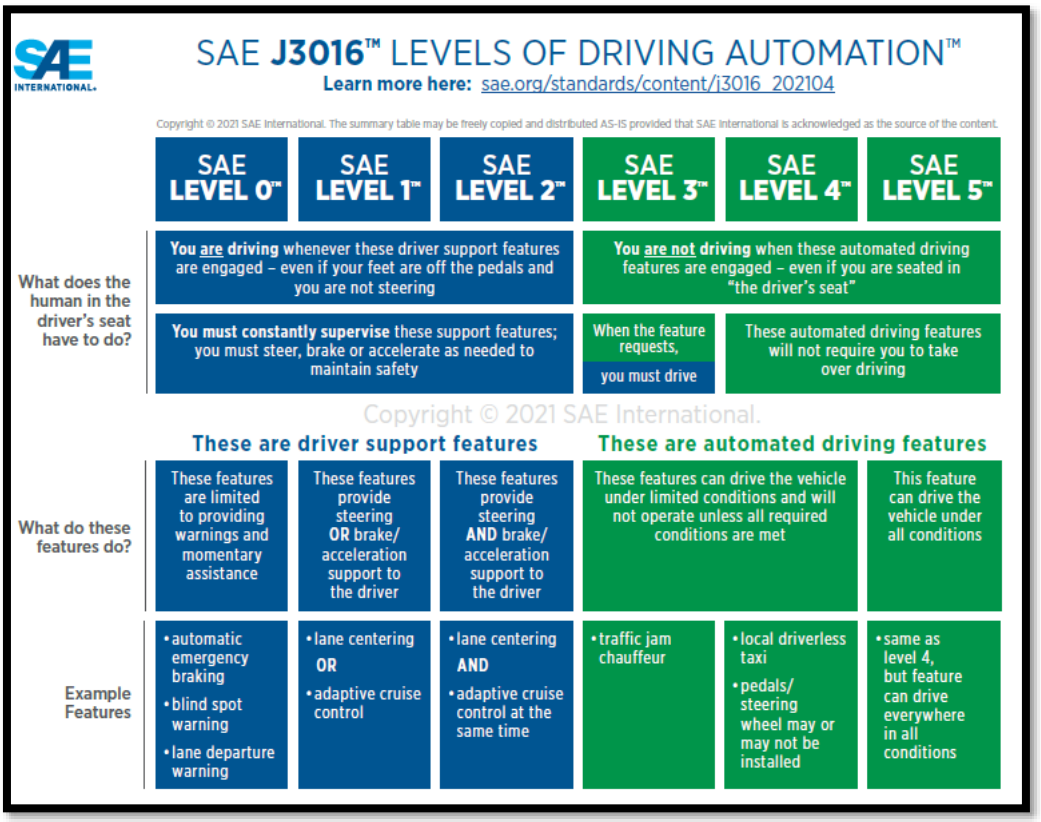
SIS funksjoner inkluderes ofte i kjøretøyene uten at de er del av godkjenningen.

I Europa godkjennes kjøretøyene i ett av EU/EØS landene. Da kan kjøretøyet benyttes i alle landene.

Både blant lovgivere, media og i ulike rettssaker har det vært mye diskusjon rundt "AutoPilot". Diskusjon gjelder ansvaret til sjåføren og hvordan det reklameres med autopilot av fabrikant.

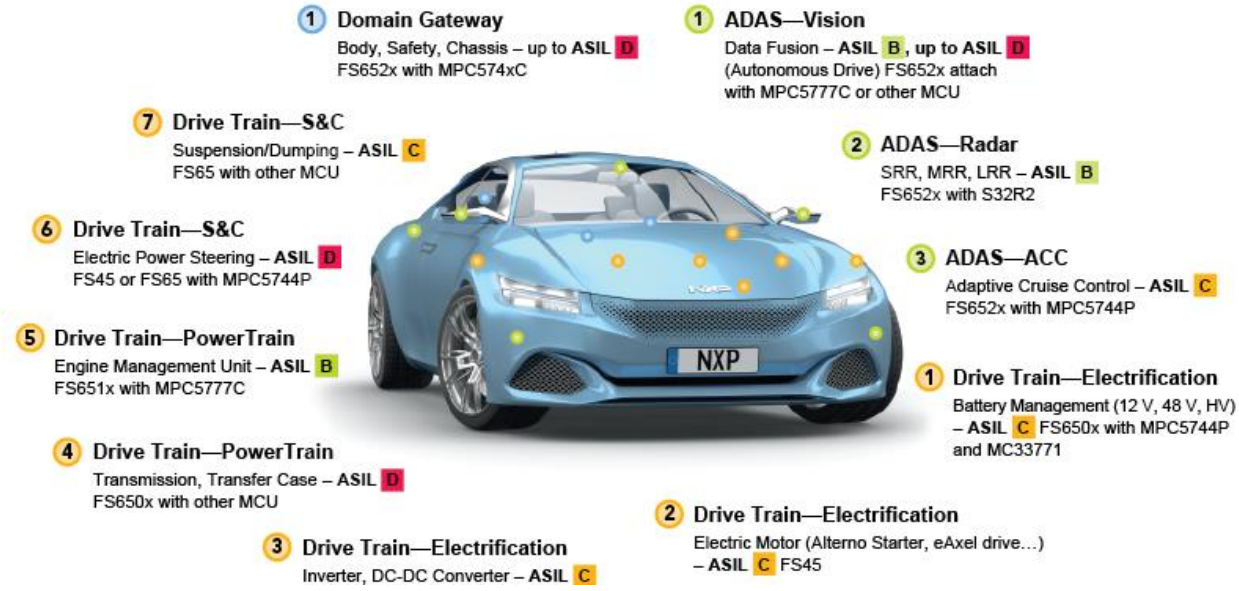
Tabellen nedenfor viser ulike grader av automatisering og autonomi innen vegtransport.

Tabell 16 Ulike nivå for automatisering, SAE J3016 [42].



Innen vegtransport er det naturlig å skille mellom biler med innebygde automatiske funksjoner og autonome busser.

For biler med automatiske funksjoner og "SIS" har man foreslått aktuelle SILx (kalles ASILx, hvor A står for automotive), men disse er kun angitt i en noe foreldet standard fra SAE, J2980:201804 [43].



Figur 16 Automotive og aktuelle "SIS" med tilhørende ASILx.

B.2 Rapporteringssystem, innsamling og klassifisering

I de siste årene har flere og flere biler inkludert OTA (over the air) systemer. Fabrikantene bruker dette bl.a. til oppdatering av data og programvare. Myndigheter og andre får vanligvis ikke tilgang til disse dataene. Men i de tilfellene det skjer ulykker relatert til disse automatiske funksjonene, så spres informasjon vi media over hele verden innen få timer.

Det er utgitt en standard for OTA; "UL 5500:2018 Standard for safety, remote software updates" [44]. I tillegg utarbeider ISO en tilsvarende standard: "ISO/DIS 24089 draft CD Software update engineering" [45].

Fabrikantene bruker OTA både for å overvåke kjøringen og til programvareoppdateringer (også kalt DevOps). ISO og IEC utvikler nå en ny standard ISO/IEC TR 5469 [46] for funksjonell sikkerhet og kunstig intelligens. Fabrikantene har kunnet oppdatere disse systemene uten ytterligere godkjenning selv om oppdateringen inkluderte sikkerhetssystemer. Det pågår en innstramming på dette området ved at UNECE har utgitt krav til programvareoppdatering. Disse kravene vil sannsynligvis bli inkludert i fremtidig lovgivning.

Når programvaren i bilene blir oppdatert, vil eieren få en oppdatert versjon av f.eks. brukermanualen. Versjonsnummer vil kunne vises på displayet i bilen. Det er opp til den enkelte sjåføren å sette seg inn i den nye versjonen. Det er viktig å merke at ifølge brukermanualen er det sjåføren som har ansvaret. Det er grunnen til at bilfabrikantene slipper unna og sjåførene sitter igjen med ansvaret.

I USA har NHTSA etablert en "hotline" hvor man kan rapportere opplevde sikkerhetsproblem med kjøretøy (dekk, bilsete eller utstyr). Man kan sende inn en klage som gjennomgås av NHTSA.

NHTSA (**) har også etablert ett frivillig system for innrapportering fra myndigheter og selskaper om erfaringer fra testing av automatiserte kjøretøyer, som en del av "AV TEST-initiativet". Fabrikanter av automatiserte kjøresystemer forbedrer sine systemer gjennom validering i interne tester og simuleringer med kontrollert testing på offentlig vei.

eCall er et felles europeisk nødmeldingssystem for varsling av trafikkulykker. Hvis en bil med eCall er involvert i en trafikkulykke, går det automatisk en varsling til nærmeste 110-sentral. Flere og flere biler har en SOS-knapp i bilen som er tilknyttet eCall. Man kan også varsle manuelt ved å trykke på SOS-knappen, men den skal kun brukes i en reell nødsituasjon.

Landets 110-sentralar bruker mye tid på å håndtere unødvendige alarmer fra nye biler. I 2020 måtte brannvesenet håndtere 4405 slike alarmer. 92 % av alarmene var falske.

Kjøretøyprosjekt basert på tillatelser fra Vegvesenet:
I vedtaket operatøren mottar før prøvedrift står følgende (dette er ett tilpasset eksempel. Kravene kan endres fra prosjekt til prosjekt):

> *Ansvarlig firma skal sørge for at det føres en kontinuerlig logg som beskrevet i forskrift om utprøving av selvkjørende motorvogn § 12 andre ledd. Vi ber derfor om tilgang på en data-log som kan vise bevegelsesmønstret til kjøretøyet mot slutten av innkjøringsfasen. Dersom sikkerhetstiltakene ikke virker slik de er tenkt eller andre forhold oppstår med hensyn til sikkerhet og fremkommelighet, skal søker varsle lokale myndigheter og Vegdirektoratet umiddelbart*.

