



Universitetet
i Stavanger

DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

MASTEROPPGAVE

Studieprogram/spesialisering: Samfunnssikkerhet	Vårsemesteret, 2019 Åpen
Forfatter: Mads Lindberg	 (signatur forfatter)
Fagansvarlig: Ole Andreas Hegland Engen Veileder(e): Kenneth Arne Pettersen	
Tittel på masteroppgaven: Digitalisering i sikkerhetsarbeidet – En studie av hvordan digitale sikkerhetsinformasjonssystemer kan bidra til resiliens i petroleumsnæringen Engelsk tittel: Digitalization in safety - A study of how digital safety management systems can contribute to resilience in the petroleum industry	
Studiepoeng: 30	
Emneord: Resilience Engineering, Resiliens, Resilience Assessment Grid, Digitalisering, Sikkerhetsinformasjonssystem, Petroleumsindustrien, Monitorering, Sikkerhet, Sikkerhetsstyring, Indikator, kunnskap, kunnskapsoverføring, Lundin Norway	Sidetall: ... 83 + vedlegg/annet: ... 7 Stavanger, ... 15.06.2019 .. dato/år

Forside for masteroppgave

Det teknisk-naturvitenskapelige fakultet



Universitetet
i Stavanger



Digitalisering i sikkerhetsarbeidet –

En studie av hvordan digitale sikkerhetsinformasjonssystemer kan bidra til resiliens i petroleumsnæringen

Mads Lindberg

Master i Samfunnssikkerhet

Våren 2019

Forord

Denne masteroppgaven markerer slutten på fem år med studier av samfunnssikkerhet, og to spennende år ved Universitetet i Stavanger. Arbeidet med masteroppgaven har vært en lærerik og utfordrende prosess, og det har derfor vært et stort privilegium å ha de sterke fagmiljøene ved UiS og Lundin i ryggen underveis i prosjektet

Jeg ønsker å rette en stor takk til Lundin, og de ansatte ved HSEQ-avdelingen som har gjort denne oppgaven mulig. Kontaktpersoner og informanter har vist stor tålmodighet og åpenhet ved å ta seg tid til å diskutere og svare på spørsmål helt ned på detaljnivå. En spesiell takk til Bjørn for oppfølging og innspill underveis i prosjektet.

Jeg ønsker også å rette en stor takk til min veileder Kenneth Pettersen, for gode innspill og diskusjoner underveis i prosjektet. Disse diskusjonene har vært til stor hjelp og gitt meg muligheten til å se prosjektet fra nye perspektiver.

Sist, men ikke minst vil jeg takke Christer, Damian, Lisa og Øyvind for lån av gjesterom under mine opphold i hovedstaden. En spesiell stor takk til Lisa for korrekturlesing og gode råd underveis i prosjektet. Jeg vil også takke Mamma og Pappa, for moralsk støtte det siste halvåret og Kine for korrekturlesing i sluttspurten av prosjektet. I likhet med oppgavens tematikk har også jeg som forsker tilegnet med mye kunnskap underveis, og jeg ser frem til å benytte denne i arbeidslivet.

Stavanger 15.06.2019

Mads lindberg

Sammendrag

Digitaliseringen har blitt beskrevet som den fjerde industrielle revolusjon, og vil i de neste årene kunne medføre en rekke endringer i petroleumsnæringen. Som et motsvar til sosio-tekniske systemers økende kompleksitet har «Resilience engineering» blitt presentert som sikkerhetslitteraturens løsning til et økende behov for nye metoder innenfor sikkerhetsstyring. Med utgangspunkt i perspektiver fra «Resilience engineering» retter dette forskningsprosjektet søkelyset på hvordan digitale sikkerhetsinformasjonssystemer kan bidra til resiliens i Lundin Norway. Basert på antakelsen om at «Resilience engineering» kan være en løsning på fremtidige utfordringer tilknyttet økt kompleksitet, er formålet med dette prosjektet å kartlegge hvorvidt digitale systemer for kunnskapsoverføring i Lundin Norway kan bidra for resiliens.

Resultatene viser at Lundin i stor grad har høy sikkerhet både i digitale programvarer, systemer og kompetente arbeidstakere. For at disse ressursene skal kunne bidra til resiliens vil det samtidig kreves målsetninger som avviker fra tradisjonell og reaktiv sikkerhetsstyring. Flere av disse målsetningene er i dag synlige i form av selskapets fokus på bruk av ledende indikatorer og kunnskapsinnhenting fra daglige hendelser uten negative utfall. Dette kan hevdes å være viktige forutsetninger for resiliens. Det er samtidig en utstrakt bruk av reaktive indikatorer i selskapet, og synlige utfordringer tilknyttet tilgjengeliggjøring og distribuering av kunnskap. Dersom «Resilience engineering» er en retning Lundin ønsker å sikte mot, bør sikkerhetsinformasjonssystemer videreutvikles slik at de i større grad legger til rette for distribuering og tilgjengeliggjøring av kunnskap. Det bør også rettes et søkelys mot dagens utstrakte bruk av reaktive indikatorer, og foretas en vurdering om å i større grad integrere bruk av ledende indikatorer inn i dagens systemer, planverk, og målsetninger. Effektivisering som følge av digitalisering må ikke gå på bekostning av sikkerhet, og det bør utøves et kontinuerlig fokus på systemene og antakelsene som skjuler seg bak forenklete visualiseringer. Dersom «Resilience engineering» kan være en løsning på fremtidige utfordringer, vil dette behovet øke i takt med den økende kompleksiteten som digitalisering kan medføre de neste årene.

Innholdsfortegnelse

Forord.....	2
Sammendrag	3
Forkortelser og begreper	6
Figurer og tabeller	7
1.0 Innledning.....	8
1.1 Problemstilling og forskningsspørsmål	12
1.2 Avgrensning	13
1.3 Oppgavens oppbygning og struktur.....	14
2.0 Kontekst	15
2.1 Lundin Norway.....	15
3.0 Teori	18
3.1 Resiliens	18
3.1.1 Resilience engineering.....	20
3.1.2 Hollnagels fire egenskaper	21
3.1.3 RAG - «The Resilience Assessment Grid»	24
3.2 Indikatorer og funksjoner	28
3.3 Sikkerhet og sikkerhetsstyring	30
3.3 Sikkerhetsinformasjonssystemer og struktur.....	31
3.3.1 Kriterier for et sikkerhetsinformasjonssystem.....	32
3.4 Digitalisering, psykologiske- og organisatoriske faktorer.....	33
3.4.1 Digitalisering	33
3.4.2 Psykologiske- og organisatoriske faktorer	35
4.0 Metode.....	37
4.1 Forskningsdesign.....	37
4.2 Forskningsstrategi	38
4.2.1 Intervju som metode	39
4.2.2 Utvalg av informanter.....	40
4.3 Datainnsamling.....	41
4.3.1 Gjennomføring av intervjuene.....	42
4.5 Datareduksjon og dokumentanalyse.....	44
4.6 Styrker og svakheter ved designet	46
4.7 Etske refleksjoner	47
5.0 Empiri og drøfting	49
5.1 F1) Hvordan benyttes digitale sikkerhetsinformasjonssystemer til monitorering av sikkerhet i Lundin Norway?.....	52

5.1.1 Synergi som monitoreringsverktøy	53
5.1.2 Indikatorer og KPI.....	56
5.2 F2) Hvordan benyttes digitale sikkerhetsinformasjonssystemer til systematisering av kunnskap i Lundin Norway?.....	62
5.2.1 Synergi som verktøy for systematisering av kunnskap	62
5.2.2 Granskinger og Synergi.....	66
5.2.3 Digitalisering og visualisering av data	69
5.2.4 Barrierepanelet	69
5.3 F3) Hvordan distribueres kunnskap fra digitale sikkerhetsinformasjonssystemer i Lundin Norway?	77
5.3.1 Lessons Learned.....	77
5.3.2 Synergi som distribusjonsverktøy	81
7.0 Konklusjon	87
8.0 Forslag til videre forskning	92
Litteraturliste.....	93
Vedlegg 1.....	97
Vedlegg 2.....	100
Vedlegg 3.....	102

Forkortelser og begreper

KPI	Key Point Indicator
LNAS	Lundin Norway AS
RE	Resilience engineering
SIS	Sikkerhetsinformasjonssystem
HMS	Helse, Miljø, Sikkerhet
HSEQ	Health, Safety, Environment, Quality

Sikkerhetsinformasjonssystem	System hvor ulykker/nestenulykker registreres, analyseres og blir benyttet som grunnlag for å utvikle og implementere risikoreducerende tiltak (Aven, Boyesen, Njå, Olsen & Sandve, 2004, s. 131).
Sikkerhetsbarriere	Systemer eller funksjoner som skal hindre eller begrense videre utvikling av en faresituasjon (Aven et al, 2004, s. 121).
Kunnskapsoverføring	Evnen til å generere kunnskap, distribuere den i organisasjonen, for deretter å nyttiggjøre den i produkter, tjenester og andre systemer (Nonaka & Takeuchi, 1995, s. 3).
Resiliens	Et uttrykk for et systems ytelse under forventede og uforventede forhold. Slike forhold innebærer både endringer, forstyrrelser og muligheter (Hollnagel, 2017, s. 14-15).
Sårbarhet	Manglende evne til å motstå en uønsket hendelse eller å opprette ny stabil tilstand dersom en verdi er utsatt for uønsket påvirkning (NS 5830, s. 5).
Sikkerhetsstyring	Alle tiltak som iverksettes for å oppnå, opprettholde og videreutvikle et sikkerhetsnivå i overensstemmelse med definerte mål (Aven et al, 2004, s. 67).
Uønsket hendelse	Hendelse som kan utsette en verdi for uønsket påvirkning (NS 5830, s. 2).

Beredskap	Forberedt evne til på kort varsel å kunne øke sikkerhetsnivå, håndtere en uønsket hendelse eller tilstand, eller evne til å gjenopprette tilfredsstillende tilstand etter en uønsket hendelse eller tilstand (NS 5830, s. 3).
Risiko	Uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen (NS 5830, s. 5).
Risikobilde	Tidsavgrenset beskrivelse av en entitets risiko (NS 5830, s. 5).

Figurer og tabeller

Figur 2-1 Utsirahøyden, av Lundin (2019)	16
Figur 2-2 Lundins funn (Rune Endresen, 2015)	16
Figur 3-3 Egendefinert figur basert på FRAM (Hollnagel, 2017, s. 86).....	25
Figur 3-4 Assessment of the potential to respond (Hollnagel, 2017, s. 70).....	26
Figur 3-5 The extended system model (Reiman & Pietikäinen, 2012, s. 1996).	29
Figur 5-6 Visualisering av forskningsspørsmål og problemstilling (Aven et al, 2004, s. 132).....	51
Figur 5-7 Skjermdump av Synergis brukergrensesnitt	53
Figur 5-8 Prosesskart for hendeshåndtering i Lundin Norway, hentet fra APOS	54
Figur 5-9 Egendefinert figur basert på (Reiman & Pietikäinen, 2012, s. 1996).....	58
Figur 5-10 Skjermdump av Synergi med eksempel på tiltaksoversikt.....	63
Figur 5-11 Skjermdump av Synergi og registrerings skjema for hendelse	67
Figur 5-12 Skjermdump av hovedside på barrierepanel	70
Figur 5-13 Skjermdump av barrierepanelets områdeoversikt	71
Figur 5-14 Skjermdump av Bow-Tie i barrierepanelet	74
Figur 5-16 Skjermdump av kategoriseringer etter storulykker i barrierepanelet.....	75
Figur 5-17 Mal Lessons Learned dokument	78
Figur 5-18 Prosessbeskrivelse for utarbeidelse og distribusjon av Lessons Learned.....	79
Tabell 3-1, Safety-I og Safety II, basert på Table 1: (Hollnagel, Wears & Braithwaite, 2015).....	20
Tabell 3-2 Spørsmål fra RAG, basert på Table 5.4 (Hollnagel, 2017, s.61).....	27
Tabell 4-3 Informantutvalg.....	41
Tabell 4-4 Presentasjon av skriftlige datakilder	44
Tabell 4-5 Presentasjon av digitale systemer i Lundin	50

1.0 Innledning

Det høye sikkerhetsnivået som i dag preger norsk petroleumsvirksomhet, kan i stor grad ses som et resultat av det kontinuerlige sikkerhetsarbeidet som har funnet sted på norsk sokkel de siste tiårene. I disse dager er petroleumsnæringen inne i en viktig digitaliseringsatsing hvor effektivitetstiltak og digitale systemer introduseres på løpende bånd. Disse endringene utfordrer arbeidet med sikkerhet, og et fortsatt høyt sikkerhetsnivå på norsk sokkel er avhengig av en videreføring av den høye arbeidsinnsatsen med sikkerhet. Kostnadsreduiseringer og effektivitetstiltak anses i dag som nødvendig for å sikre et HMS-regime som er i stand til å møte fremtidens sikkerhets- og arbeidsmiljøutfordringer (Engen, 2017, s.9).

I 2011 iverksatte SINTEF et forskningsprosjekt for å rette søkelyset mot forbedringstiltak på norsk sokkel basert på kunnskapsgrunnet fra Deepwater Horizon-ulykken på Macandofeltet i Mexicogulven. Formålet med prosjektet var å systematisk gjennomgå informasjon fra granskinger i etterkant av Deepwater Horizon-ulykken og andre større ulykker i petroleumsnæringen, og på denne måten utarbeide relevante forbedringspunkter og anbefalinger til norsk sokkel (Tinmannsvik, 2011, s.31). Flere av anbefalingene var rettet mot kunnskapsoverføring, informasjonsflyt og bruk av indikatorer. Under anbefalinger knyttet til organisasjon og ledelse ble det blant annet formulert anbefalinger om å: «Legge til rette for systematisk erfaringsoverføring og læring fra hendelser i ulike bransjer» (Tinmannsvik, 2011, s.31). Videre ble det også foreslått å «ta i bruk ulike perspektiver på storulykker og robuste organisasjoner for å granske hendelser med utgangspunkt i ulike forståelsesrammer, og dermed få bedre innsikt i, og et bredere grunnlag for å foreslå forbedringstiltak» (Tinmannsvik, 2011, s.31). Disse anbefalingene ble basert på en helhetlig vurdering av petroleumsnæringen, og besitter flere likhetstrekk med anbefalinger fremmet av Engen-utvalget. I 2016 ble en partssammensatt arbeidsgruppe, ledet av Ole Andreas Engen, bedt om å drøfte problemstillingen knyttet til HMS i petroleumsnæringen (Engen, 2017, s.10).

I rapportens konklusjoner og anbefalinger presenteres arbeidsgruppens anbefalinger for næringens videre arbeid med HMS.

Under punktet næringens og selskapenes oppfølging er følgende anbefaling formulert;

Arbeidsgruppen anbefaler at det gjøres en vurdering av partenes læring etter hendelser med sikte på å ytterligere forbedre dette. Det er i dag mange møteplasser og arenaer hvor HMS diskuteres, og det er et stort omfang av kunnskap som kan deles. Det er imidlertid behov for bedre systematisering av kunnskapen for å gi god læring etter hendelser. Næringen må bruke og vedlikeholde arenaer for å overføre erfaringer fra granskninger ol. slik at alle aktører blir kjent med dette (Engen, 2017, s.106).

De overnevnte forskningsprosjektene rettet mot den norske petroleumsnæringen har i de siste årene pekt på et behov for systemer som styrker kunnskapsoverføring. Stikkord som informasjonsflyt, bruk av indikatorer, og fokus på robuste egenskaper i organisasjoner er også gjengangere i disse forskningsprosjektene, som peker på kunnskapsoverføring som en utfordring i hele næringen.

Petroleumsnæringen befinner seg nå i en periode hvor det er stort fokus på effektivitet og kostnader, samtidig som ny teknologi introduseres. Denne perioden kan betegnes som en brytningstid hvor fokuset på utvikling av teknologi er høyt, samtidig som eldre systemer og arbeidsprosesser fortsatt råder (IRIS, 2018, s. 9). Lundin Norway har vært blant de mest aktive selskapene i Barentshavet de siste årene, og fullførte en vellykket prøveproduksjon på Altafunnet i sommeren 2018. Selskapets vekst og økende satsning i nordområdene vil sammen med digitaliseringens inntog kunne by på både utfordringer og muligheter knyttet til nettopp kunnskapsoverføring. Utfordringer vil kunne oppstå i form av ivaretagelse av systematisk sikkerhetsstyring i geografiske områder med redusert beredskap. Utbygging og vekst gir også muligheter ved at man tidlig kan inkorporere digitale systemer og rutiner for sikkerhetsarbeid og kunnskapsoverføring. De rammene som legges i dag vil kunne danne et grunnlag for fremtiden når organisasjonen vokser.

Dagens regelverk setter krav til blant annet kontinuerlig forbedring av HMS-kultur, og intern styring. For å kunne etterleve dagens regelverk er operatørene avhengig av å tilegne seg kunnskap. En systematisk kunnskapsoverføring er essensielt både for å etterleve regelverk, men også for å kunne drive en sikker virksomhet i det hele og det store (Petroleumstilsynet, 2013, s.3). Det er lite hensiktsmessig å tilegne seg kunnskap ved å for eksempel telle antall hendelser, uten at denne kunnskapen settes til verks i form av handlinger (Petroleumstilsynet, 2013, s.8).

Petroleumstilsynet beskriver utfordringen med kunnskapsoverføring i petroleumsnæringen på følgende måte;

I oljevirksomheten er det mange grenser som må krysses: Hav og land, ledelse og utførende personell, operatører – leverandører, og virksomheter og tilsynsmyndigheter. Mange grensesnitt og høyt tempo kan skape utfordringer for kunnskapsdeling. Ulike språk og ulike tankemodeller kan gjøre det vanskelig å dele kunnskap mellom faggrupper (Petroleumstilsynet, 2013, s.10).