BSI har i år publisert et eget dokument: PAS 1882:2021, Data collection and management for automated vehicle trials for the purpose of incident investigation [47], som spesifiserer krav til innsamling, lagring og deling av informasjon under forsøk med selvkjørende biler i Storbritannia. Målet er å bidra til at organisasjoner som gjennomfører forsøk med selvstyrte biler, samler data på et standardisert format.

Kjøretøy generelt:
I Norge har man en egen forskrift om varsling og rapportering av trafikkulykker og trafikkuhell: FOR-2005-06-30-793: Forskrift om offentlige undersøkelser og om varsling av trafikkulykker mv. [34].

> *"§ 4.Umiddelbar varsling om alvorlige trafikkulykker og trafikkuhell*
> *Politiet og Statens vegvesen skal straks varsle undersøkelsesmyndigheten om alvorlige trafikkulykker som enten:*
> *a) har funnet sted i en tunnel*
> *b) involverer buss eller kjøretøy med totalvekt over 7,5 tonn,*
> *c) involverer kjøretøy som transporterer farlig gods (ADR).*
>
> *Politiet og Statens vegvesen skal også straks varsle om alvorlige trafikkulykker og/eller alvorlige trafikkuhell:*
> *d) som omfattes av nærmere spesifiserte kriterier fastsatt av undersøkelsesmyndigheten, og hvor denne skriftlig har bedt om slik varsling, eller*
> *e) som de etter en samlet vurdering mener undersøkelsesmyndigheten kan ha interesse av å undersøke, jf. § 3 første ledd.*
>
> *Varsling skal skje til angitt vakttelefon hos undersøkelsesmyndigheten.*
> *Dersom varsling foretas av Statens vegvesen skal politiet umiddelbart underrettes om varslingen.*
>
> *§ 5.Rapportering av alvorlige trafikkulykker og trafikkuhell*
> *Politiet skal så snart som mulig gi skriftlig rapport til undersøkelsesmyndigheten om alle trafikkulykker og trafikkuhell som er varslingspliktige i henhold til § 4. Politiets «Rapport om vegtrafikkuhell» kan brukes som rapport etter denne bestemmelsen."*

C Maritim skipsfart

Innen maritim rapportering skiller vi mellom intern rapportering og ekstern. Den interne kan bli karakterisert som

Intern rapportering	Rapportering om bord i båt Rapportering til selskapet og egen flåte Rapportering til systemleverandører/klasse (motorprodusenter etc.)
Ekstern rapportering	Rapportering til myndigheter Pålagt rapportering ifbm. hendelser

C.1 Intern Rapportering

Dagens praksis er at det kun rapporteres innad i operatør- og/eller eierselskaper (rederi) samt til klasseselskap. I skrivende stund kjenner vi ikke til noe felles uavhengig database, men klasseselskaper som DNV, Lloyds, ABS etc. har sine databaser basert på skipene de gjør klassetjenester for. Det er stor spredning i måten man rapporterer på, og sektoren er generelt i en modningsfase når det gjelder innsamling og bruk av data. Det måles mye, men få har kontroll på kvalitet og behov. SFI gruppesystem er den mest benyttede metoden for teknisk oppfølging av skip, en metode som så dagens lys helt tilbake til 1972 og ble utviklet av SFI: Skipsteknisk Forskningsinstitutt, som ble MARINTEK, som nå har blitt SINTEF Ocean). Metoden har blitt kontinuerlig forbedret og vedlikeholdes i dag av SpecTec.

SFI Group System er det mest brukte klassifiseringssystemet for maritim og offshore industrien over hele verden. Det er en internasjonal standard, som gir en funksjonell underavdeling av teknisk og finansiell skip- eller rigginformasjon. SFI består av en teknisk kontostruktur som dekker alle aspekter ved skip/riggspesifikasjon, og den kan brukes som en grunnleggende standard for alle systemer i shipping/offshore industrien. Mer enn 6000 SFI -systemer er installert over hele verden. SFI brukes av shipping- og offshoreselskaper, verft, konsulentfirmaer, programvareleverandører, myndigheter og klassifisering.

Figur 17 SFI Quality loop.
Source: SFI Group system

SFI Group System er inndelt som følgende:

- Primærgruppe 1 - Generelt
- Primærgruppe 2 - Skrogsystemer
- Primærgruppe 3 - Lastutstyr
- Primærgruppe 4 - Skipsutstyr
- Primærgruppe 5 - Mannskap og passasjerutstyr
- Primærgruppe 6 - Maskinens hovedkomponenter
- Primærgruppe 7 - Systemer for maskinens hovedkomponenter
- Primærgruppe 8 - Vanlige systemer

De to gruppene som peker seg ut som mest relevant i denne rapporten er

- Primærgruppe 6 - Maskinens hovedkomponenter: Primærkomponenter i maskinrommet, for eksempel hoved- og hjelpemotorer, propeller, anlegg, kjeler og generatorer.

- Primærgruppe 7 - Systemer for maskinens hovedkomponenter: Systemer som betjener hovedkomponenter, for eksempel drivstoff- og smøreoljesystemer, startluftsystem, eksosanlegg og automatiseringssystemer.

C.2 Ekstern rapportering

C.2.1 Rapportering i konvensjonell shipping

Innen det maritime segmentet i Norge er det hendelser som styrer rapporteringskravet. Ulykker og nestenulykker må rapporteres inn til de ulike etater, ut fra hvilken type hendelser som skal rapporteres. Når hendelsen er av en alvorlig karakter så vil det være behov for gransking av hendelsen, som da blir en granskingsrapport til slutt.

Skipsfører eller rederi skal blant annet rapportere sjøulykker og arbeidsulykker til Sjøfartsdirektoratet på fastsatt skjema innen 72 timer etter hendelsen. Rapporteringsplikten gjelder uavhengig av om det er gitt melding om ulykken eller ikke. Skipsfører eller rederi skal uten opphold gi muntlig melding ved blant annet:

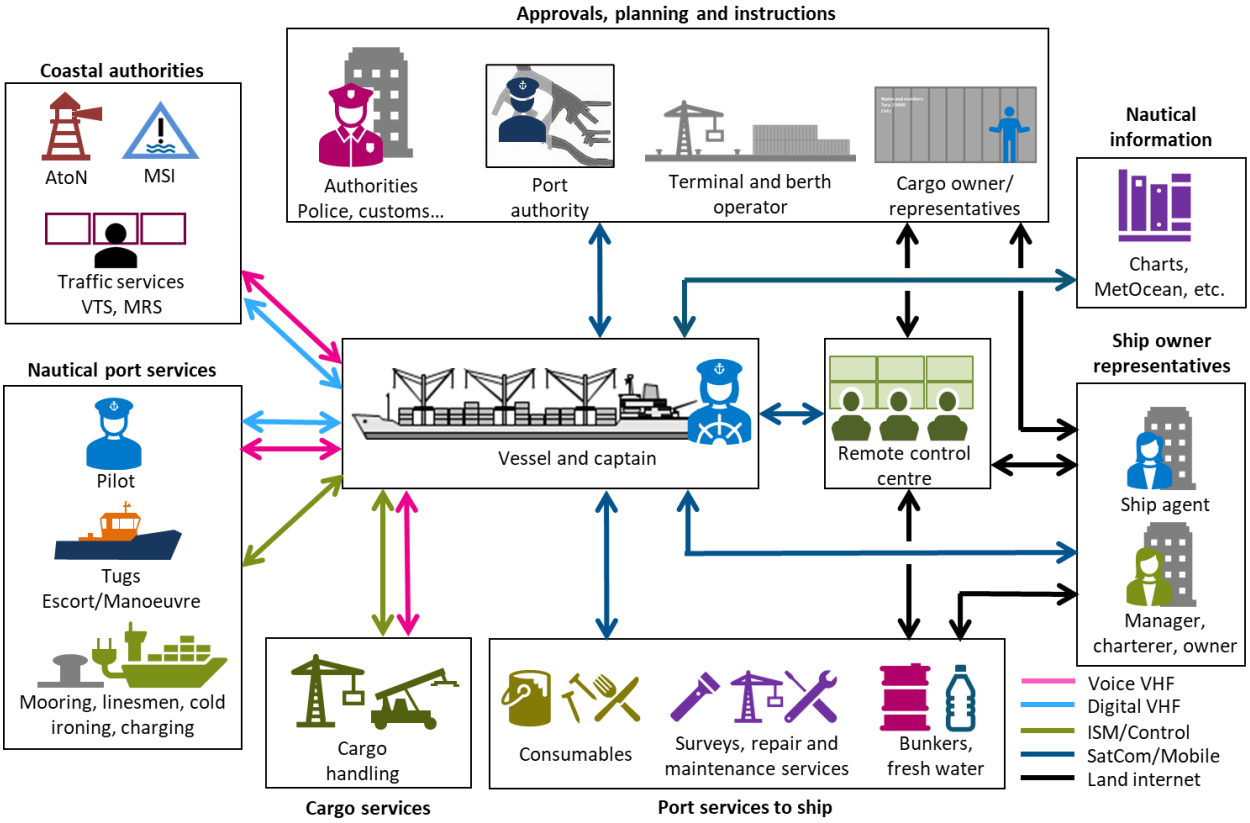
- tap av skip eller liv
- betydelig skade på person eller fartøy,
- arbeidsulykke når det kreves evakuering av den skadde
- utslipp eller sannsynlig utslipp av olje eller skadelige stoffer
- brann, eksplosjon, sammenstøt eller lignende
- grunnstøting og kollisjon

Dette gjelder også når eksternt personell som utfører arbeid om bord i fartøy, er part i en ulykke om bord eller har en ulykke om bord.