Det er åpenbart en utfordring å organisere og koordinere kunnskapsoverføring i et operatørselskap, og dette setter krav til systemer for informasjonsbehandling, rutiner og holdninger i selskapet. Det vil derfor være nærliggende å spørre seg hva som er formålet med kunnskapsoverføring, og hvordan man kan utvikle digitale systemer som tilrettelegger for kunnskapsoverføring. Sikkerhetsinformasjonssystemer har tradisjonelt blitt benyttet for å kunne effektivt benytte kunnskap- og erfaringsdata fra uønskede hendelser og forhold til å styrke sikkerheten i en organisasjon. Formålet med et sikkerhetsinformasjonssystem er å registrere informasjon om uønskede hendelser, før dette blir analysert og benyttet til å implementere risikoreduserende tiltak i etterkant av hendelsen (Aven et al, 2004, s. 131). Sikkerhetsinformasjonssystemer rolle kan dermed grovt sett deles inn etter tre formål; samle inn, systematisere og distribuere kunnskap med betydning for sikkerheten i organisasjonen. Man kan argumentere for at slike systemer utgjør selve kjernen av de formaliserte systemene for kunnskapsoverføring i en sikkerhetskontekst.

I lys av forskningsrapporter som peker på behovet for robuste egenskaper, og en faglitteratur som stadig vier økende oppmerksomhet mot «Resilience Engineering», er dette en naturlig retning å søke etter svar. Organisasjoner og sosio-tekniske systemer har i de siste årene blitt stadig mer komplekse uten at faglitteratur kan sies å ha utviklet seg i et tilsvarende tempo. RE anses som et svar til det økende behovet for nye metoder innenfor sikkerhetsstyring (Steen & Aven, 2011, s. 292). Resilience Engineering er et fagfelt som det siste tiåret har blitt viet økende oppmerksomhet i sikkerhetslitteraturen for sitt fokus på systemers evner til å tilpasse seg sine omgivelser ved å forsterke egenskaper som fremmer en motstandsdyktighet. Innenfor «Resilience Engineering» betegnes resiliens som en form for motstandsdyktighet og kan rangeres på tre nivåer; Evnen til å hindre noe galt å skje, evnen til å hindre noe galt å bli verre, og evnen til å komme tilbake til normal tilstand etter noe galt har skjedd (Bartnes, 2013). Resilience engineering har som hensikt å tilrettelegge for motstandsdyktighet eller resiliens i et system. Selv om fagfeltet er omfattende, har teoretikeren Erik Hollnagel gjort seg bemerket med sine teoretiske bidrag og verktøy for å oppnå resiliens. Hollnagel trekker spesielt frem fire

egenskaper som en organisasjon må besitte for å kunne tilrettelegge for en resilient ytelse (Bartnes, 2013). De fire egenskapene; respondere, monitorere, lære, og forutse utgjør til sammen en form for «oppskrift» som har som hensikt å tilrettelegge for resiliens (Hollnagel, 2017, s. 24).

Med hovedvekt på egenskapen monitorering har dette forskningsprosjektet som formål å kartlegge hvorvidt Lundins digitale sikkerhetsinformasjonssystemer kan bidra til resiliens. Det blir derfor nødvendig å redegjøre for hvordan sikkerhetsinformasjonssystemene i Lundin benyttes til innsamling, systematisering, og distribusjon av sikkerhetsrelevant kunnskap. Dette vil bli gjort ved å både vurdere systemenes struktur og utforming, samt den praktiske bruken av systemene. På denne måten kan man vurdere om de formaliserte digitale systemene for kunnskapsoverføring i Lundin bidrar til resiliens.

1.1 Problemstilling og forskningsspørsmål

I dette forskningsprosjektet er tematikken og problemstillingen forankret i «Resilience Engineering». Ved å benytte teoretiske utdrag fra RE vil prosjektets målsetning være å kartlegge hvordan digitale systemer for kunnskapsoverføring kan bidra til resiliens i Lundin. Håndtering av kunnskap har en nær tilknytning til organisasjoners evne til å respondere og tilpasse seg forventede og uforventede forhold, som er sentrale egenskaper innenfor RE. I tråd med etablert litteratur vil standardiserte systemer for kunnskapsoverføring i prosjektet bli betegnet som sikkerhetsinformasjonssystemer. For å kunne besvare problemstillingen har det blitt utarbeidet tre forskningsspørsmål som tar for seg tre sentrale prosesser i overføringen av kunnskap. De tre forskningsspørsmålene vil rette søkelyset mot monitorering, systematisering, og distribuering av kunnskap med betydning for sikkerheten i Lundin Norway. Med hovedvekt på egenskapen «monitorering» fra RE, vil teoretiske bidrag som RE, indikatorbruk, sikkerhetsinformasjonssystemer, og digitalisering sammen danne et teoretisk bakteppe for prosjektets analyse. Med dette utgangspunktet har det blitt formulert følgende problemstilling og forskningsspørsmål:

Hvordan kan digitale sikkerhetsinformasjonssystemer bidra til resiliens i Lundin Norway?

F1) Hvordan benyttes digitale sikkerhetsinformasjonssystemer til monitorering av sikkerhet i Lundin Norway?

F2) Hvordan benyttes digitale sikkerhetsinformasjonssystemer til systematisering av kunnskap i Lundin Norway?

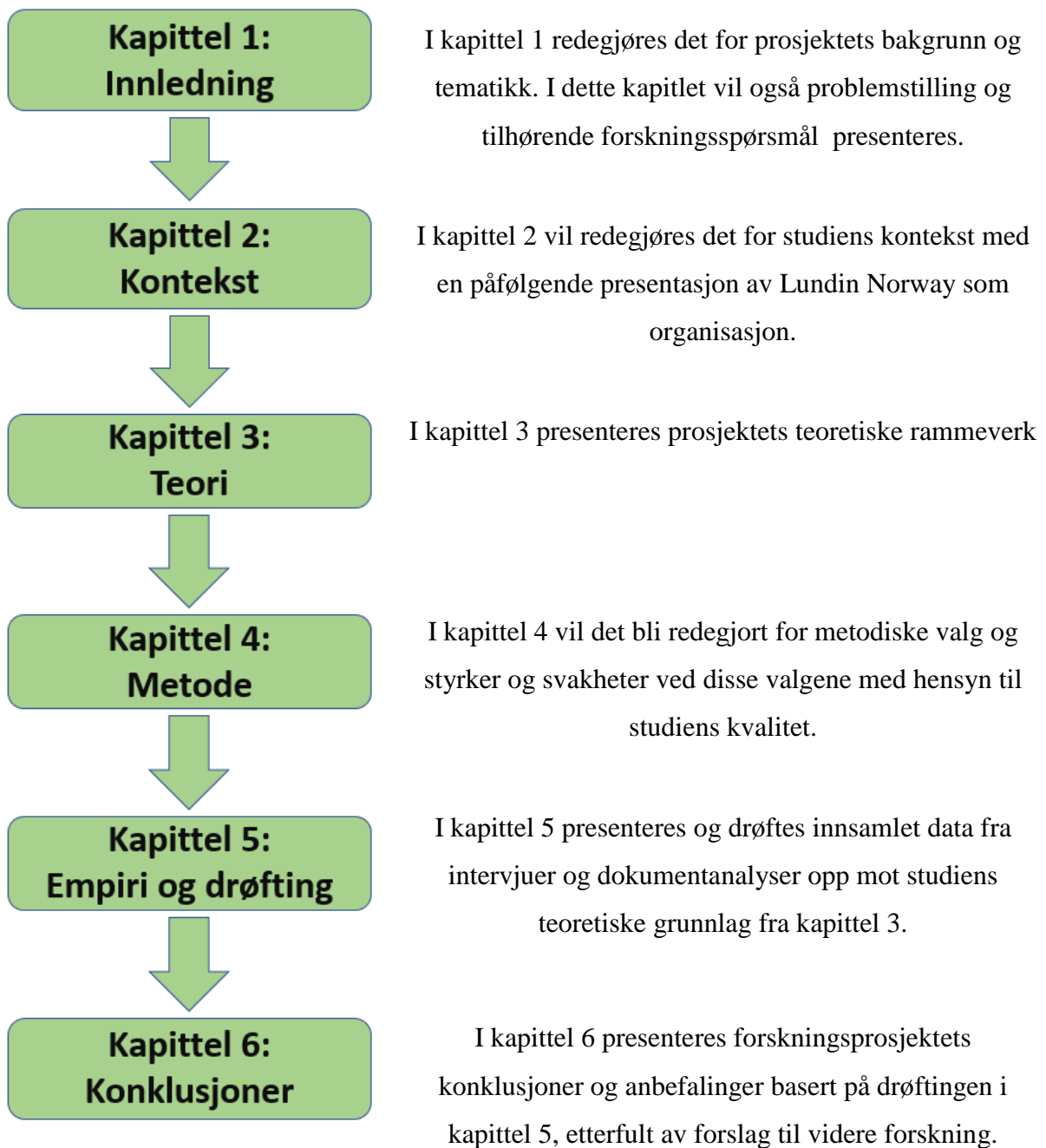
F3) Hvordan distribueres kunnskap fra digitale sikkerhetsinformasjonssystemer i Lundin Norway?

1.2 Avgrensning

Tematikken og problemstillingen i dette forskningsprosjektet er avgrenset til digitale systemer for kunnskapsoverføring med hensyn til sikkerhet i virksomheten Lundin Norway. Kunnskapsoverføring er et omfattende tema med litteratur som krysser over i flere fagfelt. Som en følge av dette har det blitt valgt å ekskludere litteratur om læring i form av sosiale og kognitive prosesser. Forskningsprosjektet er dermed avgrenset til hvordan intern digital programvare legger føringer for kunnskapsoverføring med hensyn til sikkerhet i Lundin. Denne avgrensningen er utført av hensyn til prosjektets omfang og formål. Prosjektet er også avgrenset til Lundin Norway som virksomhet, og ekskluderer dermed informasjonsprosesser hos eksterne riggselskaper og andre leverandører som Lundin benytter.

Prosjektets tematikk er avgrenset til kunnskapsoverføring med hensyn til sikkerhet, og har derfor av logiske årsaker blitt utført ved Lundins HMS-avdeling (HSEQ). Som en følge av prosjektets tematikk og kontekst har det blitt valgt å benytte et teoretisk rammeverk som retter søkelyset mot resiliens, indikatorbruk, digitalisering og SIS. Det understrekes samtidig at forskningsprosjektet ikke har som formål å kartlegge resiliens i Lundin, men heller søker etter egenskaper og prosesser som samsvarer med teori om resiliens.

1.3 Oppgavens oppbygning og struktur



2.0 Kontekst

Dette forskningsprosjektet er utarbeidet i samarbeid med Lundin Norway. Det vil i dette kapitlet derfor redegjøres for Lundin Norway som organisasjon, og selskapets rolle i den norske petroleumsnæringen

2.1 Lundin Norway

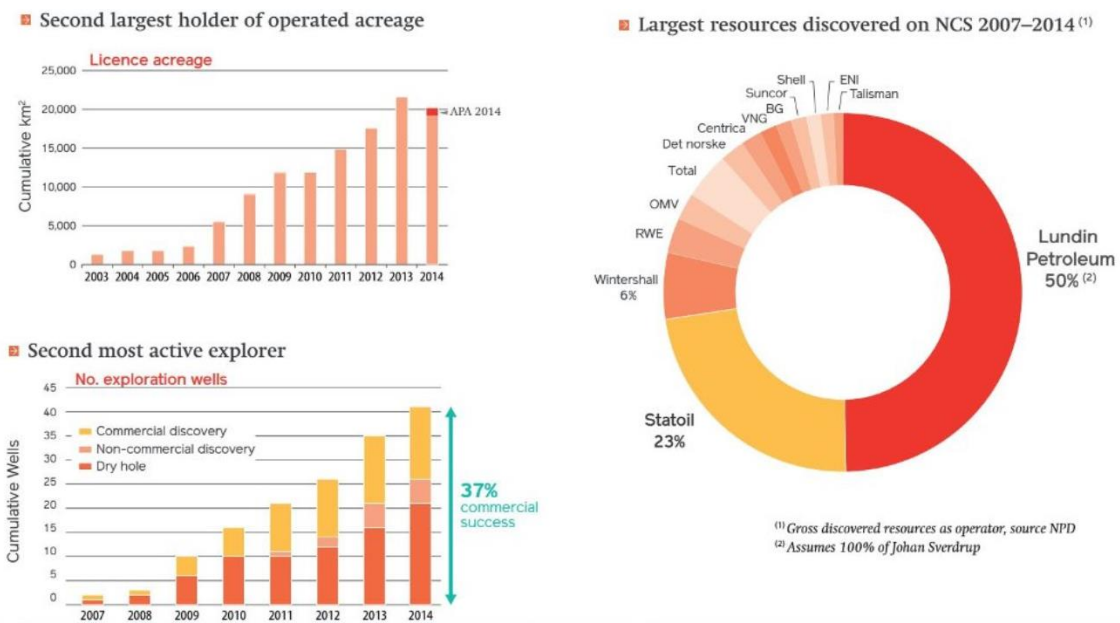
Lundin Norway er et datterselskap av det svenskeide og børsnoterte selskapet Lundin Petroleum. Lundin Norway ble etablert i 2003 etter at Lundin Petroleum anskaffet 75 prosent av aksjepostene i det norske lete- og produksjonsselskapet OER Olje. Oppkjøpet markerte starten på en rekke aktiviteter på norsk sokkel (Lundin Petroleum, 2019). Selskapet har i dag om lag 370 ansatte, hvor flesteparten er stasjonert ved hovedkontoret på Lysaker.

Lundins første letebrønn ble boret i 2007 og traff reservoaret som i dag er Edvard Grieg-feltet. Funnet resulterte i en stor feltutbygging, og ble starten på en rekke aktiviteter på Utsirahøyden i Nordsjøen, området som tidligere var avskrevet av en rekke selskaper. Det kanskje viktigste milepælen i Lundins historie var imidlertid funnet som ble gjort i 2010. Johan Sverdrup-funnet som ble gjort i 2010 skulle senere føre til det største industriprosjektet i Norge de siste årene (Lundin, 2019). Funnet er regnet som en av de største funnene som noensinne er gjort på norsk kontinentalsokkel, og strekker seg over et område på 200 km². Feltet er beregnet å ha mellom 2,1 til 3,1 milliarder oljeekvivalenter, noe som gjør feltet til et av de fem største feltene noen gang oppdaget på norsk sokkel. Feltet har en forventet platårrate på 660 000 fat per dag, noe som sannsynligvis vil føre til at produksjon fra feltet vil utgjøre 25 prosent av den norske petroleumssektoren når produksjonen starter høsten 2019 (Lundin Norway, 2019).



Figur 2-1 Utsirahøyden, av Lundin (2019) (https://www.lundin-norway.no/wp-content/uploads/sites/4/2019/04/Utsira_leiv-1500x800.jpg)

Lundin Norway er også selskapet med nest størst eierandel i Johan Sverdrup-feltet med en andel på 22,6 %. Feltet er dermed den viktigste inntektskilden for Lundin (Lundin, 2019). Funnene har også gjort Lundin Norway til et av de mest suksessfulle leteselskapene på norsk sokkel de siste tiårene.



Figur 2-2 Lundins funn. Av Rune Endresen.(2015)

(https://g.acdn.no/obscura/API/dynamic/r1/ece5/tr_1080_648_1_f/0000/nord/2015/11/24/12/lundin.JPG?chk=BA7F7E)

Lundin Norway legger mye av sin stolthet i kompetansesterke ansatte, og en selskapskultur som tørr å lete der andre ikke ser muligheter. Selskapets raske vekst gjorde det mulig å hente inn kompetansesterke ansatte med lang fartstid i næringen. Store deler av grunnlaget for selskapet er i dag tuftet på funnene på Utsirahøyden, og selskapets evne til løse de geologiske kodene for dette området (Lundin, 2019). Lundin fortsetter i dag sin offensive letestrategi og har vært blant de mest aktive selskapene i Barentshavet de siste årene. Sommeren 2018 ble en vellykket prøveproduksjon på Alta-funnet fullført, og fra høsten 2019 vil produksjonen fra Johan Sverdrup etter planen igangsettes. Lundin er i dag operatør og rettighetshaver for henholdsvis 36 og 79 lisenser. Selskapet er også operatør på to felt (Norsk Petroleum, 2019). På tross av selskapets unge alder, har Lundin på kort tid evnet å markere seg som en sterk og viktig aktør på norsk sokkel.

3.0 Teori

Teorikapittelet i dette forskningsprosjektet vil i hovedsak basere seg på teori og litteratur om resiliens, sikkerhetsinformasjonssystemer og digitalisering. Dette prosjektet omhandler kunnskapsoverføring og hvordan systematisering av kunnskap kan styrke sikkerhetsstyring i Lundin Norway ved å bidra til resiliens. I litteraturen som omhandler resiliens vektlegges faktorer og egenskaper som kan bidra til å skape en resilient organisasjon. I denne studien har teori om resiliens blitt benyttet for å kunne tilføre et moderne perspektiv på kunnskapsoverføringsprosessene i Lundin Norway. Litteratur om resiliens retter mye av søkelyset på prosesser tilknyttet kunnskapsoverføring, og i kartleggingen av Lundins evne til å praktisere kunnskapsoverføring vil det derfor være bidragsgivende å benytte veletablerte resiliensteorier. Kapittelet vil videre redegjøre for hvordan verktøy fra «Resilience Engineering», heretter referert til som RE, kan bidra til å vurdere en organisasjons resilienspotensial. Herunder vil det selekteres spesifikke områder fra RE, og prosjektets teori vil derfor avgrenses til organisasjonens evne til å innhente, behandle og systematisere kunnskap. Siden kunnskapsoverføringsbegrepet tradisjonelt sett, innebefatter svært mange aspekter vil denne studien kun fokuseres på de formaliserte systemene for overføring av kunnskap for å besvare oppgavens problemstilling. Det vil samtidig være hensiktsmessig å inkludere RAG-verktøyet da det tilbyr et sett med spørsmål for å kartlegge funksjonen til en egenskap i et system. Videre vil det redegjøres for hvordan sikkerhetsinformasjonssystemer og struktur påvirker de formaliserte systemene for kunnskapsoverføring. Avslutningsvis vil kapittelet presentere litteratur som omhandler hvordan digitaliseringsprosesser påvirker menneskene i organisasjonen, og hvordan de psykologiske faktorene påvirker kunnskapsoverføring og bruk av sikkerhetsinformasjonssystemer.

3.1 Resiliens

Begrepet resiliens ble først brukt av den britiske marinen på starten av 1900-tallet, for å beskrive hvor mye belastning ulike tresorter kunne tåle (Hollnagel, 2017). Begrepet ble senere benyttet innenfor økologistudier for å beskrive hvilken grad av endring et system kunne utsettes for uten å miste sin funksjon (Holling, 1973). Da begrepet ble overført til å beskrive organisasjoner og sosiotekniske systemer, ble også betydningen av begrepet endret fra en beskrivelse av reaktive funksjoner til beskrivelser av noe proaktiv. Bakgrunnen for dette er den reaktive naturen til økologiske systemer som er tvunget til å tilpasse seg omgivelser i endring. Sosiotekniske systemer vil i motsetning til økologiske systemer befinne seg i mer forutsigbare omgivelser, ettersom de er styrt av mennesker med klare og tydelige intensjoner.

En organisasjon vil derfor lettere kunne tilpasse seg omgivelsene og predikere fremtiden (Hollnagel, 2017, s. 11-12). Resiliensbegrepet er også svært utbredt innenfor psykologifeltet, hvor man snakker om psykologisk motstandskraft. Resiliens brukes her til å beskrive de faktorer som har sammenheng med at man beholder en psykisk styrke og helse til tross for stress og påkjenninger. Å være resilient vil si at man er robust (Skre, 2018).

Definisjonen av resiliens som dette forskningsprosjektet har basert seg på er som følger: et uttrykk for et systems ytelse under forventede og uforventede forhold. Slike forhold innebærer både endringer, forstyrrelser og muligheter (Hollnagel, 2017, s. 14-15). Denne definisjonen vektlegger hvordan et system yter under varierte omstendigheter, samtidig som definisjonen også fremhever potensielle positive og negative konsekvenser. Resiliensbegrepet inneholder også en proaktiv dimensjon ettersom man omtaler et systems ytelsesvariasjon i dynamiske omgivelser. Innenfor RE betegnes den tradisjonelle tilnærmingen til sikkerhet som «Safety-I» samtidig som den nye sikkerhetstilnærmingen i RE betegnes som «Safety-II». Dette skillet markerer forskjellen i flere grunnleggende antakelser mellom de to tilnærmingene (Hollnagel, 2017, s. 7).

I den følgende tabellen presenteres noen grunnleggende antakelser fra de to tilnærmingene. Tabellen 3-1 viser følgelig hvordan «Safety-II» skiller seg fra den tradisjonelle tilnærmingen til sikkerhet, og hvordan RE kan tilby nye perspektiver på sikkerhetsstyring. Dette er også bakgrunnen for inkluderingen av RE i dette prosjektet.

Tabell 3-1, Safety-I og Safety II, basert på Table 1: Overview of Safety-I and Safety-II i (Hollnagel, Wears & Braithwaite, 2015).

	Tradisjonell sikkerhetsstyring (Safety 1)	Resilience Engineering (Safety 2)
Perspektiv på sikkerhet	Så få uønskede hendelser som mulig	Evne til å lykkes under varierende forhold
Prinsipper for sikkerhetsstyring	Reaktiv, respondere når uønskede hendelser og uakseptabel risiko oppstår.	Proaktiv, kontinuerlig forsøke å forutse utviklinger og hendelser.
Perspektiver på menneskelige faktorer i sikkerhetsstyring	Mennesker anses som en kilde til feil og en fare for systemet.	Mennesker anses som en viktig kilde for systemets fleksibilitet og resiliens
Ulykkesgransking	Ulykker er forårsaket av svikt og feil. Formålet med en gransking er å finne årsakene	Hendelser har ofte samme årsak, uavhengig av utfall. Formålet med en gransking er å forstå hvorfor hendelser som vanligvis går bra noen ganger går galt.

3.1.1 Resilience engineering

«Resilience engineering» som fagområde ble først introdusert under et sikkerhetsfaglig møte i Söderköping i 2004, og har siden blitt beskrevet i en rekke bøker og fagartikler. Hollnagel (2017) beskriver opprinnelsen av fagfeltet som et motsvar på flere teoretikers økende misnøye mot etablerte metodikker innen risikoanalyser og risikostyring. På grunnlag av den økende utviklingen og implementeringen av tekniske og sosiotekniske systemer er det i større grad behov for å forstå hvordan RE kan benyttes i organisasjonens sikkerhetsstyring.

På bakgrunn av digitaliseringsprosesser blir organisasjoner stadig mer komplekse og utvikler seg raskt, men sikkerhetsstyringen har ikke utviklet seg i tilsvarende tempo. Derfor er det et økende behov for nye metoder og tilnærminger innenfor sikkerhetsstyring, og herunder ansees RE som et svar til dette økende behovet (Steen & Aven, 2011, s. 292). Utvalgte deler av RE vil i denne sammenheng kunne gi et nytt perspektiv på delprosesser knyttet til kunnskapsoverføring og sikkerhetsstyring i Lundin Norway.

I likhet med den overnevnte resiliensdefinisjonen brukes RE til å se komplekse forhold som en mulig kilde til både positive og negative læringssituasjoner (Rosness, 2010, s. 107-108). System-perspektivet på ulykker og årsaksforhold er sentralt i argumentasjonen til RE. Mange ulykker og uønskede hendelser er ikke et resultat av svikt i systemfunksjoner eller komponenter, men heller et resultat av uforutsigbare kombinasjoner av ytelsesvariasjon. Innenfor RE anses ytelsesvariasjon i et system som noe normalt, og det argumenteres ofte for at ytelsesbegrensende tiltak for å øke sikkerhet har liten hensikt. Ved å begrense ytelse vil en også påvirke «ytelsesavvik» som fører til positive utfall. En må derfor heller forsøke å dempe ytelsesavvik som fører til direkte negative konsekvenser (Steen & Aven, 2011, s. 292).

Fagfeltet RE har de siste årene fått økt oppmerksomhet innenfor sikkerhetslitteraturen. Som en motvekt til etablert sikkerhetsmetodikk vektlegger RE systemers evne til å være resiliente, og hvordan dette gjøres ved å anerkjenne, tilpasse og absorbere endringer og forstyrrelser på en proaktiv måte. Det kan være lett å anerkjenne resiliens som et viktig aspekt i sikkerhetsstyringen i en organisasjon, men innenfor forskningen har det lenge vært en utfordring å konkretisere hva som faktisk fører til resiliens. Det har derfor blitt rettet mye oppmerksomhet mot å utarbeide metoder og prinsipper som kan fungere som byggesteiner for utvikling av resiliens i en organisasjon (Steen & Aven, 2011, s. 292).

3.1.2 Hollnagels fire egenskaper

I *Safety-II in Practice* (2017) beskriver Hollnagel resiliens som noe en organisasjon gjør, og ikke noe den har. Han forklarer hvordan fire egenskaper, eller potensialer (potentials), kan benyttes for å måle hvorvidt et system har potensialet til en resilient ytelse. De fire egenskapene for resiliens er systemets evne til å respondere (respond), monitorere (monitor), lære (learn) og forutse (anticipate) (Hollnagel, 2017, s. 24). I dette prosjektet er det valgt å bruke monitorering som oversatt begrep for ”monitor”.

Selv om noen forskningsmiljøer har benyttet både ”overvåke” og ”observere” i sammenheng med Hollnagels fire egenskaper, kan det argumenteres for at begrepet monitorere i større grad er et beskrivende ord når man skal undersøke en organisasjons sikkerhetsstyring. Samtidig er begrepet også etablert i vokabularet til ansatte ved Lundin. Det er viktig å understreke at de fire egenskapene kan benyttes for å måle potensialet eller forutsetningene for resiliens, og ikke resiliens i seg selv. Det er heller ikke gitt at et system som oppfyller egenskapene for resiliens dermed er et system med resilient ytelse. Målingen av egenskapene tar sikte på å redegjøre for potensialet til systemet, og ikke hva selve systemet er (Hollnagel, 2017, s. 16).

Dette prosjektet har ikke som formål å vurdere hvorvidt Lundin Norway er en resilient organisasjon, men vil heller undersøke hvorvidt Lundins systemer for kunnskapsoverføring samsvarer med grunnleggende forutsetninger for resiliens ut ifra Hollnagels beskrivelser. Som følge av oppgavens avgrensning anses det som hensiktsmessig i dette prosjektet å vektlegge én av de fire egenskapene. Monitoreringsegenskapen har derfor blitt selektert basert på prosjektets digitaliseringstematikk og fokus på kunnskapsoverføring.

Selv om dette prosjektet fokuserer på egenskapen monitorering og hvilke delfunksjoner RE vektlegger for monitorering, vil det av kontekstuelle årsaker redegjøres for alle de fire egenskapene i det følgende avsnittet. RE vektlegger i utgangspunktet oppfyllelse av de fire egenskapene for å kunne oppnå resiliens, men i prosjektet vil det argumenteres for at delkomponenten monitorering kan benyttes isolert og fortsatt fremstille formålstjenlige data.

Siden Hollnagels grunntanke er at disse egenskapene må sees i sammenheng dersom man skal vurdere et systems potensiale for resilient ytelse, vil det være viktig å redegjøre for alle de fire egenskapene samlet. På denne måten vil man også da kunne diskutere om nettopp egenskapen monitorering kan benyttes isolert sett, og samtidig ha nytteverdi. Det anses allikevel ikke som hensiktsmessig å vurdere alle fire egenskapene i denne sammenhengen, da prosjektet er avgrenset til digitale systemer for kunnskapsoverføring, samtidig som prosjektet ikke har som formål å kartlegge resiliens i hele organisasjonen, men heller å vurdere Lundins evne til å praktisere kunnskapsoverføring i lys av RE. Det vil videre bli gitt en kort beskrivelse av de fire egenskapene Hollnagel legger til grunn som forutsetninger for resiliens i organisasjoner.

3.1.2.1 Respondere

Det vil være vanskelig for en organisasjon å overleve uten evnen til å respondere på ytre omgivelser. Måten en organisasjon responderer på sine omgivelser vil være betinget av blant annet erfaring, ressursforvaltning, ledelsesstrategi og hva som anses som mest hensiktsmessig fra et kost/nytte-perspektiv. Ingen organisasjoner besitter ubegrensede ressurser og en organisasjon vil kun være forberedt på et begrenset antall hendelser eller tilstander. Dette understreker behovet for en organisasjons evne til å respondere (Hollnagel, 2017, s. 54 - 55).

3.1.2.2 Monitorere

Hollnagel skriver at en organisasjons evne til å respondere vil naturligvis være betinget av evnen til å monitorere. Beslutningsgrunnlaget for å iverksette en respons vil utløses av innhentet kunnskap fra monitorering. Det er sentralt å spørre seg om hva som monitoreres og hvorfor. Dette stiller igjen grunnleggende spørsmål om prioriteringer, ressurstildelinger og hvilke data en ønsker å innhente. Indikatorene som monitoreres kan kategoriseres som ledende indikatorer og etterslepene indikatorer. En indikator kan betegnes som ledende dersom den tilfører en type informasjon som fører til iverksettelse av tiltak for å avverge eller forhindre en endring i en av hovedfunksjonene til organisasjonen. En slik proaktiv indikator har overordnet sett et formål om å predikere fremtiden. En etterslepene indikator er mer reaktiv og har som formål å gi informasjon om endringer som allerede har funnet sted (Hollnagel, 2017, s. 18).

3.1.2.3 Lære

En organisasjon som har et monitoreringspotensiale og dernest et responderingspotensiale, vil også kunne ha et læringspotensiale (Hollnagel, 2017, s. 64). Organisasjoner flest er prisgitt sine dynamiske omgivelser, og er derfor avhengig av å kontinuerlig tilpasse sin drift etter omgivelsene. Organisasjoner møter daglig ulike situasjoner av ulik størrelse som krever spesifikke håndteringer. Læring er essensen i denne prosessen og innebærer en aktiv og tilsiktet modifisering av måten organisasjonen håndterer disse daglige situasjonene, uavhengig av omfang. RE vektlegger altså hvordan læring i organisasjoner må skje i det daglige, og ikke begrenses til hendelser med negativt utfall som oppstår uregelmessig (Hollnagel, 2017, s. 64).

3.1.2.4 Forutse

Hollnagel hevder at det å være forutseende kanskje er den mest undervurderte egenskapene av de fire. Å forutse er å forsøke og si noe om fremtiden. Organisasjoner vil hele tiden være avhengig av å kunne forutse fremtidige omgivelser for å kunne overleve. Ulike bransjer vil naturligvis ha ulike behov for å forutse, men dette vil i stor grad være påvirket av den kontinuerlige utviklingen i samfunnet. Egenskapen å forutse er nært beslektet med monitorering, men i motsetning til monitorering, som hovedsakelig er knyttet til målinger av ytre- og indre omgivelser, har egenskapen å forutse til formål å benytte innhentet informasjon til å predikere fremtidige hendelser. En viktig forutsetning for å kunne forutse er en organisasjonskultur og visjon som aksepterer behovet for å bruke tid og ressurser på å tenke på fremtiden. En slik visjon må innebære en etablert idé om en ønsket fremtidig tilstand (Hollnagel, 2017, s. 65-66).

Som følge av et omfattende fagområde og naturlige ressursbegrensninger, vil dette prosjektet rette søkelyset mot egenskapen monitorering. Selv om de fire egenskapene henger tett sammen, kan det argumenteres for at evnen til å respondere og forutse, som er de to øvrige egenskapene, i stor grad styres av hvordan en organisasjon monitorerer. Det samme argumentet kan sies å gjelde for evnen til å forutse. Monitorering spiller derfor en sentral rolle og kan også knyttes direkte opp mot evnen til å innhente kunnskap.

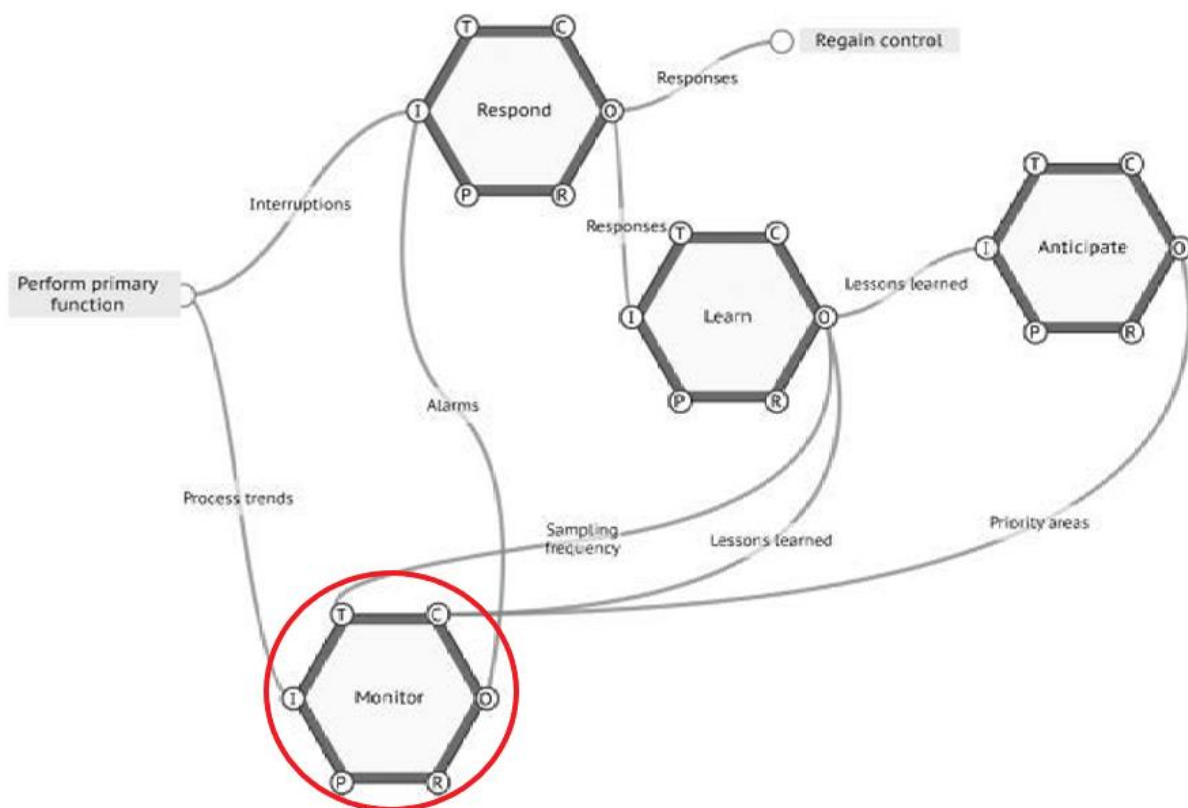
3.1.3 RAG - «The Resilience Assessment Grid»

Innenfor RE anser Hollnagel de fire presenterte egenskapene som grunnlag for resiliens dersom alle er oppfylt. Disse egenskapene må kontinuerlig måles og administreres for å vedlikeholde eksisterende resiliens i systemet. Systems ytelse under forventede og uforventede forhold kan dermed anses som et uttrykk for systemets prestasjon og potensiale. Et hvert system som skal styres i en retning må ifølge Hollnagel kunne besvare tre grunnleggende spørsmål: Hvor er vi nå? Hvor vil vi være? Og hva må til for å oppnå ønsket tilstand? (Hollnagel, 2017, s. 50).