Ulykker og hendelser klassifiseres i henhold til en rekke kjennetegn så som: Kantring, Kollisjon, Kontakt med annet objekt, Flytende objekt (last/container, is, annet), Flyvende objekt, Landbasert objekt), Skade/tap av utstyr, Brann og eksplosjon, Vanninntrenging, Grunnstøting, Skade på skrog, Tap av kontroll: Fremdrift, Elektrisk, Direksjonal, Ikke funnet, Krig, Kriminalitet, Ulovligheter. Det er også viktig å fremheve at det er forskjellige skipskategorier, fra passasjerferger til fiskebåter, fra containerskip til cruise.

Rapportering av tekniske feil gjøres ikke, dersom dette ikke er del av hendelsesårsak til en ulykke. Det er ingen felles database for innsamling av tekniske feil innen maritim sektor Det er fartøyets rederi som innhenter informasjon om båtens tilstand, som eksempelvis tilstand på fremdriftsmekanismene.

Et sammensatt bilde av rapporteringskravene i konvensjonell shipping er illustrert i Figur 18. Figuren viser hvilke informasjonsstrømmer som er for tale, digital og styring. Figuren er kompleks og det er flere typer systemer som er involvert, noen for navigasjon andre mer for statusrapportering.



Figur 18 Konvensjonell samhandling. Kilde: SINTEF

Ved rapportering av hendelser så har vi ikke i dag et eget mottakssted for teknologiske hendelser som skyldes feil på teknologi eller sensorer. Dette er noe de enkelte rederiene har selv, som må på plass for godkjenning gitt av flaggstat eller klasse, som også vil være nyttig når forsikringer inngås med forsikringsselskap. Rapportering av hendelser gjøres til ulike etater, ut fra hendelses karakter. I utgangspunktet så er det i Norge de tre etatene Kystverket, Hovedredningssentralen og Sjøfartsdirektoratet som har ulikt mandat og ansvarsområde:

- Hovedredningssentralen: Har ansvar for berging av mennesker.
- Kystverket: Har ansvaret for å begrense skadeomfang når hendelsen medfører utslipp til miljø.
- Sjøfartsdirektoratet: Har ansvar for inspeksjon av fartøy og at fartøyet har riktige sertifikater.

C.2.2 Hovedredningssentralene

Landets to hovedredningssentraler er lokalisert ved Bodø havn og i eget bygg på Sola utenfor Stavanger. Offisiell betegnelse er HRS Sør-Norge, Stavanger og HRS Nord-Norge, Bodø. Som det fremgår av betegnelsen har disse overordnet ansvar for henholdsvis Sør-Norge og Nord-Norge. Grensen for ansvarsområdene går ved 65. nordlige breddegrad i sjøområdene, og på land langs grensen mellom Nord-Trøndelag og Helgeland politidistrikt.

Samlet statistikk Hovedredningssentralen 2020															
SJØ			Jan	Feb	Mar	Apr	Mai	Jun	Jul	Aug	Sep	Okt	Nov	Des	Total
	% av Alle	% av Sjø													
Assistanse fartøy	10,6 %	29,0 %	30	42	74	72	92	110	152	92	82	47	31	39	863
Brann - Større fartøy	0,1 %	0,3 %	1	1	1	1		3	1				1		9
Brann - Mindre fartøy	1,2 %	3,2 %	3	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 %	0,3 %	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	0,3 %	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 %	0,5 %	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	0,9 %	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	4,9 %	13,4 %	39	29	30	22	34	39	42	37	23	36	34	35	400
Offshorehendelse	0,6 %	1,5 %	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	36,6 %	100,0 %	165	157	202	208	272	331	476	335	267	202	183	177	2975

Figur 19 Statistikk Hovedredningssentralen 2020 (sjø). Kilde Hovedredningssentralen

Statistikken for 2020 viser at det var 2975 hendelser som ble rapportert. Tilsvarende tall for 2019 var 3227, i 2018 var det 3427 og i 2017 ble det registrert 3809 hendelser. Dette gjelder for begge de to sentralene. Tallene viser fordelingen ut fra kategorier, hvor assistanse til fartøy hadde 863 hendelser mens signaler fra nødpeilesender, DSC, Inmarsat, Pyroteknisk og EPIRB utgjør også en stor andel. Fra tidligere studier så har det blitt avdekket av mange hendelsene med Nødpeilesender skyldes falske alarmer, hva denne prosentdelen er i denne statistikken er uvisst.

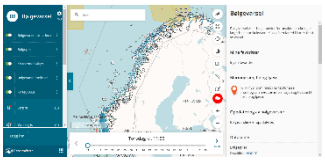
C.2.3 Kystverket

Kystverket er den etaten som har ansvaret for sjøtransport og trafikkovervåking i Norge. Kystverket er en transportetat som ligg under Samferdselsdepartementet. Mandatet er å sørge for sikker og effektiv ferdsel i farleier langs kysten og inn til havner, og sørge for nasjonal beredskap mot akutt forurensing. De viktigste oppgavene er:

- Utvikling og vedlikehold av farleder
- Fyr- og merketjenester
- Trafikksentraltjenester
- Lostjenester
- Meldingstjenester og navigasjonsvarsel
- Statlig beredskap mot akutt forurensing
- Utgreiing og transportplanlegging
- Havnesikkerheit (ISPS)
- Kystverket har også ansvar innen maritim sektor av Nasjonal transportplan (NTP), samt myndighets- og forvaltningsoppgaver knytt til lover og regelverk for hamner, farleier og losplikta.

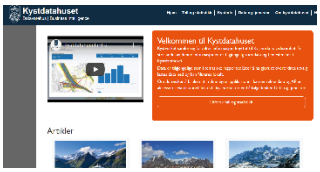
Når gjelder rapportering av skipsinformasjon er SafeSeaNet Norway portalen som skal benyttes når rapportering av skipsanløp til norske havner skal gjøres. Her vil informasjon om fartøy, om last, og om planlagt rute ligge. Portalen vil også inneholde informasjon om transport av farlig gods, som kan være en risiko. SafeSeaNet er koblet opp mot tilsvarende single window løsninger i andre Europeiske land.

Kystverket har også en tjeneste hvor de gir anbefalte ruter til maritim trafikk. Denne tjenesten heter routinfo.no og dekker per skrivende stund ruter fra sørlige punkt av Norge opp til Vesterålen. Rutene som anbefales har waypoints med posisjonsangivelse (Lat/Lon) som kan benyttes av fartøyene inn i sine kart (ECDIS), som fartøyene kan forholde seg til under en seilas. Dette er ruter som er anbefalt ut fra dybdeforhold og sikker farleder, de inneholder ikke sanntidsinformasjon om trafikk.



En annen tjeneste Kystverket formidler er Barentswatch. I denne løsningen så kan sanntidsinformasjon om farleder hentes, samt prognoser. Eksempelvis kan bølgevarsel hentes inn og være et grunnlag for en trygg planlegging av en seilas.

Kystinfo er en tjeneste hvor mye sjørelatert informasjon er samlet. Her kan informasjon om sanntidstrafikk vises, informasjon om historiske seilaser, heatmap over trafikk i områder, og marine grunnkart og statistikker som eksempler. I løsningene vil også digitale havnedatakart ligger, eksempelvis vil koordinatene til et forankringspunkt være tilgjengelig i enkelte havner.



Kystdatahuset.no er startsida for Kystverket sitt krafttak for å gi interne og eksterne brukere enkel og god tilgang til sjøtrafikkdata. Data kan hentes på to ulike måter:

1. Kystdatahuset – Menypunkt «Tall og statistikk». Inneholder ulike dashbord/spørringer med sjøtrafikkdata, hvor du får dataene presenterer i kart, figurer og datatabell. I dashbordene kan du filtrere og analysere dataene. Skjermbilder kan lagres og tabell med data eksporteres til Excel.
2. Datadelingsportal – Menypunkt «Data og tjenester». Portal for nedlasting av større datasett. Bruk og presentasjon av dataene gjøres i mottakers egne verktøy og løsninger. Portalen inneholder et utvalg av datasett både om sjøtrafikk og andre maritime data.

Vessel Traffic Services

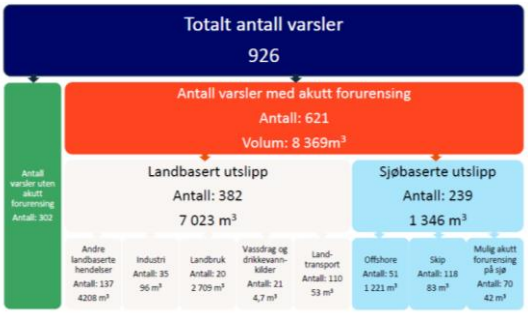
Kystverket er ansvarlig for sjøtrafikksentraltjenesten i Norge (VTS). Kystverket har fem sjøtrafikksentraler som informerer, organiserer og overvåker skipstrafikken i definerte tjenesteområder langs kysten. Sjøtrafikksentralene er et risikoreduserende tiltak for å forebygge uønskede trafikksituasjoner i definerte risikoområder med stor trafikktetthet og der det er en større andel av trafikk med farlig og/eller forurensende last. Den norske sjøtrafikksentraltjenesten bygger på nasjonalt regelverk, internasjonalt regelverk fra FNs sjøfartsorganisasjon IMO, og standarder fra den internasjonale maritime organisasjonen IALA.