«The Resilience Assessment Grid», heretter forkortet til RAG, vil i dette delkapitlet beskrives for å kunne eksemplifisere hvordan egenskapene kan måles ved bruk av spørsmål som er rettet mot delfunksjoner, og hvordan dette kan brukes som et verktøy for å måle resilienspotensialet i en organisasjon. RAG er et diagnostiseringsverktøy utviklet innenfor RE for å kunne vurdere systemers potensiale for resiliens. Hensikten med verktøyet er å kunne utføre vurderinger av de fire egenskapene for å kontinuerlig kunne sammenligne systemet med en tidligere tilstand.

Ved å gjøre dette vil en kunne kartlegge hvilken retning systemet beveger seg i, og samtidig registrere endringer i ytelse. En slik vurdering tar sikte på å vurdere om systemet har ønsket ytelse og om det er behov for eventuelle korrigeringer eller inngrep (Hollnagel, 2017, s. 53).

Verktøyet har som formål å kunne foreta en helhetlig vurdering av det aktuelle systemet, og måle hvorvidt de fire egenskapene oppfylles. Man ønsker altså å undersøke funksjonene som kreves for å oppfylle egenskapene, og i hvilken grad disse funksjonene fungerer tilfredsstillende (Hollnagel, 2017, s. 53). Figur 3-3 illustrer Hollnagels FRAM-modell, som er en utvidet versjon av RAG, og gir et bilde av egenskapenes tilknytning til hverandre, samtidig som figuren viser monitoreringsegenskapens overordnede rolle i et system.



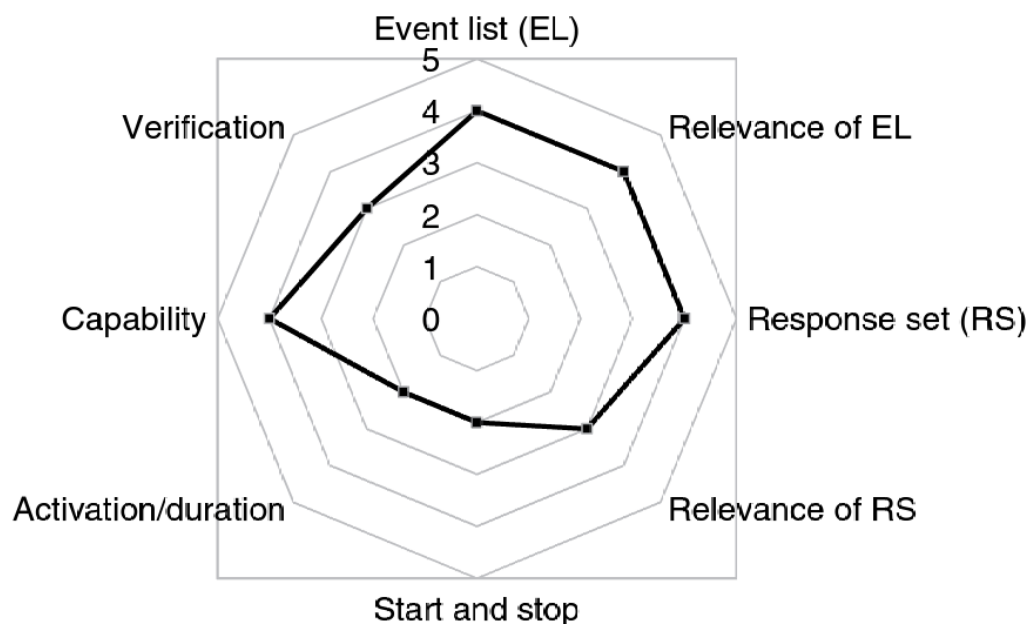
Figur 3-3 The Basic Model of the Four Potentials, using the FRAM (Hollnagel, 2017, s. 86).

RAG tar utgangspunkt i et sett med forhåndsdefinerte spørsmål som har til hensikt å undersøke i hvilken grad forutsetningene for egenskapene og dermed resiliens oppfylles. Spørsmålene kan sendes til ulike deler av systemet, eller avdelinger i organisasjonen. Spørsmålene skal være både diagnostiserende og formative. Diagnostiserende i den grad de kan besvare hvorvidt egenskapen oppfylles fra et operativt aspekt. Formative ved å innhente data som kan brukes til konkrete aktiviteter, inngriper eller forbedringer.

Spørsmålene må være tilpasset det spesifikke systemet, og generiske spørsmål bør derfor unngås. RAG tilbyr et sett med diagnostiserende spørsmål som kan benyttes som utgangspunkt for utarbeidelse av mer systemspesifikke spørsmål.

Spørsmålene som benyttes i RAG dekker åtte delområder for hver egenskap, og tar sikte på å kartlegge forutsetningene for hver av de fire egenskapene (Hollnagel, 2017, s. 53).

RAG-verktøyet har som formål å vurdere en tilstand sammenlignet med en tidligere tilstand, og må derfor brukes regelmessig med gitte tidsintervaller. Resultatene bør derfor presenteres på en måte som belyser eventuelle endringer fra tidligere vurderinger. Hollnagel mener at det kan være fordelaktig å benytte seg av en graderingsskala, ettersom en graderingsskala evner å vise utviklinger og endringer i vurderinger fra tidligere undersøkelser, her vist i form av et radardiagram i figur 3-4.



Figur 3-4 Assesment of the potential to respond (Hollnagel, 2017, s. 70).

RAG er et eksempel på hvordan egenskapene kan måles i en organisasjon og er i denne sammenheng inkludert for å kunne operasjonalisere metodikken. Dette prosjektet omhandler kunnskapsoverføring og digitaliseringsprosesser og vil derfor benytte spørsmål som blant annet undersøker Lundins monitoreringsevne og indikatorbruk. Prosjektet hviler dermed på antagelsen om at hensiktsmessig kunnskapsoverføring i stor grad er basert på evnen til å monitorere. Evnen til å monitorere vurderes følgelig etter spørsmål og kriterier fra RAG.

På denne måten vil utdrag fra RAG benyttes til å vurdere hvorvidt Lundin oppfyller delkriterier for resiliens i måten selskapet ved å monitorere hendelser og forhold. Hensiktsmessig praktisering av kunnskapsoverføring vil naturlig nok ikke føre til resiliens i seg selv, men kan være et viktig element i veien mot resiliens.

I boken *Safety-II in Practice* foreslår Hollnagel et sett med diagnostiserings spørsmål i sin presentasjon av RAG. Disse spørsmålene har som formål å vurdere en organisasjons potensiale til å monitorere. Disse spørsmålene omhandler i stor grad utforming og bruk av indikatorer (Hollnagel, 2017, s. 61). Disse spørsmålene presenteres følgende i tabell 3-2.

Tabell 3-2 Spørsmål fra RAG, basert på Table 5.4 *Ex amples of detailed issues relating to the potential to monitor*

Egenskaper	Spørsmål
Indicator list	Does the organisation have a list of regularly used performance indicators?
Relevance	Is the list verified and/or revised on a regular basis?
Validity	Has the validity of indicators been established?
Delay	Is the delay in sampling indicators acceptable?
Sensitivity	Are the indicators sufficiently sensitive? Can they detect changes and developments early enough?
Frequency	Are the indicators measured or sampled with sufficient frequency? (Continuously, regularly, every now and then?)
Interpretability	Are the indicators/measurements directly meaningful or do they require some kind of analysis?
Organisational support	Is there a regular inspection scheme or schedule? Is it properly resourced? Are the results communicated to the right people and put into use?

(Hollnagel, 2017, s.61).

Et annet viktig argument bak valget om å fokusere på monitoreringsegenskapen, er inkluderingen av et mer proaktivt perspektiv på sikkerhetsstyring. Formålet med ledende indikatorer er å predikere fremtiden, og på denne måten kunne fange opp forhold med betydningen for sikkerheten. Monitoreringevnen til organisasjonen vil derfor ha stor betydning i et proaktivt sikkerhetsperspektiv, og vil kunne være avgjørende for hvorvidt man evner å fange opp forhold og avvik med betydning for sikkerheten. Det viktige betydningen av monitorering innenfor et resiliens-perspektiv understrekes også av Pettersen (2019) som i sin artikkel omtaler «Precursor Resilience» som en av flere typer resiliens. Precursor resilience beskrives som evnen til å monitorere forhold i et system og evnen til å gripe inn å korrigere dersom det oppstår uakseptable forhold. Behovet for monitorering understrekes også av tidligere forskning som peker på at mindre forhold over tid kan utvikle seg til ulykker og uønskede hendelser (Pettersen, 2019, s. 52).

3.2 Indikatorer og funksjoner

Reiman & Pietikäinen (2012) beskriver indikatorer som kvalitative eller kvantitative målinger som har som hensikt om å produsere informasjon om et interesseområde. I artikkelen «Leading indicators of system safety – Monitoring and driving the organizational safety potential» presenterer Reiman & Pietikäinen et teoretisk rammeverk for å anvende indikatorer tilknyttet sikkerhetsytelse i sikkerhetskritiske organisasjoner (Reiman & Pietikäinen, 2012, s. 1993). I artikkelen trekkes ledende indikatorer frem som et nyere tilskudd i sikkerhetslitteraturen, hvor bruk av etterslepene indikatorer har vært den mest etablerte praksisen. Det teoretiske rammeverket som presenteres i artikkelen er basert på et sosio-teknisk systemperspektiv på sikkerhet og innebærer med dette at et systems sikkerhet anses som en fremtredende egenskap av hele systemets funksjon. Dette innebærer både teknologi, mennesker, og interaksjonen som finner sted mellom mennesker og teknologi (Reiman & Pietikäinen, 2012, s. 1995). Sikkerhetsindikatorer beskrives følgelig som verktøy for evaluering og forbedring av systemets funksjon, og kategoriseres av forfatterne i tre kategorier: Drive-indicator, Monitor-indicator og Outcome-indicator.

Drive indicator

«Drive indicators» beskriver regelmessige målinger av aktiviteter som utføres med hensyn til sikkerhetsstyring i organisasjonen. Resultatene fra disse indikatorene benyttes i sikkerhetsstyringen ved å endre, vedlikeholde, forsterke eller redusere ulike parametere i organisasjonen.

Hovedfunksjonen til denne typen indikatorer er å lede den sosiotechniske aktiviteten ved å motivere for visse sikkerhetsrelaterte aktiviteter (Reiman & Pietikäinen, 2012, s. 1996).

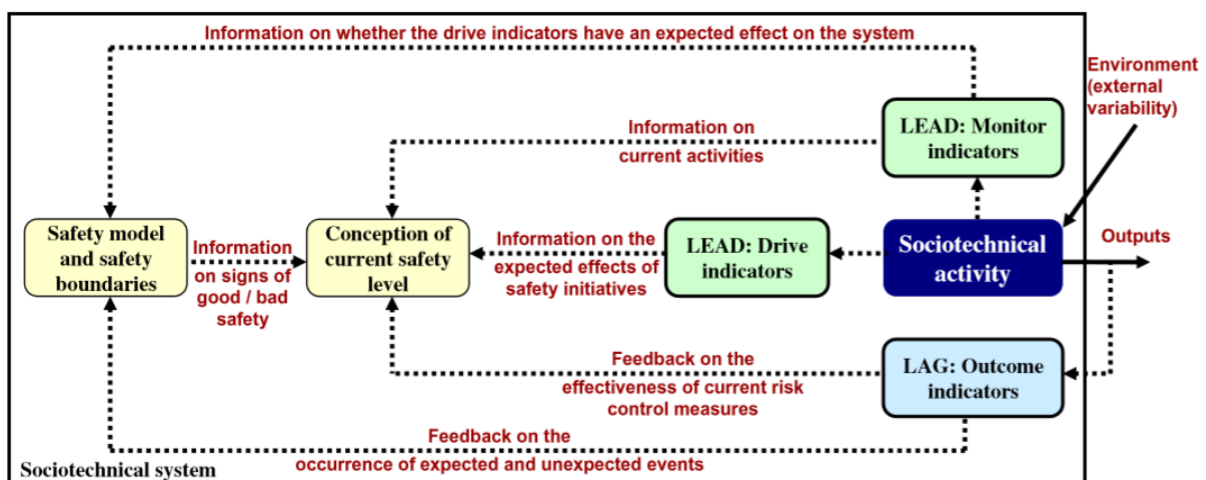
Monitor indicator

Monitor indicators er indikatorer som måler et systems evne og potensiale til sikker ytelse. Disse indikatorene overvåker dynamikken i sosio-tekniske systemer, og har som formål å gi informasjon om aktivitetene som utføres i systemet. Reiman & Pietikäinen (2012) foreslår også at slike indikatorer burde benyttes til å overvåke de eksterne omgivelsene som omringer organisasjonen. Formålet med dette er å innhente informasjon som bidrar til at organisasjonen i større grad kan forberede seg på forhold og tilstander forårsaket av eksterne endringer (Reiman & Pietikäinen, 2012, s. 1996)

Outcome indicators

Outcome indicators måler de konkrete resultatene fra systemet, altså et midlertidig sluttresultat av en kontinuerlig prosess eller en aktivitet. I praksis benyttes disse indikatorene ofte til å gi konklusjoner om sikkerhetsnivå eller valg av prioriteringer i sikkerhetsstyringen. Dette kan i praksis være en lite hensiktsmessig bruk av indikatorene, da de har en redusert evne til å reflektere det reelle sikkerhetsnivået i organisasjonen. Outcome indicators kan i midlertidig benyttes til å justere sikkerhetsbarrierer eller korrigerende tiltak i sikkerhetssystemer (Reiman & Pietikäinen, 2012, s. 1998).

Reiman & Pietikäinen illustrer de tre indikatorkategoriene i sin modell:



Figur 3-5 The extended system model showing the feedback from the indicators (Reiman & Pietikäinen, 2012, s. 1996).

3.3 Sikkerhet og sikkerhetsstyring

Da dette forskningsprosjektet har som formål å vurdere hvilken betydning kunnskapsoverføring har for sikkerheten i Lundin, vil det være viktig å redegjøre for betydningen av sikkerhetsbegrepet. Når man snakker om kunnskapsoverføring i en sikkerhetskontekst vil dette kunne betegnes som én eller flere prosesser som har til hensikt å øke eller opprettholde sikkerhetsnivået i organisasjonen. Slike prosesser vil dermed kunne inngå i en klassisk betegnelse på sikkerhetsstyring: «Alle tiltak som iverksettes for å oppnå, opprettholde og videreutvikle et sikkerhetsnivå i overensstemmelse med definerte mål» (Aven et al, 2004, s. 67). Norsk Standard (NS) definerer sikkerhet som «Reell eller oppfattet tilstand som innebærer fravær av uønskede hendelser, frykt eller fare» (NS, 5830, s. 2). Denne definisjonen har blitt selektert for dette prosjektet da den henviser til en tilstand, og baserer seg ikke utelukkende på reaktive målinger av frekvensvariasjon. En sikkerhetsdefinisjon hvor sikkerhet er definert og begrenset til en frekvensvariasjon formuleres ofte som fravær av uønskede hendelser. Sikkerhetsbegrepet brukes ofte i forbindelse med situasjoner hvor en ønsker å redusere sannsynligheten for, og konsekvensene av uønskede hendelser. Begrepet brukes også for å beskrive et systems evne til å unngå tap og skader (Aven et al., 2004, s. 17).

Man kan argumentere for at definisjoner basert på frekvensvariasjoner har mulige svakheter. En tilstand hvor uønskede hendelser har vært fraværende vil kunne oppleves som en sikker tilstand, og vil på denne måten oppfylle beskrivelsen av sikkerhet. Man kan likevel stille spørsmål hvorvidt et fravær av uønskede hendelser er det samme som en sikker tilstand eller sikkerhet. En organisasjon kan eksempelvis besitte en nærmest feilfri statistikk uten uønskede hendelser eller ulykker, hvor også de ansatte opplever høy sikkerhet. Et slikt fravær av uønskede hendelser vil samtidig ikke være en indikator for den reelle sannsynligheten for en uønsket hendelse i organisasjonen. En storulykke kan fortsatt være rett rundt hjørnet, på tross av statistikk som peker i en annen retning. Fraværet av uønskede hendelser kan eksempelvis være et resultat av rene tilfeldigheter og ikke en konsekvens av høy sikkerhet i organisasjonen.

I Norge er sikkerhetsbegrepet et bredt begrep som kan sies å inneha flere betydninger. Vi skiller i hovedsak mellom sikkerhet som tilstand og sikkerhet som følelse. Sikkerhet dekker også de engelske begrepene «safety» og «security».

I Skandinavia er det vanlig å definere «Safety» som sikkerhet i hensyn til ulykker, og «security» som sikkerhet mot tilsiktede handlinger, slik som ran og terrorisme (Engen, Kruke, Lindøe, Olsen, Olsen & Pettersen, 2016, s. 78). I dette prosjektets kontekst er det som tidligere nevnt valgt å definere sikkerhet som en tilstand, reell eller oppfattet, med et fravær av uønskede hendelser, frykt eller fare. Denne definisjonen vil kunne ha en større relevans i forbindelse med prosjektets sikkerhetsforståelse, og vil kunne være nyttig i undersøkelsen av Lundins kunnskapsoverføringsprosesser, særlig med hensyn ledende og etterslepene indikatorer

3.3 Sikkerhetsinformasjonssystemer og struktur

Sikkerhetsinformasjonssystemer (SIS) referer til organisasjoners systematiske tilnærming til styring av sikkerhet, og inkluderer organisatoriske strukturer, ansvar, retningslinjer og prosedyrer. Generelt inkluderer disse systemene flere komponenter som sikkerhetsledelse, utnevning av nøkkelpersonell, identifisering av farer og risikoreduksjon, granskning og revisjon, samt monitorering av sikkerhetstilstanden (Thomas, 2012). SIS har blitt et viktig verktøy innenfor sikkerhetsstyring. SIS er et system som benyttes til å styre og kontrollere sikkerhet. Prinsippene bak et SIS er at avvik fra normal drift registreres og lagres i et eget system for datalagring. I et SIS registreres avvik i form av ulykker og nesten-ulykker som er direkte knyttet til sikkerheten i organisasjonen. Datagrunnlaget benyttes til å analysere hendelsene før en senere utvikler og iverksetter risikoreducerende tiltak rettet mot de aktuelle hendelsene. Et SIS er kan beskrives som et avvikssystem, ettersom det benyttes til å registrere uønskede hendelser. Sikkerheten måles i denne sammenheng som en reduksjon av uønskede hendelser og avvik. SIS er i praksis et «feedback control»-system som kontinuerlig forsøker å korrigere avvik og forhold i nåtilstanden, som ikke samsvarer med forhåndsdefinerte mål i organisasjonen. Dette utgjør en styringsløyfe som reaktivt forsøker å forbedre systemet ved å redusere antall uønskede hendelser (Aven et al., 2004, s. 131).

Systemer for håndtering av avvik vil utgjøre en viktig del av kunnskapsoverføringen i en organisasjon, ettersom systemene tar sikte på å redusere uønskede hendelser og forhold ved å benytte kunnskap til å utføre endringer i organisasjonen. En kan dermed argumentere for at et SIS utgjør selve kjernen i kunnskapsoverføring. Dersom et SIS skal kunne fungere i praksis kreves det en hensiktsmessig datainnsamling. En vellykket datainnsamling vil være avhengig av flere faktorer i organisasjonen. Det er viktig at de ansatte som rapporterer ser nytten og betydningen av å rapportere. Rapporteringsprosessen må også bære preg av å være lite byråkratisk, og på den måten ikke føre til mye ekstraarbeid.

Et annet viktig moment er begrepsbruken i skjemaer for innrapportering. Det må eksistere en felles forståelse av begrepene og kategoriene som brukes i rapporteringsskjemaer slik at en reduserer sjansen for misforståelser. Det er også viktig at en unngår en syndebukk-mentalitet hvor frykten for sanksjoner fører til at ansatte ikke rapporterer inn hendelser (Aven et al., 2004, s. 131). Dette understreker også James Reason i sin litteratur, hvor han beskriver kriterier for hva som er viktig for en god rapporteringskultur (Reason.,1997, s. 197). Innsamlet data som er lagret i et SIS, vil kunne danne grunnlaget for analyser og eventuelle indikatorer i organisasjonen. Resultatet av disse analysene vil deretter bli spredt til beslutningstakere i ulike deler av organisasjonen. Tiltak vil deretter bli utarbeidet før de implementeres i systemet (Aven et al., 2004, s. 131).

3.3.1 Kriterier for et sikkerhetsinformasjonssystem

For at et SIS skal fungere best mulig er det som nevnt en rekke prinsipper som må følges. De følgende kriteriene for et SIS er inspirert av kontroll- og systemteoretiske forståelsesrammer, og kan betraktes som de viktigste kriteriene for funksjonen (Aven et al., 2004, s. 131-133):

- 1) **Relabilitet** - Dersom innsamlet data skal kunne brukes i analyser, er det viktig at datagrunnlaget er så nøyaktig og konsistent som mulig. Relabilitet i datagrunnlaget kan derfor anses som en viktig forutsetning for meningsfulle analyser.
- 2) **Validitet** - For at innsamlet data skal være representativt for tilstanden i organisasjonen, er det viktig at indikatorer og prestasjonsmål er dekkende for det man ønsker å måle. Data må gi et reelt og gyldig bilde av tilstanden i organisasjonen.
- 3) **Relevans** - Informasjonsflyten må være relevant for de beslutningstakere som mottar informasjonen. Det er derfor viktig at beslutningstakere ikke overbelastes med unødvendig informasjon, men mottar informasjon som er relevant for de beslutningsprosessene som skal utføres.
- 4) **Tilgjengelighet** - SIS må generere informasjon som er tilgjengelig til brukerne av systemet på en oversiktlig og lettvinnt måte.
- 5) **Tidsoptimalitet** - En for langsommelig informasjonsflyt vil kunne føre til at tiltak blir iverksatt for sent og en risikerer dermed at risikobildet har endret seg fra slik det opprinnelig var i utgangspunktet. Dersom dette er tilfelle vil det øke sannsynligheten for at tiltak ikke har ønsket effekt.
- 6) **Kosteffektivitet** - Et SIS må bidra til sikkerheten i organisasjonen, og det må derfor være et reelt behov for systemet. En kan dermed si at et SIS må gi mer sikkerhet per krone enn alternative løsninger.

- 7) **Forståelig og akseptert** - De operative delene av organisasjonen må være informert om formålet med et SIS. Det er også viktig at det eksisterer kollektiv aksept for behovet for datainnsamling, analyser og risikoreduserende tiltak blant de ansatte i organisasjonen (Aven et al., 2004, s. 131-133).

3.4 Digitalisering, psykologiske- og organisatoriske faktorer

I dette delkapittelet vil det redegjøres for hvordan digitalisering, psykologiske- og organisatoriske faktorer påvirker samspillet mellom mennesker og digitale systemer.

3.4.1 Digitalisering

Siden nedturen i petroleumsnæringen i 2014 har næringen hatt et gjennomgående fokus på effektivitet. I en større undersøkelse utført av DNV GL i slutten av 2018, svarte over 791 deltakere fra seniorstillinger i olje- og gassnæringen på spørsmål angående forventninger for 2019. 60% av deltakeren svarte at de forventet at deres selskap ville øke investeringen av digitalisering i 2019 (DNV GL, 2019A, s.30). Petroleumsnæringen befinner seg nå i en periode hvor det er stort fokus på effektivitet og kostnader, samtidig som ny teknologi introduseres. Denne perioden kan betegnes som en brytningstid hvor fokuset på utvikling av teknologi er høyt, samtidig som eldre systemer og arbeidsprosesser fortsatt råder (IRIS, 2018, s.9). Det finnes ingen konsensus bak definisjonen av begrepet digitalisering, og begrepet har ofte ulik betydning etter hvem som bruker det. I artikkelen «Digital Transformation on Purpose» (2017) fra MIT Sloan Management Review, presenterer Unruh og Kiron et rammeverk for å forstå digitalisering og skiller mellom tre viktige begreper: digitizing, digitalisering og digital transformasjon (Unruh & Kiron, 2017):

Digitizing er en beskrivelse av prosessen hvor en konverterer noe fra analogt til digitalt.	Digitalisering beskriver hvordan forretningsmodeller og prosesser endres for å utnytte digitizing.	Digital transformasjon beskriver endringer på et høyere samfunnsnivå, hvor institusjoner og økonomiske endringer oppstår som en konsekvens av digitalisering og digitizing.
--	---	--

I dette forskningsprosjektet anses det som hensiktsmessig å snakke om digitalisering tilknyttet systemer for kunnskapsoverføring. Digitizing og digitalisering er som beskrevet ovenfor en del av en digital transformasjon som påvirker petroleumsnæringen. I denne sammenhengen er det derfor mest interessant å se på hvordan interne prosesser påvirkes og endres av digitalisering.

Samtidig som digitalisering vil kunne ha positiv effekt på effektivisering av prosesser tilknyttet HMS, vil sammenslåing av IKT og utvidelser av systemers funksjonalitet kunne medføre utfordringer. Systemforståelsen til brukerne av systemene vil kunne svekkes som en direkte konsekvens av digitaliseringen, da man risikerer at de underliggende antagelsene og forutsetningene som ligger bak systemene blir mindre synlig. Dette vil igjen kunne resultere i svekkede beslutningsprosesser som følge av beslutningstakeres begrensede systemforståelse. I slike prosesser risikerer man å miste oversikten over det reelle sårbarhetsbildet ved at det oppstår en fremmedgjøring mellom brukerne og de digitale systemene (IRIS, 2018, s. 14-15).

Fremmedgjøring har som fenomen blitt benyttet til å beskrive sentrale deler av hendelsesforløp i flyulykker. I slike tilfeller har piloter mistet oversikten over de opprinnelige intuisjonene bak systemene, og handlet feil (Carr, 2014 referert i IRIS, 2018, s. 42). Karl Weick (2001) beskriver hvordan fremmedgjøring er tilknyttet det han kaller «Sensemaking» i forbindelse med introduksjon av nye teknologier (Weick, 2001 referert i IRIS, 2018, s. 42). Nye systemer med økt kompleksitet og lite synlige prosesser som følge av forenklet visualisering, vil kunne føre til utfordringer tilknyttet denne meningsdannelsen. Systemer vil ofte være utsatt for stadige oppdateringer og endringer, noe som vil medføre utfordringer tilknyttet bruk og meningsdannelse. Når de underliggende intuisjonene bak systemene blir usynlige vil dette kunne påvirke risikopersepsjon som igjen påvirker beslutningstaking (Weick, 2001, i IRIS, 2018, s. 42). Carr (2014) beskriver også hvordan «Automation bias» kan føre til utfordringer i digitaliseringsprosessen. Ved «Automation bias» oppstår en form for kunstig tillit til resultatene som systemene produserer, hvor brukerne oppfatter data som korrekt ettersom det er produsert av en maskin. Carr understreker også hvordan gevinsten i form av effektivisering fra automatisering og digitalisering til dels må betales som tap av menneskelig intuisjon i systemene (IRIS, 2018, s. 42)

3.4.2 Psykologiske- og organisatoriske faktorer

Kriterier for SIS som ble beskrevet i delkapittel 3.3 tar utgangspunkt i en generell beskrivelse av et SIS, og struktur og utforming vil naturligvis variere etter selskap. Som tidligere nevnt er operatørselskaper i petroleumsnæringen pålagt å registrere og undersøke uønskede hendelser og forhold. SIS som verktøy er allerede etablert i oljebransjen, men det er ikke gitt at en organisasjon som oppfyller disse kriteriene vil ha et velfungerende SIS, eller at et SIS har en positiv effekt på sikkerhetsarbeidet i selskapet.

«Empiriske evalueringer av ulike SIS-er har stort sett konkludert med at SIS i flertallet av tilfellene ikke klarer å oppfylle kravene, og at SIS i noen tilfeller faktisk kan ha en negativ effekt på sikkerhetsarbeidet i organisasjonen» (Aven et al., 2004, s.133). Aven trekker frem fem ulike organisatoriske- og psykologiske faktorer som påvirker den praktiske bruken av et SIS:

Attribusjon - Attribusjon viser til de psykologiske mekanismene som påvirker hvordan vi forstår årsaksforhold til hendelser. I etterkant av en ulykke vil involverte personer være mer tilbøyelige til å skyldes på tekniske, eller andre ikke-menneskelige faktorer som årsaksforhold. Alvorlige ulykker eller hendelser vil oftere bli forklart som menneskelig svikt. Dersom personene som gransker ulykken har viktige fellestrekk med de som er involvert i ulykken, vil granskerne være mer tilbøyelige til å vektlegge labile egenskaper som årsaksforhold. Et eksempel på dette er å skyldes på sviktende konsentrasjon hos operatører som årsak til ulykke. Dette fenomenet vil igjen kunne føre til at informasjon om reelle kausale forhold i et SIS vil kunne påvirkes av feilrapportering og systematiske skjevheter (Aven et al., 2004, s.134).

Insentivstruktur - Insentivstruktur viser til hvordan sanksjoner og belønninger blir brukt i forbindelse med rapportering av avvik og uønskede hendelser. Både beskrivelse av hendelse og selve innrapporteringen vil være direkte knyttet til insentivstrukturen i organisasjonen. Insentivstruktur vil derfor kunne by på utfordringer for ledelsen i organisasjonen, ettersom en både ønsker et lavt antall avvik, men samtidig ønsker flest mulig innrapporteringer. En operativ del av organisasjonen vil ofte være mer tilbøyelig til å rapportere inn forhold som kan resultere i belønninger, kontra sanksjoner. Dersom operativt personell føler at SIS blir brukt til å forfølge og overvåke de ansatte vil dette naturligvis påvirke villigheten til å bruke systemet (Aven et al., 2004, s.135).

Filter - Filter viser til de mekanismene som påvirker hvordan informasjon passerer gjennom ulike nivåer i et SIS. Etersom informasjonsflyten innebærer at informasjon passerer ulike avdelinger og personell, vil informasjonen i denne prosessen passere forskjellige filtre. Slike filtre kan oppstå i form av kvalitetssikring av informasjon, eller andre områder hvor informasjon blir fortolket og videreformidlet. Et uoffisielt filter vil kunne være en leder som endrer en rapport dersom han er uenig i innholdet. Både offisielle og uoffisielle filtre som informasjon passerer igjennom vil kunne sammenlignes med viskeleken, hvor sluttresultatet er informasjon som ikke nødvendigvis samsvarer med reelle forhold (Aven et al., 2004, s.135).

Lokal kunnskap - Det vil kunne oppstå forskjeller mellom den forenklete og formaliserte informasjonen som ligger i et SIS og den rike situasjonsbestemte informasjonen som ligger i den operative delen av en organisasjon. Differansen mellom disse kunnskapsnivåene kan føre til at operativt personell opplever rapportering av tiltak som lite hensiktsmessig (Aven et al., 2004, s.135).

Organisatoriske rammebetingelser og struktur - Rammebetingelser og struktur er overordnede forhold som vil kunne påvirke hvordan informasjon samles og analyseres. Eksempler på slike forhold er rapporteringsprosedyrer og retningslinjer for databehandling. Selve strukturen til et SIS vil legge føringer for hvilken informasjon det er mulig å registrere og hvor lett det oppleves å registrere informasjonen. Hensiktsmessige kategoriinndelinger vil være en viktig faktor, ettersom det legger føringer for hvordan informasjonsflyten styres (Aven et al., 2004, s.136).

4.0 Metode

I dette kapitlet vil det bli redegjort for metodiske valg som har blitt utført i forbindelse med arbeidet for å besvare problemstillingen og de tilhørende forskningsspørsmålene. Det vil også bli redegjort for begrunnelsene bak de metodiske valgene som har blitt utført, og om hvorfor valgt metodikk anses som mest relevant og hensiktsmessig for å besvare oppgavens problemstilling. Ved å besvare problemstillingen i dette prosjektet vil man kunne belyse hvorvidt standardiserte og etablerte digitale systemer bidrar til å styrke og/eller opprettholde sikkerhetsnivået i Lundin Norway. Forskingen i denne oppgaven omhandler en organisasjon som enhet, og søker å besvare hvordan organisasjonens systemer kan bidra til en form for resiliens i tråd med teori om RE. Det første delkapitlet vil presentere valg av forskningsdesign og hvorfor de valgene som er utført anses som relevant for oppgavens problemstilling. Videre vil forskningsstrategi og datainnsamlingen i form av forskningsintervjuer og dokumentanalyse bli presentert, etterfulgt av praktiske erfaringer i forbindelse med innsamlingen, samt sterke og svake sider ved de valg som er utført. De siste delkapitlet vil forsøke å vurdere den helhetlige kvaliteten på det forskningsarbeidet som har blitt utført. Dette innebærer kritiske refleksjoner med hensyn til validitet, reliabilitet og etikk.

4.1 Forskningsdesign

Et forskningsdesign viser til hvordan valg av metode, informantutvalg og analyseopplegg sammen skal svare på oppgavens problemstilling (Thagaard, 2018, s. 45). Forskningsdesignet kan anses som en oppskrift eller plan for hva, hvem, hvor og hvordan en undersøkelse skal utføres, og hva den skal være rettet mot (Thagaard, 2018, s. 50). Det overordnede målet til en kvalitativ oppgave er å utvikle data som utgjør et relevant bidrag i tråd med foreliggende kunnskap på området (Thagaard, 2018, s. 48). I denne studien utgjør dette i praksis hvorvidt digitale systemer for behandling av sikkerhetsrelevant informasjon kan bidra til resiliens i Lundin Norway. For å besvare denne problemstillingen var det nødvendig med en datainnsamlingsmetode som effektivt samlet inn relevant data, med hensyn til validitet og reliabilitet.

Ved å innhente data om organisasjonen Lundin Norway, på bakgrunn av intervjuer og dokumentanalyser fra HSEQ-avdelingen i organisasjonen, vil oppgavens metodikk ha en tydelig avgrensning, og vil innebære dybdeinformasjon om få enheter. Studien vil derfor utgjøre en kvalitativ case-studie.

Case-studier kjennetegnes ved innhenting av mye informasjon om få enheter, og case viser i denne sammenheng til en avgrenset kontekst (Thagaard, 2018, s. 51). Den avgrensede konteksten er i denne studien både Lundin Norway, HMS-avdelingen, og de digitale systemene som benyttes for behandling av sikkerhetsrelevant informasjon.

Jacobsen (2015) skiller mellom intensive og ekstensive design. Intensive design fokuserer på dybde, har ofte få undersøkelsesobjekter, og man får detaljert informasjon om hver enhet. Dette designet sier noe om tilnæringsmetoden i forskningen, og selv om man kan si at et intensivt forskningsdesign vil gi data som er mindre generaliserbart, vil forskningen potensielt kunne utvikle data med større teoretisk generaliseringspotensiale. Ekstensive design handler om bredde, og sier noe om antall undersøkelsesobjekter man ønsker å betrakte. Man vil få lite informasjon om hver enhet, selv om dataen vil kunne ha større statistisk generaliseringskraft (Jacobsen, 2015, s. 133).

For dette forskningsprosjektet var det mest hensiktsmessig å gjennomføre et intensivt undersøkelsesdesign av flere årsaker. Forskningsspørsmålene søker å kartlegge hvordan større prosesser utføres ved bruk av digitale systemer, og det var derfor meningsfullt å innhente dybde informasjon om systemer og praktisk bruk. For å kunne besvare spørsmål om monitorering, systematisering, og distribuering vil det i større grad kreves dybde data. Det er derfor ikke ønskelig å innhente data som sier noe om overfladiske brukererfaringer av systemene, men heller data som sier noe om vesentlige funksjoner i Lundins SIS. Det å gå i dybden betyr at man forsøker å få fram så mange nyanser og detaljer som mulig av det valgte fenomenet. Det var også ønskelig å innhente data om hvordan informantene opplever systemene de benytter, dette støttes også av Jacobsen (2015) da det å få en så helhetlig forståelse som mulig av forholdet mellom informantene og den konteksten de inngår i er mulig i når man går i dybden framfor bredden (Jacobsen, 2015, s. 133).