Beredskap

Kystverket (er også Kystverkets) har ansvaret for å koordinere statlig, kommunal og privat beredskap. Formålet med beredskapen mot akutt forurensning er å verne om liv, helse, naturmiljø og næringsinteresser til sjøs og på land. I utgangspunktet er det ansvarlig forurenser som har tiltaksplikt ved akutt forurensning. Dersom den ansvarlige ikke kan eller vil gjennomføre nødvendige tiltak vil det offentlige, ved Kystverket, ta over. Ved hendelser som medfører fare for et større tilfelle av akutt forurensning kan Kystverket bestemme at staten skal lede håndteringen av aksjonen. Det betyr at Kystverket tar ansvaret for å lede aksjoneringen både på sjø og i strandsonen. Nødvendige tiltak vil være tiltak for å hindre at fare for akutt forurensning bli til faktisk forurensning. Har forurensning inntrådt vil nødvendige tiltak bestå i å stanse, fjerne eller begrense virkningen av forurensningen.

Alle hendelser med akutt forurensning eller fare for akutt forurensning på fastlandet skal varsles som beskrevet i varslingsforskriften, Forskrift om varsling av akutt forurensning eller fare for akutt forurensning, 1993, som er fastsatt med hjemmel i forurensningsloven § 39, Lov om vern mot forurensninger og om avfall (forurensningsloven) [48], 1983, og svalbardmiljøloven § 70 [49] når forurensningen inntrer eller truer med å inntre på Svalbard eller i farvannet rundt. Varslingsplikten påhviler som hovedregel den ansvarlige for

forurensningen, men alle som oppdager akutt forurensning eller fare for akutt forurensning plikter å varsle på brannvesenets nødnummer 110. For fartøy til havs varsles nærmeste kystradio eller Hovedredningssentralen (HRS). For nærmere informasjon om varsling, se Kystverkets hjemmeside eller varslingsinstruksen [50].



Kystverket mottar og behandler vanligvis 1 000 – 1 400 ulike varsler og meldinger om akutt forurensning eller fare for slik forurensning hvert år. Disse blir loggført i Kystverkets krisestøtteverktøy "KystCIM" og danner grunnlaget for statistikk over akutt forurensning. Statistikken omfatter både innrapporterte hendelser som har ført til akutt forurensning og hendelser hvor det har vært fare for akutt forurensning, men hendelsen ikke førte til utslipp. Figuren viser oversikt over antall varsler og utslippsvolum (m3) fordelt på hovedkategorier som ble behandlet av Kystverkets beredskapsvaktlag i 2020.

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**

Tabellen viser loggførte hendelser rapportert til Kystverkets beredskapsvakt (med og uten utslipp) i tidsrommet 2013 - 2020 fordelt på ulike typer hendelser.

Kystradiostasjonene

Kystradio består av to døgnbemannede stasjoner – Kystradio Nord og Kystradio Sør – og rundt 120 fjernstyrte VHF-stasjoner. Kystradio er også en del av Redningstjenesten i Norge, og er bindeleddet mellom fartøyet i nød og Hovedredningssentralen. Kystradio ivaretar en av Telenor sine mange samfunnspålagte oppgaver, og er en del av redningstjenesten i Norge. Redningstjenestens behov for radiokommunikasjon over kystradioene leveres av Telenor og drives i kombinasjon med den kommersielle delen av kystradiotjenesten. Den høyest prioriterte oppgaven innenfor dette er å være bindeleddet mellom fartøyet i nød og hovedredningssentralene.

Kystradiostasjonene skal ivareta oppgaver som:

- Vakthold på de internasjonale nødfrekvensene
- Motta meldinger og opprette samband med fartøy i nød
- Sørge for effektiv sambandsavvikling under søk og redningsaksjoner
- Alarmere hovedredningssentralene
- Varsle skip og eventuelle andre enheter som kan bidra med redningsressurser
- Sende ut meldinger som har sikkerhetsmessig betydning for trygg seilas og navigasjon.
- Formidle legeråd (Radio Medico)
- Formidle kommersiell trafikk

Global Maritime Distress Safety System (GMDSS)

Global Maritime Distress Safety System (GMDSS) er et sett med internasjonalt godkjente prosedyrer for sikkerhet, utstyrstyper og kommunikasjonsprotokoller, og som skal øke sikkerheten og gjøre det lettere å redde nødstedte fartøy og fly. Fartøy over 15 m og alle fartøy med passasjertrafikk skal ha GMDSS-godkjent utstyr om bord for det havområdet de seiler i. I 2014 kom det også strengere krav til GMDSS utstyr for fiskefartøy under 15 m.

Krav til utstyr er avhengig av hvilke områder skipet opererer i, og er knyttet til dekningsområdet for ulikt radioutstyr. Områdene av interesse dekker de fire områdekategoriene:

- **A1:** Områder innenfor rekkevidde av landbaserte VHF-stasjoner (20-30 nm).
- **A2:** Områder innenfor rekkevidde av landbaserte MF-stasjoner (100-150 nm) med unntak av A1-områder.
- **A3:** Områder innenfor rekkevidde av Inmarsat (mellom ~70 ° N og ~70 ° S) med unntak av A1 og A2-områder.
- **A4:** Områder utenfor A1-A3, som eksempelvis nordområdene.

Utstyrskravene er utformet slik at man skal ha mulighet til å sende og motta varsler og nødsignaler i de områdene man opererer; et "minimumskrav" for operasjon i A1-området, med ekstra krav til MF/HF-utstyr og satellittutstyr dersom man ferdes utenfor dette området.

Utstyr som omfattes av GMDSS-krav er bl.a.

- Radioinstallasjoner – krav avhenger av område. I tillegg til installert radio skal det også være portable transivere for bruk i livbåt.
- DSC (Digital Selective Calling) – Et system som sender en predefinert digital melding via MF, HF eller VHF. En nødmelding sendt med DSC inneholder skipets MMSI og er vanligvis også koblet opp mot skipets GPS, slik at skipets identitet og posisjon automatisk kommer med i meldingen. I tillegg til raskt å kunne sende meldinger, vil et skip ha utstyr for mottak av slike meldinger.
- EPIRB (Emergency Position-Indicating Radio Beacon) – En nødpeilesender som sender signaler som kan oppfattes av COSPAS-SARSAT satellittsystemer.
- EGC og Navtex er ikke tatt med.

C.2.4 Sjøfartsdirektoratet

Sjøfartsdirektoratet er et forvaltningsorgan underlagt Nærings- og fiskeridepartementet og Klima- og miljøverndepartementet. Sjøfartsdirektoratet er forvaltnings- og tilsynsmyndighet for arbeidet med sikkerhet for liv, helse, miljø og materielle verdier på fartøy med norsk flagg og utenlandske fartøy i norske farvann. Direktoratet har også ansvar for å sikre rettsvern for norskregistrerte skip og rettigheter i disse. Aktivitetene blir bestemt av nasjonalt og internasjonalt regelverk, avtaler og politiske beslutninger. Hovedoppgavene til Sjøfartsdirektoratet er:

1. Trygge liv og helse, miljø og materielle verdier
2. Registrere fartøy og rettigheter i fartøy
3. Føre tilsyn med bygging og drift av fartøy med norsk flagg, og deres rederier
4. Utstede sertifikater for sjøfolk og føre tilsyn med norske utdanningsinstitusjoner
5. Føre tilsyn med utenlandske fartøy i norske havner
6. Føre tilsyn med og fremme gode arbeids- og levevilkår på fartøy
7. Forvalte og utvikle norsk og internasjonalt regelverk
8. Markedsføre Norge som flaggstat
9. Forvalte tilskuddsordninger på vegne av departementet
10. Overvåke risikobildet
11. Drive forebyggende arbeid for å redusere antall ulykker i både fritidsflåten og næringsflåten

Ulykker og nestenulykker skal innrapporteres. Dette er regulert i Lovdata, Forskrift om melde- og rapporteringsplikt ved sjøulykker og andre hendelser til sjøs [51]. Denne forskriften gjelder melde- og rapporteringsplikt ved:

a) sjøulykker og svært alvorlige sjøulykker, jf. sjøloven § 472a fjerde og femte ledd [52],
b) alvorlige ulykker, jf. sjøloven § 472a første ledd,
c) arbeidsulykke, selv om tilfellet ikke er å anse som en sjøulykke, jf. skipssikkerhetsloven § 47 [53],
d) utslipp eller fare for utslipp av farlige eller forurensende stoffer, selv om tilfellet ikke er å anse som sjøulykke, jf. skipssikkerhetsloven § 34,
e) sabotasje eller piratvirksomhet, jf. skipssikkerhetsloven § 39 og § 47, selv om tilfellet ikke er å anse som en sjøulykke,
f) yrkessykdom, jf. skipssikkerhetsloven § 47, slik det fremgår av den enkelte bestemmelse.


Sjøfartsdirektoratet

Rapport om sjøulykke, arbeidsulykke og nestenulykke

Skipsfører eller rederi er ansvarlig for at rapport om sjøulykke og arbeidsulykke sendes Sjøfartsdirektoratet innen 72 timer etter hendelsen. Les mer om rapportering av ulykker på skip her:

Skjemaet sendes: post@sdir.no
Postadresse: Sjøfartsdirektoratet, Pb 2222, N-5509 HAUGESUND, Norway

Del A. Generelt

Fartøyets navn: | Kjenningssignal:
Type fartøy: | IMO nr:
Ulykkestidspunktet dato(d:m:år): | klokkeslett(lokal tid):
Posisjon ved ulykkestidspunktet: (Nord/Sør) (Øst/Vest) Stedsnavn:
Geografisk område: | Type farvann:
Kontaktperson:
Telefon: | E-post:

Hva har skjedd? Gi en kortfattet beskrivelse av hendelsesforløpet før, under og etter ulykken:

Fortsett eventuelt på side 5 (Del K)

Konsekvenser (kryss av så mange som nødvendig):

tap av liv	personskade	ingen personskade
fartøy tapt eller forlatt	fartøy/utstyr skadet	ingen skade på fartøy
forurensing	last/eiendom skadet	ingen forurensing
nestenulykke med fare for liv, store materielle skader eller alvorlig forurensing.		