4.2 Forskningsstrategi

Jacobsen (2015) skriver at en strategi er induktiv når man samler inn empiri uten at man på forhånd har for mange antagelser, og deduktiv når man begynner med noen antagelser og deretter samler empiri for å bekrefte eller avkrefte disse (Jacobsen, 2015, s. 29). Dette prosjektet anses å ha en deduktiv strategi, da det søker å benytte etablert teori om resiliens for å undersøke systemer for kunnskapsoverføring i Lundin.

Det teoretiske grunnlaget man får ved å studere sikkerhetsstyringslitteratur vil i seg selv gi antakelser om hvordan sikkerhetsstyring fungerer i praksis. Kunnskapsoverføring ble også trukket frem som et interessant tema ved de innledende fasene av samarbeidet mellom Lundin og undertegnede. Samarbeidet ble også igangsatt i etterkant av et lengre opphold hos Lundin i forbindelse med en sommerjobb. Den kunnskapen som ble opparbeidet ved dette oppholdet kombinert med kunnskapen fra de innledende møtene vil utvilsomt ha medført til antakelser om de digitale systemene som denne studien forsker på. Denne kunnskapen ble også tatt i betraktning under beslutningsprosessene ved valg av teori. Tidligere forskning har trukket frem visse systemer og prosesser som vil kreve større fokus i fremtiden, og innenfor RE trekkes resiliens frem som motsvaret til systemers økende kompleksitet som følge av digitalisering. Studien er derfor til dels basert på antakelsen om at resiliens styrker sikkerhet, slik som RE også hevder.

Ifølge Thagaard (2018) innebærer en deduktiv tilnærming at forskeren utvikler analytiske rammer på bakgrunn av etablert teori. En analytisk ramme gir grunnlag for å forstå mønstre i dataen” (Thagaard, 2018. 194). Det analytiske rammeverket for denne oppgaven tar utgangspunkt i teori om resiliens og SIS, indikatorbruk og digitalisering. Dette rammeverket ble brukt til å analysere delfunksjoner som sammen utgjør Lundins systemer for kunnskapsoverføring.

4.2.1 Intervju som metode

I dette forskningsprosjektet er formålet å undersøke funksjonene som utgjør de digitale systemene for kunnskapsoverføring. For å kunne foreta hensiktsmessige undersøkelser anses det som viktig å belyse flere aspekter ved disse systemene. Dette innebærer å undersøke systemene fra både et teoretisk og praktisk perspektiv. Ved å undersøke systemene fra et teoretisk perspektiv vil formål, retningslinjer og systemenes utforming kunne redegjøres for. I denne delen av innsamlingen ble det tydeliggjort hvilke forutsetninger for kunnskapsoverføring systemene legger. For å videre kunne innhente data om forutsetninger og praktiske bruk, ble det anset som et naturlig neste steg å intervju informanter med direkte eller indirekte tilknytning til systemene. Hvordan systemene oppleves i det daglige, og hvorvidt det er mangler eller utelatte områder knyttet til systemenes funksjoner er sentrale spørsmål som intervjuene hadde som formål å besvare. Intervjuene ble også benyttet for å redegjøre hvorvidt studiens teoretiske rammeverk er synlig i Lundins tilnærming til sikkerhetsstyring. På denne

måten ble spørsmål formulert på en måte som også forsøkte å lete etter paralleller mellom det teoretiske grunnlaget for studien og Lundins praksis.

Det ble derfor valgt å intervju både brukere, systemadministratorer, og andre ansatte som benytter seg av kunnskapen som distribueres fra systemene.

Thagaard, (2018) beskriver intervju som en egnet metode for å bygge kjennskap til intervjuobjektene ved å lære hvordan de opplever og forstår seg selv og sine omgivelser. I denne sammenhengen er det viktig å fortolke intervjudata i lys av nettopp slike sosiale og kulturelle rammer (Thagaard, 2018, s.58). Intervjuene som ble foretatt ved Lundin var i stor grad farget av de kontekstuelle rammene som omringet intervjuprosessen. Alle informantene er ansatt ved Lundin og er derfor i ulik grad påvirket av sine relasjoner med Lundin som arbeidsgiver. Det var derfor viktig å formulere både åpne spørsmål, men også spørsmål som var mer direkte. Mer direkte spørsmål ble benyttet i deler av intervjuguiden for å unngå at informantene kom med svar som var basert på selskapets interesser, men heller ga et direkte svar på spørsmålet som ble stilt. De interaksjonene som forekommer mellom intervjuobjekt og forsker kan også betraktes som en sosial handling, hvor intervjuobjektene vil rettferdiggjøre sine egne erfaringer og plassere sine opplevelser innenfor de kulturelle rammene som de befinner seg i (Thagaard, 2018, s. 53). Alle informantene ble fortalt hensikten med studien, og som en del av denne samtalen ble det forklart at studiens hensikt ikke var å finne feil, men heller å undersøke hvordan Lundin utfører kunnskapsoverføring ved bruk av digitale systemer. Alle informantene ga dermed uttrykk for at de hadde forståelse av studiens hensikt.

4.2.2 Utvalg av informanter

Utvalget av informanter er i dette forskningsprosjektet basert på informasjon om organisasjonsstruktur og ansvarsfordeling innhentet ved hjelp av dokumentanalyser og samtaler med kontaktpersoner i selskapet. Det ble utført samtaler med kontaktpersoner i Lundin Norway i forkant av datainnsamlingen, hvor tilgjengelige og relevante informanter ble kartlagt. Basert på strategisk utvelging, ble informanter valgt ut og intervjuet. Strategisk utvelging baseres på en systematisk utvelgelse av personer eller enheter som besitter kvalifikasjoner eller andre egenskaper som er strategiske med hensyn til datainnsamling og besvarelse av problemstillingen (Thagaard, 2018, s. 54). Tilnærmingen til informantsutvelgelse tok også utgangspunkt i kriteriebasert utvalg av informanter hvor valg av informanter baserte seg på

informasjonen som var ønsket å innhente underveis i prosjektskrivingen. Informantene ble intervjuet en etter en, helt til datainnsamlingen ikke lengre tilførte ny informasjon til prosjektet og til det ble oppnådd det som opplevdes som en teoretisk metning i datautvalget.

Med disse kriteriene som grunnlag for informantutvelgelsen, ble det i dette prosjektet valgt å intervju syv informanter med følgende tilhørighet:

Tabell 4-3 Informantutvalg

Tittel	Avdeling	Fagområde
Informant nr. 1	HSEQ	Rådgiver
Informant nr. 2	HSEQ	Operativ-HSEQ
Informant nr. 3	HSEQ	Rådgiver
Informant nr. 4	HSEQ	Rådgiver
Informant nr. 5	Drift	Document controller
Informant nr. 6	HSEQ	Teknisk sikkerhet
Informant nr. 7	HSEQ	Risikostyring

Alle informantene hadde en direkte tilknytning til HMS-avdelingen ved Lundin, og dette er en faktor som kan ha bidratt til det som opplevdes som en teoretisk metning etter syv intervjuer. Det er også verdt å bemerke seg at Lundin er en liten organisasjon med omtrent 370 ansatte. De syv informantene utgjør derfor en betydelig andel av organisasjonen og spesielt HMS-avdelingen. Dette er også en faktor som taler for et datagrunnlag som er representativt for kunnskap og holdninger som besittes av de ansatte ved HMS-avdelingen hos Lundin.

4.3 Datainnsamling

Blaikie (2010) skiller mellom primær-, sekundær- og tertiærdata. Primærdata er innsamlet av forskerne selv med det formålet å besvare et konkret forskningsspørsmål. Sekundærdata er ikke samlet inn av forskerne selv, men er det som kan kalles rådata. Dette kan for eksempel være offentlig statistikk, eller datagrunnlaget fra et annet forskningsprosjekt som ikke har blitt analysert. Tertiærdata er data som er blitt analysert, enten av forskerne som samlet den inn eller av forskere som har benyttet sekundærdata (Blaikie, 2010, s. 160). I dette prosjektet benyttes data fra dokumenter og intervjuer innsamlet av forskeren og blir derfor betegnet som primærdata. Primærdata er i denne studien brukt som betegnelse på data innsamlet ved bruk av intervjuer med nøkkelinformanter i Lundin Norway, prosessstyringsdokumenter og dokumenter fra internrevisjoner i Lundin.

Blaikie (2010) skriver at det er lettere for forskere å bedømme kvaliteten på primærdata enn på sekundær og tertiærdata, da de har kontroll og oversikt over produksjonen og analysen av data. Dette prosjektet vil i all hovedsak basere seg på primærdata, da det er ønskelig å innhente data som belyser vesentlige funksjoner i Lundins SIS, både i form av dokumenter og ved intervju. Det foreligger ikke et datagrunnlag som har blitt analysert med dette til formål, og innsamlet data får derfor betegnelsen primærdata i denne studien. Blaikie (2010) skriver videre at prosessen med å bevege seg fra primærdata til tertiærdata ofte er utilgjengelig for forskerne som benytter den, og at tertiærdata derfor behandles med varsomhet. Da tertiærdata uansett har begrenset verdi, vil de utviklede dataene i dette prosjektet kunne gi større teoretisk generaliseringskraft, enn når man delvis eller helt baserer datainnsamlingen på tertiærdata (Blaikie, 2010, s. 161).

For å kunne samle inn relevant data om systemene som benyttes for kunnskapsoverføring av sikkerhetsrelevant informasjon var det naturlig å rette søkelyset mot den delen av organisasjonen som har dette fagområdet som sitt ansvar, altså Lundins HMS-avdeling. Lundin Norway opererer med avdelingen HSEQ som er avdelingen for HMS-, og kvalitetssikringsarbeid. Ved å gjennomgå styringsdokumenter og andre relevante dokumenter med retningslinjer og informasjon om sikkerhetsinformasjonssystemene ble dokumentanalyser benyttet for å danne et informasjonsgrunnlag om sikkerhetsinformasjonssystemene. I denne fasen av datainnsamlingen var hensikten å innhente informasjon om systemenes formål, struktur, utforming og retningslinjer. Neste fase av datainnsamlingen var å utføre intervju av nøkkelpersonell ved HSEQ-avdelingen. Intervjuer av systemadministratorer og brukere av systemet vil ha som formål å kartlegge hvordan systemene fungerer i praksis og hvorvidt det er forhold som ikke samsvarer med foreliggende dokumentasjon. Intervjuene tilførte også informasjon som ikke ble synliggjort ved å gjennomgå dokumenter.

4.3.1 Gjennomføring av intervjuene

Dette prosjektet ble gjennomført ved et kartleggingsmøte etterfulgt av to opphold ved Lundin Norways hovedkontor på Lysaker. Under kartleggingsmøtet ble mulige tematikker og problemstillinger diskutert, samtidig som mulige informanter ble kartlagt. Møtet klargjorde også hvilke datoer som passet for datainnsamling, med hensyn til informanter og kontaktpersoner. I forkant av oppholdene var det planlagt å intervju tre informanter med nær

tilknytning til Lundins SIS. Under oppholdene ble ytterligere informanter utvalgt basert på kriterier som tilsa at informantene kunne besitte kunnskap med interesse for prosjektet. Under det første oppholdet ble 4 informanter intervjuet ved hjelp av lydopptaker og en intervjuguide utarbeidet på forhånd. Data som ble samlet inn under dette oppholdet dannet grunnlaget for det neste oppholdet, og medførte noen mindre endringer i intervjuguiden. Se vedlegg. Det første oppholdet bidro også til å tydeliggjøre hvilke informanter det var ønskelig å intervju under neste opphold. Relevante dokumenter ble samlet inn kontinuerlig under begge oppholdene. Alle lydopptak ble slettet i etterkant av transkriberingen, og data ble oppvart forsvarlig før det ble benyttet i studien.

4.5 Datareduksjon og dokumentanalyse

I denne studien ble det samlet inn flere skriftlige datakilder i underveis prosessen med å kartlegge kunnskapsoverføring med hensyn til sikkerhet. De følgende kildene ble benyttet i prosjektet:

Tabell 4- 4 Presentasjon av skriftlige datakilder

Dokumenter	Formål	Relevans til studien
Audit Report – Execution and learning from investigations	Revisjon av alle interne granskinger av uønskede hendelser. Fra 2015 - 2017	Dokumentet gir et bilde av prosesser tilknyttet kunnskapsoverføring i forbindelse med interne granskinger.
Experience transfer / Lessons Learned	Internt styringsdokument for prosesser tilknyttet Kunnskapsoverføring i form av Lessons Learned	Dokumentet gir en oversikt over arbeidsprosesser, roller, kompetansekrav, samt et visuelt prosesskart for prosesser tilknyttet Lessons Learned.
Incident management	Internt styringsdokument for prosesser tilknyttet håndtering av rapporteringsverdige hendelser.	Dokumentet gir en oversikt over arbeidsprosesser, roller, kompetansekrav og prosesskart for alle prosesser fra innrapportering til lukking rapporteringsverdige hendelser.
Onepager / Lessons Learned Mal	Mal for utforming av Lessons Learned-dokumenter	Dokumentet er en mal for hvordan Lessons learned-dokumenter skal utformes. Se figur 5-16.

Dokumentanalyse er et sentralt virkemiddel innenfor kvalitativ metode, og vil i denne oppgaven utgjøre datainnsamlingen som omhandler styringsdokumenter og andre skriftlige datakilder som vist i tabell.

Enkelte teoretikere har hevdet at betegnelsen dokument i en kvalitativ sammenheng viser til alle de former for skriftlige kilder som forskeren har tilgjengelig for sine analyser (Thagaard, 2018, s. 118). Ved å utføre dokumentanalyser vil en utarbeide data på bakgrunn av innholdet i de dokumentene en undersøker. Det vil derfor være vesentlig å vurdere dokumentene en ønsker å benytte, mot flere kriterier.

Innenfor dokumentanalyser er det spesielt viktig å vurdere kildene med hensyn til konteksten som kildene er utarbeidet innenfor (Thagaard, 2018, s. 119).

Thagaard beskriver i sin bok; «Systematikk og innlevelse», flere trinn som bør følges når en skal vurdere en dokumentkilde (Thagaard, 2018, s. 119). Det første trinnet en bør rette søkelyset mot er relevansen til dokumentet. Hvorvidt et dokument er relevant for problemstillingen er åpenbart viktig. I denne prosessen er det naturlig å vurdere hvordan ulike dokumenter kan bidra til ulik informasjon, med hensyn til problemstillingen. Det andre trinnet en bør utføre er å vurdere dokumentets autenticitet. Autenticitet beskriver i hvilken grad dokumentet er ekte, og om en kan stole på opphavspersonen (e). Det neste trinnet i dokumentanalyseprosessen er å vurdere dokumentets troverdighet. I denne vurderingen er det vesentlig å stille spørsmål ved hvilke motiver som ligger bak utarbeidelsen av dokumentet og hvordan disse motivene påvirker innholdet. Ved å stille slike spørsmål vil en i prosessen redegjøre for hvorvidt en kan ha tillit til informasjonen og innholdet i dokumentet (Thagaard, 2018, s. 119). Alle dokumentene som ble hentet ved datainnsamlingen er dokumenter utarbeidet internt i organisasjonen, altså av Lundin og for Lundin. Dokumentene har blitt valgt ut da de inneholder informasjon som bidrar til å besvare prosjektets problemstilling, og ble derfor ansett som relevante. Men relevans vil også være betinget av autenticitet og troverdighet som Thagaard (2018) beskriver. Alle dokumentene er tilgjengelige for hele Lundin som organisasjon og er utarbeidet som offisielle dokumenter og veiledere, det var derfor få eller ingen synlige årsaker til å betvile dokumentenes autenticitet. Troverdigheten til dokumentene og deres innhold ble ansett som det største usikkerhetsmomentet i denne sammenhengen.

Det opplevdes ikke at det eksisterte årsaker til å betvile troverdigheten til styringsdokumenter og mal for Lessons Learned. Dokumentet «Audit Report – Execution and learning from investigations» er en rapport som redegjør for etterlevelsen hendelsesgransking i årene 2015 – 2017. Rapporten har som formål å vurdere det arbeidet som har blitt utført i forbindelse med granskinger, og er utarbeidet internt i selskapet. Uten at det finnes åpenbare årsaker til å betvile dokumentets troverdighet, er det likevel rimelig å anta rapportens vurderinger vil kunne være påvirket av å være utarbeidet internt i organisasjonen.

For å kunne verifisere innholdet i større grad, ble det derfor valgt å inkludere spørsmål om rapporten i intervjuguidene. Studien har også som hensikt å vurdere arbeidsprosesser i Lundin, og interne dokumenter var derfor av interesse uavhengig av andre faktorer.

Det er vanlig å benytte seg av dokumenter for å danne bakgrunnsinformasjon når en undersøker organisasjoner. Ved å gjennomgå og analysere relevante dokumenter vil en kunne danne et grunnlag som bidrar til at intervjuer og andre supplerende undersøkelser blir betydningsfulle. Denne oppgaven er som tidligere beskrevet en case-studie, som følger av et begrenset omfang med hensyn til enheter. (Thagaard, 2018) beskriver hvordan det i kvalitative studier med begrenset omfang er særlig viktig å finne settinger i organisasjonen som er strategiske for videre analyser. I denne oppgaven vil de videre analysene bestå av intervjuer av relevante informanter. Ved å analysere dokumenter om organisasjonen hvor en skal utføre prosjektet vil en klargjøre hvilke settinger og områder av organisasjonen som er mest relevant å studere med hensyn til oppgavens problemstilling (Thagaard, 2018, s. 119-120). Det ble derfor valgt å fokusere på HMS-avdelingen i dette studien.