KS-0197 B - norsk Side 1 av 5

Figur 20 Rapporteringsskjema Sjøulykker. Kilde Sjøfartsdirektoratet

Forskriften gjelder for:

a) Norske skip, herunder flyttbare innretninger, fiskefartøy og fritidsbåter.
b) Utenlandske skip:
    1. Ved sjøulykke i norsk territorialfarvann.
    2. Ved utslipp, eller ved fare for utslipp av olje, farlige eller forurensende stoffer i norsk territorialfarvann, herunder territorialfarvannet rundt Svalbard og Jan Mayen og i norsk økonomisk sone.

For roroferger og hurtiggående passasjerfartøy som går i rutetrafikk til eller fra norsk havn til havn i en EØS-stat, gjelder forskriftens bestemmelser også når sjøulykken inntreffer utenfor norsk sjøterritorium, dersom Norge var den siste EØS-staten skipet besøkte før ulykken.

Forskriften gjelder ikke for militære fartøyer, unntatt som nevnt i første ledd bokstav d, samt ved sjøulykker som ikke bare involverer militære fartøy.

For varsling av akutt forurensning eller fare for akutt forurensning kommer forskrift 9. juli 1992 nr. 1269 til anvendelse.

Med basis i innrapporterte hendelser så sender Sjøfartsdirektoratet ut jevnlig informasjon om "læring av hendelser" med utgangspunkt i ulykker og hendelser. Eksempelvis har Sjøfartsdirektoratet fått rapportert en del ulykkesrapporter med årsaken "sovnet på vakt". Det har som oftest gått bra med mannskapet om bord, men noen fartøy har forlist, fått store materielle skader, eller ulykken har ført til miljøutslipp. Smakebiter fra rapporten er som følgende:

> ***Hva har skjedd?***
> "Fører sovnet…..» «….styrmann sovnet på vakt…» «…sovnet ved roret…» «…besetningsmedlemmet sovnet ved roret…» «…båtfører sovnet på veg til oppdrag…» «…autopilot har vært på og jeg har sovnet…» «…grunnstøtt pga. fører sovnet på vakt og utkikk var gått ned fra broa for å vaske i messa/byssa…» «…rorvakten sovnet…» «…vakthavende sovnet…» «…sovnet før han ankom lokaliteten og våknet av at han traff land…» og «…én person på brua og den personen sovnet."

Opplistingen er hentet fra et utvalg ulykkesrapporter siste året, og oppgitt som årsak til at fartøy gikk på grunn. I de tilfellene vi får rapporter med årsak "sovnet på vakt", har det som oftest gått bra med mannskapet om bord, men noen fartøy har forlist, fått store materielle skader, eller ulykken har ført til miljøutslipp.

Årsaker

Noen sovnet etter en lang seilas og vakt, gjerne på slutten av vaktperioden, mens andre nylig startet sin vakt. Det å være tilstrekkelig uthvilt beror ofte på hva en har brukt hviletiden til, og om kvaliteten på hviletiden er god. Hviletid og vakter som er preget av støy, vibrasjon, lite søvn eller forstyrrelser, kan føre til at brovakta blir krevende å gjennomføre. Tid på døgnet og rett brobesetning har også en betydning.

Avtagende dagslys, monotone oppgaver og lite som skjer, dårlig luftkvalitet på broa, lange vakter, eller feil bruk av tekniske hjelpemidler med redundans-funksjon (eks.: brovaktsalarm), kan være andre årsaker. Lista med direkte og bakenforliggende årsaker kunne vært lenger, resultatet er «sovnet på vakt».

Tiltak

Ulike tiltak er lovpålagt, eller krever en vurdering gjort av rederi og mannskap om bord. Tiltak kan være brovaktsalarm, brovakt i henhold til sjøveisregler og vaktholdsforskriften, rett bemanning, o.l. Listen er lang over ulike tiltak som skal hindre at noe går galt, og at noen sovner på vakt. Den enkelte som har tjeneste om bord må også, uavhengig av lover og regler, se til at kvaliteten på hviletiden er god før ny vaktperiode. God planlegging av arbeids- og hviletid, gir sikrere vakter, og bedre hvile og nødvendig søvn.

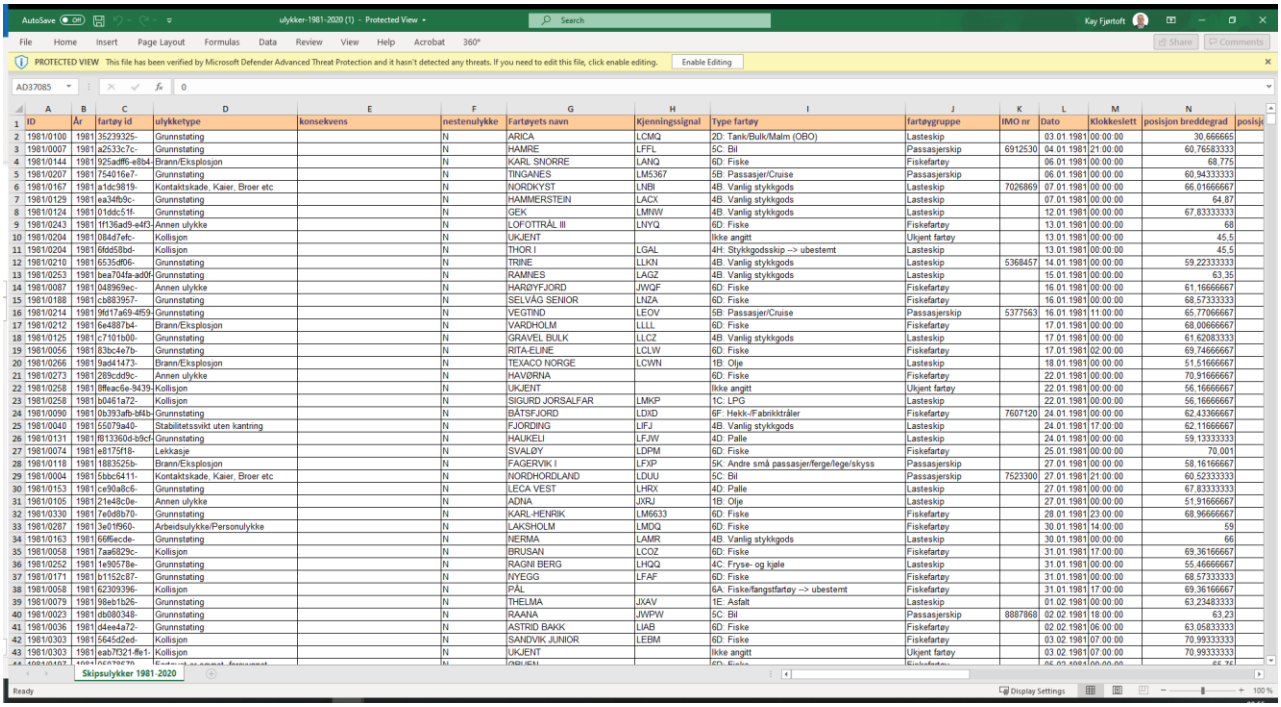
Mer informasjon om læring fra hendelser ligger her:

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

Sjøfartsdirektoratet har sammen med Kystverket utarbeidet forslag til maritim strategi for digital sikkerhet. Etatene kommer med flere konkrete anbefalinger, inkludert etablering av nasjonalt responssenter. Link til mer informasjon om dette finnes her, hvorav en av rapportene som pekes mot er SINTEFs trusselvurdering i forbindelse med strategi for maritim digital sikkerhet:

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

Sjøfartsdirektoratet bruker data fra innrapporterte ulykker til å lage ulykkesstatistikker. Disse publiseres gjerne etter seks måneder og ved årsslutt. Det finnes også en ulykkesstatistikk for fritidsfartøy.



ID	År	fartøy id	ulykketype	konsekvens	nestenulykke	Fartøyets navn	Kjenningssignal	Type fartøy	fartøygruppe	IMO nr	Dato	Klokkeslett	posisjon breddegrad
1981/0100	1981	35239325-	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	LFFL	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	a1dc9819-	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-a4f3-	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	6fdd58bd-	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	65,77666667
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	289cdd9c-	Annen ulykke		N	HAVØRNA		6D: Fiske	Fiskefartøy		22.01.1981	00:00:00	70,91666667
1981/0258	1981	8ffeac6e-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	e8175f18-	Lekkasje		N	SVALØY	LDPM	6D: Fiske	Fiskefartøy		25.01.1981	00:00:00	70,001
1981/0118	1981	1883525b-	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	5bbc5411-	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
1981/0105	1981	21e48c0e-	Annen ulykke		N	ADNA	JXRJ	1B: Olje	Lasteskip		27.01.1981	00:00:00	51,91666667
1981/0330	1981	7e0d8b70-	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	66f6ecde-	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	98eb1b26-	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	8887868	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	5645d2ed-	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

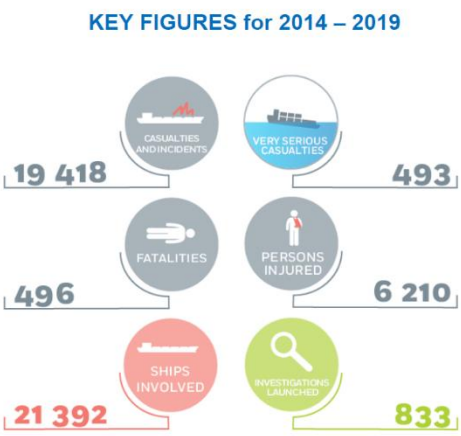
Figur 21 Ulykkesstatistikk. Kilde: Sjøfartsdirektoratet

C.2.5 EMSA

EMSAs oppdrag er å tjene EUs maritime interesser for en trygg, sikker, grønn og konkurransedyktig maritim sektor og fungere som et pålitelig og respektert referansepunkt i den maritime sektoren i Europa og over hele verden.

EMSA arbeider med maritim sikkerhet, sikkerhet, klima, miljø og indre markeds spørsmål og oppgaver, først som en tjenesteleverandør til medlemsstatene og Kommisjonen, men også som en innovativ og pålitelig partner og kunnskapshub for den europeiske maritime klyngen og potensielt utover en referanse internasjonalt.

Artikkel 1 i EMSAs stiftelsesforordning sier at formålet med byrået er å sikre et høyt, enhetlig og effektivt nivå av maritim safety and security, forebygging av og respons på forurensning forårsaket av skip samt respons på marin forurensning forårsaket av olje- og gassinstallasjoner og, der det er hensiktsmessig, å bidra til den totale effektiviteten av sjøtrafikk og sjøtransport for å lette etableringen av et europeisk sjøtransportrom uten barrierer.

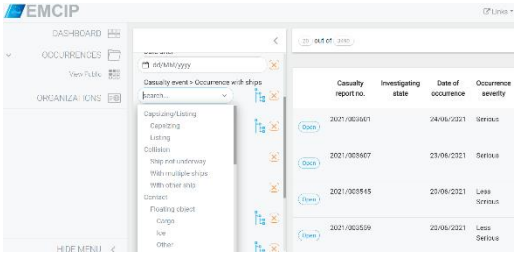


Figur 22 EMSA hovedstatistikk over ulykker 2014-19. Kilde EMSA

2019 var et positivt år med tanke på forbedring eller stabilisering av noen indikatorer, for eksempel antall tapte skip, omkomne og skadde. Det ble rapportert om 3062 hendelser i 2019. Det ble registrert en reduksjon på 200 omkomne sammenlignet med året 2018. Det totale antallet hendelser som er lagret i EMCIP-databasen har vokst til 19500 i løpet av 2014-2019. Dette representerer et gjennomsnitt på 3236 marine tap eller hendelser per år i løpet av perioden.

Totalt 106 veldig alvorlige tap rapportert i 2018, som tilsvarte en økning på 68% sammenlignet med 2017, mens det totale antallet falt tilbake til 63 i 2019. En lignende utvikling angående antall tapte skip ble notert: etter en topp i 2018 ble en nedgang i 2019 registrert, med 21 skip tapt.

I løpet av perioden 2014-2019 resulterte 320 ulykker i totalt 496 menneskeliv tapt. Etter en kontinuerlig viktig nedgang fra 2015 til 2017 ble det registrert en begrenset økning for årene 2018 og 2019. 88,3% av ofrene var besetningsmedlemmer. Dødsfall skjedde hovedsakelig under kollisjoner. Når begivenheten er begrenset til personer, var fall den viktigste årsaken til tap av liv. Hovedhendelsen som resulterte i omkomne var kollisjoner når det var relatert til et skip og falt når det var relatert til personer. I perioden 2014-2019 ble det registrert 6210 skader, tilsvarende 5424 ulykker. Besetningsmedlemmer er hovedkategorien for personer som er skadet til sjøs med 79.3% av ofrene.



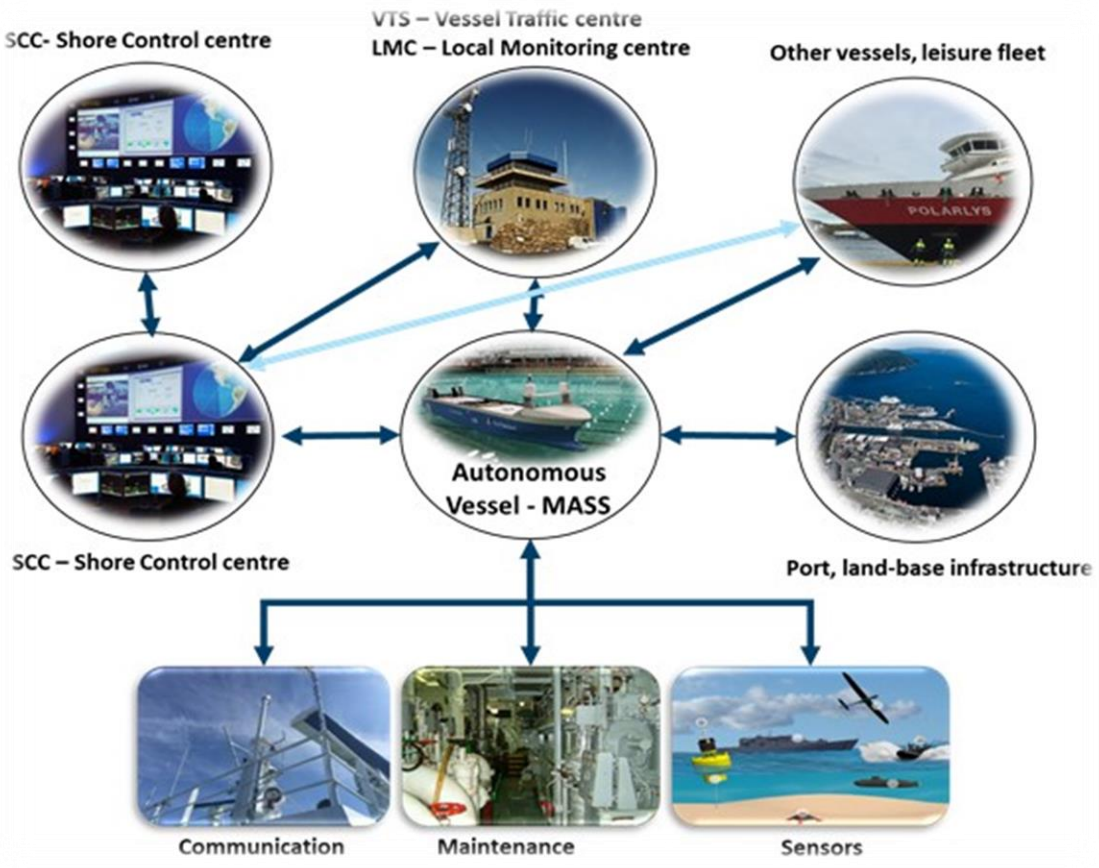
Figur 23 EMCIP database. Kilde EMSA

EMCIP står for European Marine Casualty Information Platform, og er en sentralisert database for EU-medlemsstater for å lagre og analysere informasjon om havarier og hendelser til havs. EMCIP er fylt med data av kompetente nasjonale myndigheter. Det er disse dataene som danner grunnlaget for den årlige oversikten over sjøulykker og hendelser. Ved å søke opp i databasen får man også tilgang til hendelsesrapportene. Linken til databasen er:
https://portal.emsa.europa.eu/emcip-public/#/dashboard

C.3 Rapportering autonome fartøy

C.3.1 Informasjonsflyt autonome fartøy

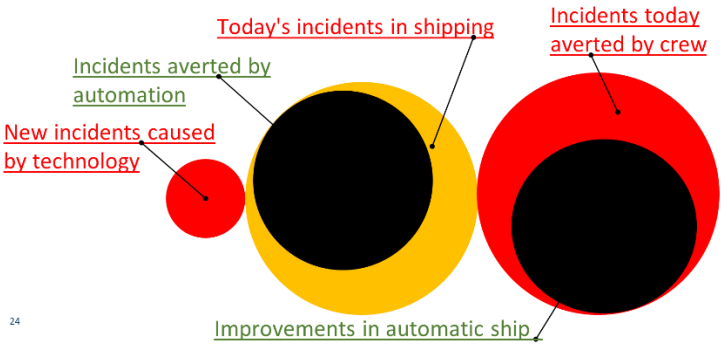
Figur 24 viser hvem som trenger informasjon fra et autonomt fartøy. Til høyre i figuren så har vi et kontrollsenter som er skipets ansvarlige og som også har ansvaret for å utveksle informasjon med andre kontrollsenter, med VTS'er, og med øvrig trafikk som påvirker en seilas. Et fartøy må enten direkte eller indirekte via kontrollsenteret utveksle informasjonen med havner og myndigheter som trenger denne informasjon både for å ivareta sikkerhet, så vel som for å kunne styre trafikken inn til havn. Under MASS fartøyet så vises noen sensorer som er nødvendig for at et autonomt fartøy kan seile trygt. Eksempelvis så vil navigasjonssensorer være avgjørende, som kan være sensorer som ligger i farleden, så vel som sensorer som møter skipet når det legger til kai. Dette kan også være rapportert vær som benyttes til å beregne fartøyets kapabiliteter. Kommunikasjon er avgjørende for at data skal sendes mellom fartøy og land, samt for innhenting av data til navigasjonsformål, og ikke minst avgjørende dersom fartøyet skal styres fra et kontrollsenter.