4.6 Styrker og svakheter ved designet

For at forskning skal bli ansett som generaliserbar og troverdig bør den være pålitelig og gyldig (Ringdal, 2018, s. 247). Reliabilitet viser til datamaterialets etterprøvnbarhet og pålitelighet, og beskriver hvorvidt en annen forsker som benytter de samme metodene vil kunne komme frem til de samme resultatene, og er knyttet til repliserbarhet. I kvalitative undersøkelser vil det kunne betviles om hvorvidt reliabilitet vil kunne oppnås. Reliabilitet har sin opprinnelse fra positivistisk forskningslogikk hvor resultatene er uavhengige av relasjonene mellom forsker og informant. Fra et konstruktivistisk perspektiv ses data som noe som produseres i prosesser gjennom samarbeid mellom forsker og informant. Ifølge forhold i denne logikken blir reliabilitet lite relevant. Forskeren kan ikke oppfattes som uavhengig i sin relasjon til informanten når studien baserer seg på menneskelig interaksjon.

Som motvekt til dette anbefales det å gjøre forskningsprosessen, teori og data så gjennomskiktig som mulig (Thagaard, 2018, s. 202). I denne studien har det blitt produsert data fra både dokumenter og intervjuer, og i lys av betraktningene til Thagaard (2018) vil det være mest hensiktsmessig å vurdere reliabiliteten knyttet til data innsamlet ved bruk av intervjuer. Det er naturlig nok vanskelig å stadfeste hvorvidt studien har produsert etterprøvnbar data, da data produseres i prosesser ved samarbeid mellom forsker og informant.

Det er allikevel grunn til å tro at beskrivelser av systemer omhandler noe fysisk og håndfast og derfor vil være etterprøvbart. På en annen side vil informantenes betraktninger om brukererfaringer fra systemene og organisasjonen være subjektivt betinget av de sosiale og kulturelle rammene som omringer intervjusituasjonen. Denne dataen vil derfor kunne være påvirket av tillit og troverdighets forhold mellom forsker og informant. Det opplevdes allikevel ikke at dataens reliabilitet ikke hadde noen nevneverdige svakheter, som følge av spørsmål som var rettet mot konkrete prosesser og systemer. Det allikevel ikke med sikkerhet utelukkes at det finnes svakheter i datagrunnlaget, da dette i større grad krever en mulighet til å etterprøve resultatene.

Validitet omhandler en undersøkelses gyldighet og ser om resultatene fra de innsamlede dataene faktisk er knyttet til undersøkelsen, og ikke ytre faktorer (Jacobsen, 2015, s. 230). I datainnsamlingsprosessen ble det benyttet lydopptaker og intervjuene ble transkribert. Å benytte seg av lydopptaker vil gi større mulighet til å fokusere på informantene og vil kunne fristille forskeren til å stille gode oppfølgingsspørsmål. Ved å transkribere intervjuene vil det også være mulig å sitere informantene og redusere sannsynligheten for misforståelser, noe som igjen kan være med å styrke validiteten.

For dette forskningsprosjektet er det kun benyttet informanter som er ansatt i Lundin Norway. Dette vil potensielt kunne svekke dataens validitet, ettersom informantene ikke nødvendigvis vil dele informasjon som svekker deres egen posisjon i selskapet. Informantutvalget for dette prosjektet utgjør en betydelig andel av ansatte ved HSEQ-avdelingen, og dette vil kunne styrke validiteten da studien til syvende og sist ønsker å kartlegge informasjon og holdninger fra avdelingen som til daglig jobber med kunnskapsoverføring.

4.7 Ethiske refleksjoner

Denne studien ble utført våren 2019 i etterkant av et lengre opphold i forbindelse med en sommerjobb hos Lundin. Undertegnede tilbragte 2 måneder ved hovedkontoret til Lundin sommeren 2018. Dette oppholdet resulterte naturligvis i en rekke relasjoner og inntrykk av organisasjonen. Det har derfor vært viktig å ivareta en forskerrolle så objektiv som mulig underveis i arbeidet med dette prosjektet. En kan argumentere for at denne bevisstgjøringens tilstedeværelse underveis i prosjektet har bidratt til objektivitet i forskingen.

Samtidig er det vanskelig å eliminere alle antakelser og inntrykk man har som menneske, både bevist og underbevist. Det kan derfor ikke med sikkerhet utelukkes at personlige antakelser og refleksjoner ikke har påvirket dette forskningsprosjektet, selv om dette har vært en problematikk som har forskeren har vært bevist på.

Alle informantene fikk tilsendt intervjuguide med spørsmål og prosjektbeskrivelse på forhånd av intervjuene. Thagaard (2018) beskriver at informert samtykke må innebære at informantene underveis i prosjektet har en rett til å avbryte sin deltakelse uten at dette har konsekvenser for dem (Thagaard, 2018, s. 26). Informantene ble informert om at de kunne trekke sin deltakelse når de måtte ønske, også etter at intervjuene og oppholdet hos Lundin var avsluttet. Det ble også utvekslet kontaktinformasjon som informantene kunne benytte dersom de hadde slike ønsker.

Thagaard (2018) beskriver betydningen av konfidensialitet som viktig for etisk forsvarlig forskning. «De som gjøres til gjenstand for forskning, har krav på all informasjon de gir, blir behandlet konfidensielt.» (Thagaard, 2018, s. 28). Som en følge av Lundin størrelse som organisasjon, ble dette prinsippet ansett som spesielt viktig. Hele organisasjonen omfatter om lag 370 ansatte, og HMS-avdelingen er derfor begrenset i størrelse. Disse faktorene medfører at informanter lettere kan identifiseres og derfor blir mere sårbare. På bakgrunn av dette har karakteristikk som alder, kjønn, og arbeidstittel blitt utelatt av dette prosjektet. I listebeskrivelsen av informantene har informantenes tittel blitt til dels generalisert for å kunne ivareta deres konfidensialitet. Disse hensynene blir også ivaretatt i kapittel 5, hvor empiri og drøfting presenteres.

5.0 Empiri og drøfting

Dette forskningsprosjektet har som formål å vurdere hvorvidt digitale sikkerhetsinformasjonssystemer i Lundin bidrar til resiliens i tråd med teori og litteratur. Denne vurderingen skal her utføres ved å besvare tre forskningsspørsmål ved bruk av det teoretiske rammeverket presentert i kapittel 3. Som et resultat av forskningsspørsmålenes ulike teoretiske baktepper har det blitt valgt å slå sammen empiri og drøfting til ett kapittel. Hensikten med dette er å gi leseren et tydeligere bilde over hva som drøftes, samtidig som teoretiske bidrag ligger ferskt i minnet til personen som leser. Prosjektets datagrunnlag er også basert på ulike datakilder i form av intervjuer av ansatte og analyser av relevante dokumenter og systemer, som sammen danner det empiriske innholdet i prosjektet. Som følge av mangfoldet i datakilder, empiri og teori anses også dette som et argument for en sammenslåing av empiri-kapittelet og drøftings-kapittelet. For å kunne besvare problemstillingen og forskningsspørsmålene er dette kapittelet delt opp i tre delkapitler som tar for seg de tre forskningsspørsmålene. Formålet med denne delen er altså å drøfte datainnsamlingen opp mot teorigrunnlaget, og dermed forsøke å besvare prosjektets problemstilling. Forskningsspørsmålene har som hensikt å redegjøre for de tre overordnede prosessene som inngår i kunnskapsoverføring, og vil underveis beskrive funksjonene til ulike digitale systemer i disse prosessene. I dette kapittelet vil flere digitale systemer omtales og diskuteres. For å kunne gi leseren en oversikt, anses det som hensiktsmessig å presentere en tabell med oversikt over de digitale systemene som omtales i kapitelet.

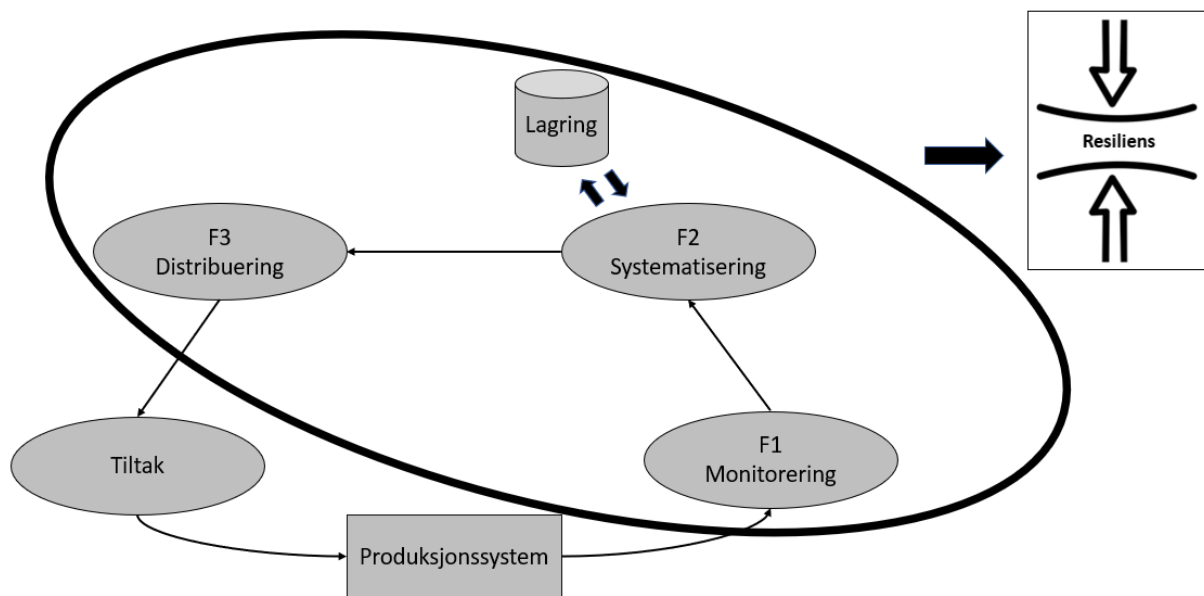
Tabell 4-5 Presentasjon av digitale systemer i Lundin

Systemnavn	Systembeskrivelse
Apos - Arbeidsprosess Orientert Styring.	Lundins offisielle prosessverktøy. Har som formål å sikre at arbeidsprosessene etterlever lover, regler, krav og øvrige standarder. Systemet visualiserer de ulike arbeidsprosessene i flytskjemaer, og gir en oversikt i form av prosesskart.
Synergi Life	Lundins SIS. Digital programvare som benyttes til innrapportering av hendelser og forhold med betydning for sikkerheten, samt dokumentering av saksgang etter rapportering. Programvaren er utviklet for å støtte HMSK prosesser i selskapet.
Barrierepanel	Digital programvare som gir en visuell oversikt over status på sikkerhetsbarrierer med hensyn til storulykkesrisiko ved plattformen Edvard Grieg
SAS – Honeywell Asset Sentinel	Digital programvare som gir en visuell sanntidsstatus på komponenter offshore, som for eksempel gassdetektorer.
Workmate	Digital programvare for organisering av arbeidsordrer offshore. Fungerer i praksis som en direkte kobling mellom dokumenter og fysisk utstyr.

Det første forskningsspørsmålet i dette kapittelet omhandler monitorering og vil besvares ved å forklare hvordan uprosessert data/rådata fanges av Lundins SIS og prosesser for monitorering. Forskningsspørsmål nummer to vil besvares ved å beskrive hvordan innsamlet data systematiseres, kategoriseres og tilgjengeliggjøres av de aktuelle digitale systemene. Det siste forskningsspørsmålet vil besvares ved å redegjøre for hvordan systematisert informasjon distribueres til relevante deler av organisasjonen som en del av selskapets sikkerhetsstyring.

Problemstillingen i dette forskningsprosjektet har som hensikt å besvare hvorvidt sluttproduktet av disse tre delprosessene kan bidra til resiliens i selskapet. Figur 5-6 gir en overordnet visualisering av prosjektets formål

«Hvordan kan digitale sikkerhetsinformasjonssystemer bidra til resiliens i Lundin Norway?»



Figur 5-6 Visualisering av forskningsspørsmål og problemstillingens formål basert på skjematiske fremstilling av SIS (Aven et al, 2004, s. 132).

5.1 F1) Hvordan benyttes digitale sikkerhetsinformasjonssystemer til monitorering av sikkerhet i Lundin Norway?

Alle operatørselskap skal i dag ha systemer for innsamling av data med betydning for HMS-arbeidet i selskapet. Styringsforskriften (2010) inneholder flere paragrafer som direkte henviser til slike systemer, samt hvilke funksjoner disse systemene bør inneholde. Styringsforskriftens §10 og §19 henviser spesielt til operatørens ansvar, både med tilknytning til innsamling av data, og bruk av måleparametere/indikatorer.

§ 10 Måleparametere og indikatorer

Den ansvarlige skal etablere måleparametere for å overvåke forhold som er av betydning for helse, miljø og sikkerhet, deriblant graden av måloppnåelse, jf. § 7 og § 8. Operatøren eller den som står for driften av en innretning eller et landanlegg skal etablere indikatorer for å overvåke endringer og trender i storulykkesrisikoen og miljørisikoen (Styringsforskriften, 2010, § 10).

§ 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. (Styringsforskriften, 2010, § 19).

Selv om styringsforskriften legger føringer for systematisering av data i operatørselskaper, gjenstår det fremdeles et spillerom med hensyn til systemenes struktur, type og utforming. Selv om formålene bak forskriftene er synlig, vil det ikke dermed være gitt at operatørselskapenes etterlevelse av forskriftene oppfyller disse formålene. Det hviler derfor et stort ansvar på operatørselskapene, og deres evne til å utforme og implementere systemer som etterlever forskriftene. Man kan argumentere for at systemene som styringsforskriften henviser til i praksis utgjør ulike former for SIS, da det i stor grad samsvarer med betegnelsen på SIS, selv om denne betegnelsen ikke spesifikt benyttes i styringsforskriften (2010) § 19.

5.1.1 Synergi som monitoreringsverktøy

Synergi Life er en programvare som benyttes til rapportering, håndtering av hendelser og tiltaksimplementering. Programvaren er et digitalt verktøy utviklet for å støtte HMSK prosesser i organisasjoner og er utviklet av DNV GL (2019B). Synergi Life, heretter referert til som Synergi, kan i praksis hevdes å være et sikkerhetsinformasjonssystem (SIS) i tråd med betegnelsen til (Aven et al., 2004, s. 131). Synergi innehar en rekke funksjoner knyttet til innrapportering og saksbehandling av forhold og hendelser. Begrepet hendelse benyttes i systemet som en samlebetegnelse på ulykker, nesten-ulykker, farlige forhold/tilstander og kvalitetsavvik. Systemet brukes derfor i praksis til å dokumentere observasjoner med tapspotensial, med hensyn til HMS, kvalitet, kostnad eller forsinkelser. Synergi er et viktig og sentralt verktøy i etterlevelsen av styringsforskriftene, og er spesielt tilknyttet styringsforskriften (2010) §10, §19-20, og §22 -23.

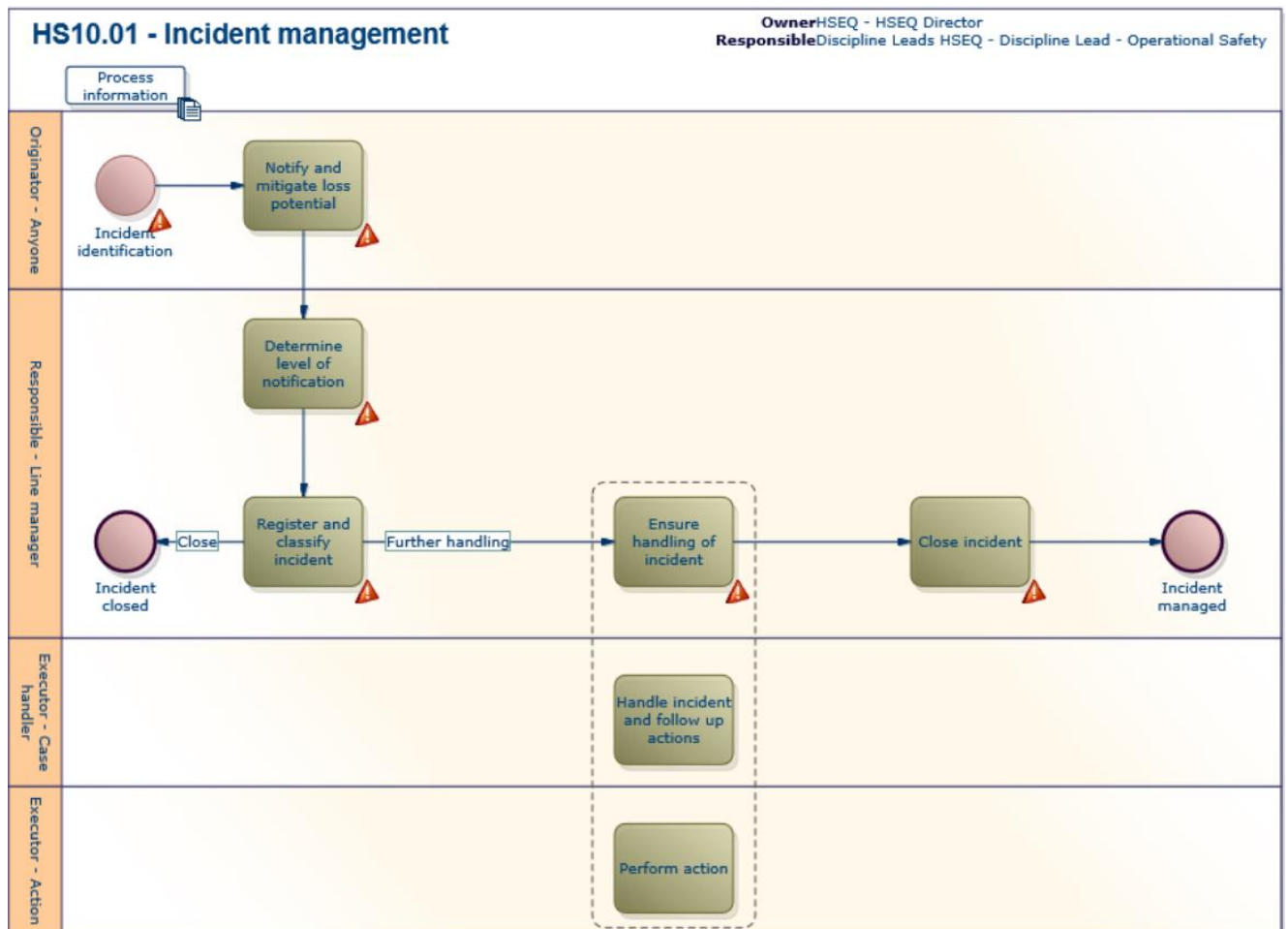


Figur 5-7 Skjermdump av Synergis brukergrensesnitt

Synergi er en etablert programvare både i Lundin og i petroleumsnæringen generelt. I Lundin representerer Synergi selve betegnelsen på et avviksrapporteringssystem og har blitt benyttet siden 2015. «Folk lager ikke avvik lengre, de lager en synergi, det er begrepet man bruker. Man lager ikke en hendelsesrapport, man lager en synergirapport» (Informant nr. 3).