Figur 24 En maritimt autonomt verdikjede. Kilde SINTEF

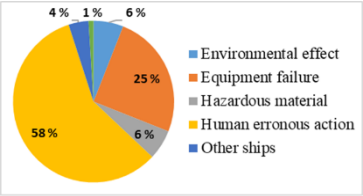
C.3.2 Nye hendelser ved autonomitet

Figur 25 viser forventet utvikling når gjelder innføring av autonomitet innen maritim shipping. Helt til venstre så viser den røde sirkelen at vi forventer at det vil komme nye hendelser ved innføring av autonomitet. Type hendelser og konsekvens er fortsatt i stor grad ukjent da vi har begrenset bakgrunnsdata ennå. Den oransje sirkelen er ulykker som er i dag med konvensjonell shipping, mens den svarte sirkelen indikerer forventet reduksjon som følge av innføring av autonomitet. Helt til høyre så forteller den røde sirkelen antall ulykker som i dag er forhindret grunnet mannskapets tilstedeværelse, mens den sorte sirkelen er det vi forventer at automasjonen selv kan forhindre i sammenheng med dagens hendelser som er avverget av mannskapet om bord.



Figur 25 Ulykkestyper autonomitet. Kilde SINTEF

Erfaring fra ulykkesscenarioer med konvensjonell shipping viser at utstyrsfeil utgjør nesten en fjerdedel av ulykkestallene. Tallene viser videre at en høy grad av ulykkene skylder menneskelige faktorer.



Figur 26 EMPIC (EMSA 2018). Kilde EMSA

Vi har videre gjort studier på disse tallene, hvor vi har vurdert forskjellig grad av autonomitet og satt dette opp mot noen utvalgte effekter. Vår sammenligning belyste autonomitetsgradene full autonom, delvis autonom, betydningen av kontrollrom, betydning av høy grad av teknisk resilience, samt betydningen av å ha mer kvalitet i planene forbundet med en seilas. Vi har antydet hva autonomitet vil bety i form av nye ulykker som kan oppstå grunnet autonomitet, sammenligning bildet opp mot dagens ulykkesbilde, samt hvilke som kan forhindres med en høyere grad av autonomitet. Fargekoden betyr grønn=bedre, rød=forventet negativ effekt.

Som en videre forklaring så kan eksempelvis innføring av full autonomitet ha følgende betydningsfulle effekter:

- Høyere krav til bruk av sensorer, automatisering og landkontroll fører til at operatørene i et kontrollsenter kan miste noe av situasjonsforståelsen for både miljø, skip og til den tekniske ytelsen til systemene om bord i fartøyene.
- Mye lavere eksponering for fare for mannskapet.
- Et fartøy uten mannskap gjør det vanskelig å inspisere utstyr eller systemer som rapporterer feil eller problemer.
- Ved fjerning av sårbar teknologi vil faren for brann bli redusert, eksempelvis grunnet reduksjon av teknologi forbundet med mannskapskomfort som bysse, vaskeri og avfallssystemer. Dette er utstyr som har en relativt høy risiko for brann på bemannede skip.

	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

Figur 27 Effekter på type begrensninger. Kilde SINTEF

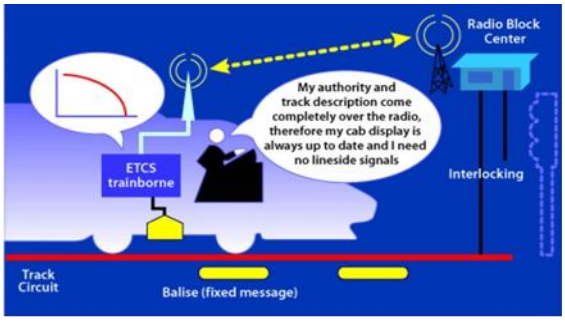
D Jernbane

D.1 European Rail Traffic Management System (ERTMS)

Det pågår utskifting og modernisering av signalanleggene på den Norske jernbanen. Dagens signalteknologi erstattes med ERTMS (European Rail Traffic Management System), et digitalisert signalsystem som blir felles for hele Europa og skal ivareta samtrafikkevnen. ERTMS baserer seg på teknologiske løsninger som legger til rette for mer automatisering og er et fundament for selvkjørende tog i fremtiden. Systemet vil umiddelbart bidra til å effektivisere togfremføring og gi mulighet for økt kapasitet på jernbanen gjennom bedre utnyttelse av sportilgang. Samtidig ivaretas hensynet til sikkerheten gjennom kontinuerlig hastighetsovervåking. Dagens signal- og kontrollanlegg består av ATC (Automatic Train Control) i kombinasjon med utvendige lyssignaler langs sporene som gir informasjon til togfører. Med ERTMS vil informasjon til togfører og kjøretillatelse bli sendt direkte til en datamaskin i togets førerpanel (ETCS) gjennom jernbanens eget mobilnett (GSM-R). Togfører har fortsatt kontrollen, men om denne kjører for fort eller bremser for sent, vil togets datamaskin overta og bremse toget til rett hastighet, eller til full stopp. Automatiseringen, og den mer integrerte løsningen i toget som ERTMS innebærer reduserer derfor mulighetene for menneskelige feil. Samtidig vil konsekvensene av menneskelige feil reduseres ved at automatikken (hastighetsovervåkning) tar over.

ERTMS som system består av følgende:

- ETCS (European Train Control System-hastighetsovervåkning og signalering)
- GSM-R (for kommunikasjon mellom tog og signalanlegg)
- Felles europeiske trafikkregler



ETCS datamaskin i tog

ETCS førerpanel i tog

Figur 28 ERTMS-prinsippet

ETCS vil som følge av ERTMS-implementeringen i Norge og ellers i Norden erstatte dagens ATC-system. I en overgangsfase vil imidlertid begge systemene være i drift. Når da et tog med ETCS en periode også skal kunne kjøre på strekninger med ATC må det utrustes med en såkalt STM (Specific Transmission Module). Denne enheten oversetter informasjon fra ATC-systemet til et språk det nye ETCS-systemet forstår. På denne måten kan ETCS tas i bruk gradvis.

Ved overgang fra dagens ATC til ERTMS (med ETCS og GSM-R) må trafikkreglene også justeres noe grunnet andre egenskaper ved ERTMS, spesielt ved avvikssituasjoner. Den største forskjellen ved overgang til ERTMS er at både signalanlegget og toget vil innta samme kjøremodi.

De mest vanlige kjøremodi i ERTMS er:

- FS (Full Supervision): Kjøretillatelse med strekningens tillatte hastighet
- OS (On-Sight): Kjøretillatelse med hastighetsbegrensning

- SH (Shunting): Kjøretillatelse for "togskifting" med hastighetsbegrensning
- SR (Staff responsible): Tillatelse til å kjøre med hastighetsbegrensning når kjøretillatelse i FS/OS ikke kan gis grunnet feil i tog eller infrastruktur.

D.2 Rapporteringssystem, innsamling og klassifisering

Forskrift om sikkerhetsstyring for Jernbanevirksomheter, §7-2 [54] krever bl.a. at virksomheten *skal ha system for intern rapportering, registrering, granskning og analyse av jernbaneulykker, alvorlige jernbanehendelser og jernbanehendelser*.

Manuell rapportering av hendelser, og tilløp til hendelser i jernbanen gjøres i dag i ulike systemer. Relevante systemer i denne sammenheng er "Synergi" "TIOS" og "AT-melding". Dette er registreringer av avvik- og sikkerhetsrelaterte hendelser i Bane NOR. Synergi er et kjent HMS&K-rapporteringssystem som er i almen benyttelse i ulike virksomheter/bransjer. I TIOS (Trafikkinformasjon- og Oppfølgingssystem) lagres planlagte og faktiske togtider samt årsak til forsinkelse/innstillinger. I dette systemet rapporteres årsaken til forsinkelser/innstillinger fordelt på ulike årsakskategorier/koder inndelt etter type aktør/forhold. Noen relevante koder knyttet til togfremføring og signal finnes i tabellen nedenfor (jfr. Bane NOR: Avtale om sportilgang-AST, Vedlegg 4). Disse kodene benyttes av infrastruktureier og jernbaneforetak.

Tabell 17 Årsakskoder i TIOS.

Kode nr. og navn	Forklaringer
Kode 2 – Sikringsanlegg, signalanlegg og fjernstyring	«Trafikkstyrer får ikke stilt signal». Feil på linjeblokk, pærekontroll, stillverk/fjernstyringsanlegg, ATC-balise, vegsikringsanlegg, rasvarslingsanlegg. Sporveksel ikke i kontroll. Utilsiktet passering av signal i stopp grunnet teknisk feil ("signalfall"). Sporfeltbelegg inkl. saltbelegg. Feil ved nødstrømsanlegg.
Kode 4 – Tele og transmisjonsfeil	Tele- og transmisjonsfeil som fører til driftsforstyrrelser. Feil ved GSM-R-systemet. Feil ved høyttaler/anviser. Feil på FIDO kommunikasjon.
Kode 6 - Kjøretøy med feil sperrer spor/blokkstrekning	Benyttes på forsinkelser som oppstår for et tog når et annet, havarert tog/tog med feil sperrer linjen. Nyttes også dersom enkeltsporet drift må iverksettes grunnet dette. Skal benyttes selv om havarert tog/ tog med feil på kjøretøyet har begynt å kjøre igjen. Når linjen er klar for trafikk, men togleder velger å holde tilbake et motgående tog i påvente av kryssing, skal dette toget ha Kode 7 (Trafikkavvikling). Havarert tog / toget med feil skal ha Kode 81 (Feil på kjøretøy).
Kode 7 - Trafikkavvikling	Helhetsvurderinger gjort av trafikkstyrer vedrørende rekkefølge/valg av kryssingssted, konstruksjons/systemfeil i ruteplan. Årsaker i forhold til trafikkstyring: Signal stilles for sent, får ikke meldt tog til betjent stasjon, køkjøring, overbelastet banestrekning, feil i hjelpesystem FJS (Automat/ ATL/TLS). Bane NORs personale bruker FIDO-systemet feil.
Kode 81 – Feil på kjøretøy	Alle feil ved kjøretøy som medfører stans eller redusert kjørehastighet. Lastforskyvning på godstog. Feil på ombordutrustningen til FIDO eller ved feil på ombordutrustningen til ERTMS.

AT-melding benyttes i Bane NOR når det er "*Feil på infrastruktur som påvirker mer enn ett tog*" og når "*Stoppende tog påvirker andre*". Dette er m.a.o. også meldinger av relevans for trafikkstyring, og dette systemet bidrar til å formidle informasjon raskere ut til togselskapene parallelt med trafikkstyringssentralen. Når situasjonen er normalisert, og driftsforstyrrelsen opphørt, sendes en ny AT-melding om at problemet er opphørt. Denne vises på skjerm i 20 minutter før den fjernes. I tillegg til nevnte systemer har Bane NOR en varslingskanal for varsling av kritikkverdige forhold. Her kan medarbeidere i jernbaneforetaket, leverandører, kunder og samarbeidspartnere varsle om bl.a. forhold som innebærer fare for liv og helse.

Om det er behov for, om det eksisterer, eller planlegges nye systemer for registreringer av (sikkerhetsrelaterte) hendelser knyttet til automatiserte systemer som ERTMS er foreløpig uklart. Det uttales

på Bane NORs hjemmesider følgende: "*ERTMS gir oss blant annet økt sikkerhet gjennom tekniske barrierer og kontinuerlig overvåkning av alle tog, økt punktlighet grunnet færre feil og automatisk håndtering av avvik. Over tid vil systemet kunne gi økt kapasitet med automatisk kjøring av tog samt dynamisk avstand mellom togene.* "

Med ERTMS-implementeringen arbeides det parallelt med prosedyrer og instrukser i Bane NOR og hos togoperatørene for å ta i bruk systemene. Her kan det tenkes at det planlegges nye rutiner for deteksjon og registrering av hendelser fra de digitale systemene.

En serie IEC-standarder stiller krav til ombordsystem for kontinuerlig innsamling, lagring og bruk av audiovisuell informasjon (lyd- og videoopptak) fra førerhuset ved kjøring av tog. Dette går under betegnelsen «On-board Driving Data Recording System» (forkortet ODDRS). IEC 62625-1:2013 [35] og IEC 62625-2:2016 [55] omhandler systemspesifikasjon og krav til samsvarstesting av slike systemer som kan refereres til i regelverket. IEC TC-9 har nå på gang IEC NP 62625-3 som skal komplettere del 1 og 2 av IEC 62625. Her stilles tilleggskrav til lyd- og videoopptak som kan benyttes i forbindelse med undersøkelse av faktiske manøvrer fra førerhuset under en hendelse eller ulykkeshendelse, men også for observasjon av fører når dette kreves i andre sammenhenger. Slike lyd- og videoopptak skal kunne gjengi følgende:

- Hva togfører har sagt
- Hva togfører burde ha hørt
- Hva togfører kunne ha sett, og
- Hvilke handlinger togfører utførte i den gitte situasjonen

Den nye standarden IEC 62625 vil stille krav til innhenting, lagring og fremvisning av slike lyd- og videoopptak fra førerhuset, samt videoopptak av utsyn fra frontvinduet i lokk-kabinen. Følgende opptak er aktuelle:

- Samtaler togfører har via (kablet) interkommunikasjon
- Video av jernbanesporet sett fremover ut fra førerhuset
- Omgivelseslyd og stemmer ellers i førerhuset
- Video av togførerens kontrollpanel(er)
- Video med oversikt over førerhuset ellers

IEC 62625-3 vil ta i betraktning at 1) nasjonale krav eller regionale forskrifter, arbeidsavtaler osv. kan begrense hva slags lyd- og videoopptak som er tillatt, og 2) at det ikke er påkrevd å gjøre opptak av alt av lyd- og visuelle observasjoner.

Merk: I sammenheng med granskning av hendelser krever IEC 62625-1 [35] at ODDRS kontinuerlig skal registrere informasjon på et *sikret* lagringsmedium med en minimumskapasitet på 24 timers opptak. For observasjon / «audit» av fører over tid er kravet å registrere hendelsene kontinuerlig på et *ordinært* lagringsmedium med en minimumskapasitet på 8 dagers opptak.

D.3 Aktørbildet og rammevilkår for rapportering

Det er de ansvarlige i jernbaneforetakene selv sammen med leverandører og trafikksentralene som rapporterer hendelser knyttet til signal og kjøring av tog. Trafikksentralene vil ha totaloversikt mht. trafikkstyring, mens de HMS- og kvalitetsansvarlig hos foretakene vil ha oversikten over sikkerhetsrelaterte hendelser hos enkeltaktørene.

Det vil trolig også være en del av opplæringen ved implementering av ERTMS å få innføring i gjeldende prosedyrer og rutiner for deteksjon og registrering av hendelser/feilhendelser for de digitale systemene som tas i bruk.

E Kraftforsyning

E.1 Leveringspålitelighet

NVE og systemansvarlig stiller en rekke krav til registrering og rapportering av feil og avbrudd (se FASIT | Statnett

Ved hjelp av FASIT programvare kan feil- og avbruddsstatistikk i totalnettet registreres.

Formålet med FASIT er å fremskaffe informasjon om leveringspåliteligheten i det norske kraftsystemet, både informasjon om historisk leveringspålitelighet og informasjon for å estimere fremtidig forventet leveringspålitelighet.

I FASIT registreres informasjon om:

- driftsforstyrrelser (automatisk utkobling, påtvungen utkobling og utilsiktet utkobling)
- planlagte utkoblinger som har medført avbrudd (både planlagt varslet utkobling og planlagt ikke varslet utkobling)

Driftsforstyrrelser (hva er feil, hvor er det feil, og hvorfor er det feil) dekker et komponent- og systemfokus, mens avbrudd for rapporteringspunkt (inkl. avbrutt effekt, avbruddsvarighet, ILE og KILE) dekker et sluttbrukerfokus.

Feil som skal registreres i FASIT er feil som har innledet eller utvidet en driftsforstyrrelse. Det medfører at enkelte "trivielle" feil blir registrert fordi de (tilfeldigvis) medførte en driftsforstyrrelse, mens enkelte "alvorlige" feil ikke blir registrert fordi de ble oppdaget og håndtert før feilen resulterte i en driftsforstyrrelse.

Det forutsettes at alle feil uansett årsak og konsekvens håndteres i andre av konsesjonærenes systemer, f.eks. i et vedlikeholdssystem.

E.2 IKT-sikkerhet

I utgangspunktet var NVE utpekt som sektorvist responsmiljø for kraftsektoren, men de har siden 2018 delegert denne oppgaven til KraftCERT.

I sin rapport om NVEs arbeid med IKT-sikkerhet i kraftforsyningen, påpeker Riksrevisjonen at det er "svakheter ved selskapenes evne til å oppdage IKT-hendelser og underrapportering" [7].

KraftCERT bekrefter at de deler informasjon om hendelser til sine kunder/medlemmer både i form av Structured Threat Information eXpression (STIX) via Trusted Automated eXchange of Indicator Information (TAXII) , samt på kryptert Internet Relay Chat (IRC). Imidlertid er det relativt lite som tilflyter KraftCERT fra medlemmer/kunder, størstedelen av informasjonsstrømmen om angrep og kompromitteringsindikatorer er enveis fra KraftCERT.

Det finnes en rekke alternative verktøy for informasjonsdeling, inklusive MISP og HIVE, men det største problemet er at man ikke har klart å bli enige i bransjen om en standard. Per i dag deles informasjon om hendelser etc. like gjerne i form av PDF-dokumenter.

Det er mye som tyder på at flere av aktørene i kraftbransjen deltar i NSMs Varslingssystem for Digital Infrastruktur (VDI), men dette er ikke offentlig tilgjengelig informasjon. Basert på det som er kjent, kan man

slutte at NSM har utplassert inntrengningsdeteksjonssensorer hos deltakerne, slik at angrepsforsøk automatisk kan meldes tilbake til NSM. Vi kan imidlertid anta at VDI ikke er opptatt av dagligdagse hendelser, men heller fokuserer på mer fundamentale ting som avanserte persistente trusler (APT).

Automatisering av varsling er også et stort poeng for KraftCERT, og de jobber med et eget sensorprosjekt for sine medlemmer. Leverandørene Claroty, Nozomi Networks og tidligere CyberX (nå Azure Defender for IoT) har utstyr som sitter inne i OT-nettverkene, og oppdateres automatisk med feed fra leverandører som ABB, Siemens (og mange andre). Kan dermed få automatisk liste over aktiva, programvareversjon etc.

Utover rapportering til sektorvist responsmiljø, finnes det også en europeisk Information Sharing & Analysis Centre (ISAC) for energibransjen, European Energy ISAC (EE-ISAC), som foretar proaktiv informasjonsdeling av kompromitteringsindikatorer osv., og bidrar til analyse av hendelser i ettertid. KraftCERT er registrert som partner av EE-ISAC. Det finnes også en amerikansk søsterorganisasjon, E-ISAC.

F Vann- og avløpssektoren

VA-sektoren omfattes ikke generelt av NIS-direktivet [56], kun VA-verk over en viss størrelse (dvs. som dekker et visst minimum antall innbyggere) er med. I Norge er det derfor kun Oslo VAV som faller inn under NIS-direktivet.

Oslo VAV er medlem av KraftCERT, men sender i utgangspunktet ikke varsler om hendelser til dem. Det er Mattilsynet som er tilsynsmyndighet for VA-verk, men så langt er det kun hendelser som er relatert til vannkvalitet som rapporteres til dem.