Synergi er et system for hendelsesbasert risikostyring og er på denne måten reaktiv av natur. Synergis brukergrensesnitt og utforming er utarbeidet av DNV GL, på bestilling fra Lundin.

Denne bestillingen og utformingen av programmet har sitt opphav i prosessbeskrivelsen av programvarens funksjon:



Figur 5-8 Prosesskart for hendelseshåndtering i Lundin Norway, hentet fra APOS

Prosesskartet er hentet fra det digitale prosessverktøyet APOS som er en forkortelse for «Arbeidsprosess Orientert Styring». Systemet har som formål å visualisere arbeidsprosessene i Lundin ved hjelp av flytskjemaer som gir en oversikt over roller, kompetansekrav, stillinger og koblinger som er direkte knyttet til ulike prosesser i selskapet. Prosesskartet viser hvordan hele hendelsesforløpet i etterkant av en innrapportert hendelse skal dokumenteres i Synergi, og hvordan selve klassifiseringen av hendelsens alvorlighetsgrad utføres i Synergi. Når en hendelse eller et forhold registreres i Synergi må blant annet konsekvenser og alvorlighetsgrad fylles inn. Den innrapporterte informasjonen vil danne beslutningsgrunnlaget i vurderingen av den videre saksgangen for hendelsen/forholdet, og dersom rapporten overstiger en gitt poengsum som representerer alvorlighetsgrad, vil dette iverksette en granskingsprosess. Hver sak vil også være tilknyttet tiltak/aksjoner som må oppfylles før saken kan avsluttes.

Tiltak og aksjoner tildeles til ansatte som er ansvarlig for områder hvor utbedringer eller annet arbeid må utføres for at saken skal kunne vurderes som avsluttet. Ansatte vil ved innlogging i Synergi få en oversikt over tildelte tiltak/aksjoner og tidsfrister for utførelse.

Aven et al. (2004) trekker frem ansattes holdninger til SIS som et viktig moment. Dette er beskrevet både i kriterier for SIS, «Forståelig og akseptert», og i psykologiske faktorer, under «insentivstruktur og lokal kunnskap». Alle ansatte ved Lundin har tilgang til Synergi; ved plattformene og riggene er det også utplassert PCer med anonym innlogging, samtidig som innrapporteringer også kan gjøres på papir som legges i postkasser. Det ble også nylig introdusert nettbrett på plattformen Edvard Grieg, for å forenkle prosessen ytterligere og samtidig gi ansatte en større oversikt over pågående saker og tiltak. Informant nr. 1, 2, 3 og 5 beskriver Synergi som etablert og akseptert blant de ansatte i Lundin. Dette gjenspeiles også i vokabularet blant informantene som eksempelvis henviser til å «skrive en synergi». Aven et al. (2004) beskriver også hvordan reliabilitet er et viktig kriterium for funksjonen til et SIS. Datagrunnlaget må være så nøyaktig og konsistent som mulig for at det skal kunne være etterprøvbart. Synergi beskrives av informant nr. 1 som en termometer som hovedsakelig er reaktiv. Informant nr. 2 beskriver at det ikke er reliabiliteten i datagrunnlaget som er utfordringen, men heller datamengde og tilgjengelighet.

Det er mye av utfordringen vi har, rett og slett det å filtrere bort det som er irrelevant og strukturering av data. Det er egentlig en gigantisk database med kanskje mye uinteressant informasjon, men spørsmålet er hvordan en skal finne det som faktisk er interessant (Informant nr. 2).

Som informant nr. 1 og 2 beskriver, oppleves uthenting av data som utfordrende. Dette kan medføre til komplikasjoner når historiske data skal benyttes til å hente kunnskap fra tidligere hendelser. Disse utfordringene vil naturlig nok også kunne fremme spørsmål omkring reliabilitet i datagrunnlaget, da etterprøvbareheten av data vanskeliggjøres av mangelen på tilgjengelighet.

Synergi gir muligheten til å se antall innregistrerte hendelser kategorisert etter type hendelse og innenfor ønsket tidsrom. Synergi gir samtidig ingen statistiske trendlinjer som kan knytte innrapporterte forhold og hendelser til andre variabler, slik som antall arbeidstimer. Det er dermed ikke mulig å hente ut rater som blant annet sier noe om skader fordelt på arbeidstimer. Det eksisterer heller ingen automatiske funksjoner i Synergi som varsler om trender eller hendelser over tid. Dersom det eksempelvis skulle oppstå flere mindre hendelser på en borerigg med like karakteristikk, vil det ikke utløses noen automatiske varsler eller alarmer i Synergi.

Det er opp til mennesker å fange trender og utviklinger i innrapporteringer. Frekvenskurver med hensyn til «Key Point Indicators» og rater som fraværsskader regnes ut ved at ansatte manuelt henter ut statistikk fra Synergi og fører dette inn på et regneark. Slike indikatorer er dermed i stor grad utarbeidet manuelt. Dette innebærer at en ansatt har dette som ansvarsområde og utfører utregningene ved hjelp av regneark i Microsoft Excel. Dette kan anses å ha både positive og negative konsekvenser. Ulempen ved denne praksisen kan være at feil i utregninger fører til statistikk som ikke er korrekt, man kan også argumentere for at en automatisert prosess vil kunne være mer effektiv og produsere større mengder statistikk. Den manuelle utregningen kan også anses som en positiv prosess hvor data kvalitetssikres før det presenteres som statistikk. Man kan hevde at en slik vurdering er betinget av datamengde, og derfor må ses i lys av selskapets størrelse.

5.1.2 Indikatorer og KPI

I følgende delkapittel vil Lundins bruk av indikatorer presenteres og drøftes opp mot indikatoregenskapene som Hollnagel (2017) presenterer i sin RAG-modell. Indikatorene som det henvises til i dette delkapittelet vil omhandle overordnede KPI-er, men også andre former for kunnskapshenting som ansatte betegner som indikatorer. KPI er en forkortelse for Key Performance Indicator, og brukes som en betegnelse på indikatorer som er direkte tilknyttet overordnet måloppnåelse i arbeidet på HSEQ-avdelingen ved Lundin. Drøftingen vil kunne belyse hvorvidt indikatorene og KPI-ene har egenskaper som samsvarer med monitoreringsegenskaper fra RAG. I det følgende avsnittet vil også Reiman & Pietikäinens (2012) teoretiske rammeverk for indikatorbruk benyttes til å kategorisere indikatorene etter formål.

5.1.2.1 Indikatorlister og relevans

I spørsmålsettet hentet fra RAG omtaler Hollnagel (2017) bruken av indikatorer og trekker frem betydningen av en liste med relevante ytelsesindikatorer som brukes regelmessig. Det fremheves også som viktig at disse indikatorene revideres og gjennomgås kontinuerlig. Lundin utfører årlig en «management review», som er en selskapsrevisjon hvor hver avdeling vurderer sitt arbeid basert på målsetninger satt året før. Som en del av denne vurderingen vil hver avdeling rette eventuelle ønsker eller mangler mot andre avdelinger, med hensyn til ressurser og arbeidskapasitet. Informant nr. 1 påpeker hvordan denne gjennomgangen har en stor nytteverdi, ettersom den bidrar til å synliggjøre viktige fokusområder i HMS-arbeidet. Den årlige gjennomgangen legger på denne måten mye av grunnlaget for planverk for det kommende året, samtidig som det utarbeides en plan for de ulike avdelingene hos Lundin.

I Lundins «HSEQ Plan 2019» spesifiseres disse målsetningene, viktige fokusområder, og KPI-er for det kommende året. Dokumentet inneholder også en oppsummering av fjorårets data og ytelse med hensyn til HSEQ-arbeidet (LNAS, 2019).

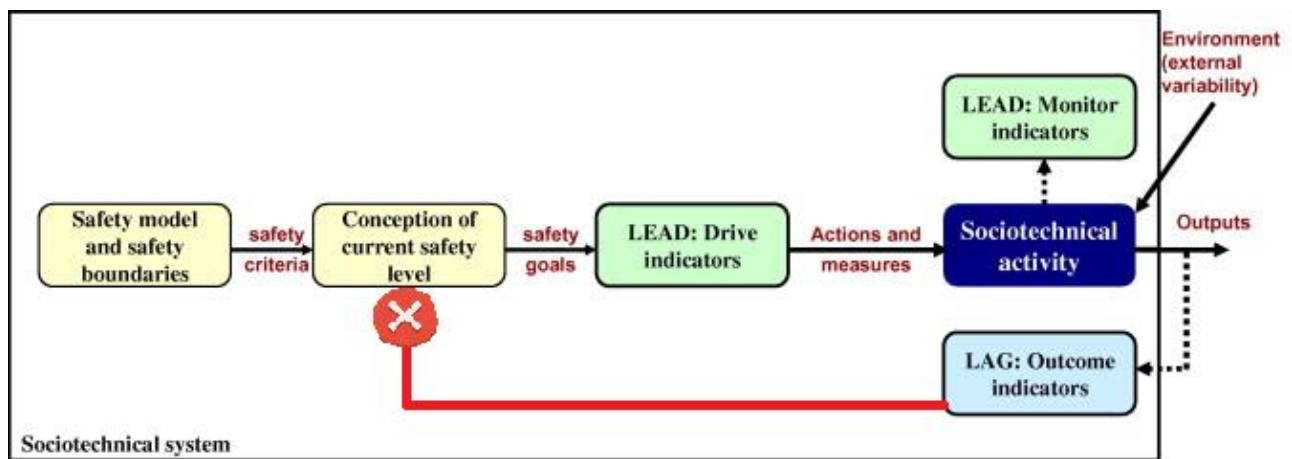
Reiman & Pietikäinen (2012) beskriver indikatorer som verktøy for evaluering og forbedring av systemets funksjon, og kategoriserer indikatorer i tre ulike kategorier etter formål: Drive, monitor, og outcome. Drive-indikatorer omtaler målinger av aktiviteter tilknyttet sikkerhetsstyring. Monitor-indikatorer omtaler indikatorer som måler dynamiske forhold i organisasjonen, slik som holdninger og kultur. Outcome-indikatorer måler konkrete resultater fra systemer, slik som antall uønskede hendelser. Reiman & Pietikäinen (2012) beskriver disse tre indikatorformene som viktige i sikkerhetsstyringen. For å kunne kartlegge fordelingen av de ulike indikatorene i Lundins KPI-liste er det derfor valgt å inkludere disse i vedlegg nr.1. Dette er interessant da det kan gi en pekepinn som sier noe om prioriteringer i Lundins sikkerhetsstyring. Det er også gjort et forsøk på å kategorisere indikatorene som kvalitative/kvantitative, og etterslepene/ledende. Formålet med tabellen i vedlegg nr. 1 er å gi en oversikt over hvilke indikatorer som benyttes som KPI-er og hva som kjennetegner dem. I tabellen i vedlegg nr. 1 er Lundins KPI-er for 2019 kategorisert etter det teoretiske rammeverket til Reiman & Pietikäinen (2012).

Indikatorene i vedlegg nr. 1 beskriver avdelingens kriterier for måloppnåelse og gir en pekepinn på hvilke delområder avdelingen skal sette søkelys på. Det presiseres også i HSEQ-planen at de ulike indikatorene skal håndteres av sine respektive fagområder innad i avdelingen (LNAS, 2019). Indikatorene er i stor grad basert på kvantitativ og målbar data fra registrerte hendelser og forhold, og kan dermed hevdes å være etterslepene eller reaktive indikatorer.

Som illustrert i tabellen i vedlegg nr .1 kan de fleste indikatorene kategoriseres som «Outcome-indikatorer». Kategoriseringen i tabellen viser at hele 10 av de 15 indikatorene kan betraktes som «Outcome-indikatorer». Av de gjenstående indikatorene kan 4 betraktes som «drive-indikatorer», og 1 som «monitor-indikator». Denne kategorisering er veiledende, og det vil kunne argumenteres for at enkelte indikatorer vil kunne tolkes annerledes. Man kan allikevel hevde at kategoriseringen reflekterer hvordan KPI-ene i stor grad er basert på kvantitative «outcome-indikatorer» som igjen speiler hvordan overordnede indikatorer i selskapet belager seg på reaktive målinger, i form av etterslepene indikatorer. Reiman & Pietikäinen (2012) påpeker i sin forskningsartikkel hvordan ledene indikatorer er et nyere tilskudd i sikkerhetslitteraturen, hvor bruk av etterslepene indikatorer har vært den etablerte praksis.

Ledende indikatorer er som nevnt et nyere tilskudd, som også Hollnagel (2017) trekker frem som et verktøy mot resiliens. Det er dermed ikke sagt at bruk av etterslepene indikatorer ikke kan bidra til resiliens, eller at dette er synonymt med noe negativt. Det fordrer imidlertid at de etterslepene «outcome-indiaktorene» er basert på et tilgjengelig datagrunnlag.

Ettersom det kan oppleves som vanskelig å hente ut informasjon i Synergi, kan dette medføre en svekket verdi i indikatorene som beslutningsgrunnlag, herunder illustrert i figur 5-8, med modellen til Reiman & Pietikäinen (2012). Modellen viser feedback fra indikatorer, den røde linjen representerer en mulig svekket informasjonsflyt fra «Outcome indicators», som i praksis er basert på historisk og reaktiv datainnsamling i Synergi.



Figur 5-9 Egendefinert figur basert på "The extended system model showing the feedback from the indicators" (Reiman & Pietikäinen, 2012, s. 1996).

5.1.2.2 Indikatorenes validitet og tidsforsinkelser

I likhet med Hollnagel fremmer også Aven (2004) validitet som et av flere viktige kriterier i et SIS. For at data skal være representativt for organisasjonens tilstand er det viktig at indikatorer og prestasjonsmål er dekkende for det man ønsker å måle. Tidsforsinkelser vil også kunne svekke validiteten til indikatoren, da langsomme prosesser kan medføre at indikatorene ikke lenger er representative for virkeligheten. De overordnede KPI-ene for HSEQ-avdelingen utarbeides årlig, og er til dels basert på etablerte indikatorer i næringen. KPI-ene er utarbeidet av HSEQ og reflekterer på denne måten avdelingens ønsker og målsetninger for det kommende året. Resultater og statuser på KPI-ene skal gjennomgås og revideres kvartalsvis, før de deretter presenteres for ledergruppen. Både informant nr. 1 og 3 presiserer at uønskede hendelser av større omfang vil varsles direkte til ledergruppen og at det på denne måten ikke eksisterer noen tidsforsinkelser av betydning i disse kommunikasjonsprosessene.

Gjennomgangen som utføres kvartalsvis av indikatorstatusene, utføres for å fange opp trender eller utviklinger med betydning for sikkerheten. Uønskede hendelser og forhold vil håndteres fortløpende med risikoreducerende tiltak tilpasset etter hva som anses som den beste løsningen. Disse beslutningene utføres av ansatte med dette som fagområde og utføres i samråd med fagområder tilknyttet hendelsen. Hendelser og forhold registreres i Synergi hvor saken gis en poengsum basert på konsekvenser og alvorlighetsgrad. Den innrapporterte informasjonen vil danne beslutningsgrunnlaget i vurderingen av den videre saksgangen for hendelsen/forholdet. Programvaren vil derfor danne et beslutningsgrunnlag ved hjelp av poengverdier. Selv om beslutninger for hendelseshåndtering utføres av ansatte, kan det hevdes at Synergis struktur påvirker disse beslutningene, da beslutninger fattes på grunnlag av tilgjengelig informasjon i Synergi.

Det arrangeres også et månedlig allmøte hvor antall hendelser og status på KPI-er presenteres. KPI-enes validitet kan diskuteres fra flere perspektiver; man kan diskutere både validiteten til datagrunnlaget bak KPI-ene, og validiteten til selve KPI-ene, samt om hvorvidt den gir et gyldig bilde av sikkerhetstilstanden i organisasjonen. Det er i liten grad synlige årsaker til å betvile validiteten til datagrunnlaget bak KPI-ene, da dette datagrunnlaget er basert på innrapporterte forhold og hendelser i Synergi. Ansatte i Lundin er pliktige til å rapportere inn uønskede hendelser og forhold med betydelig omfang, samtidig som ansatte med relevant tilknytning til det aktuelle området vil varsles direkte. En kan på denne måten hevde at det er mindre sannsynlig at innrapporterte forhold med stor betydning forsvinner i mengden. Betydelige hendelser og forhold vil som regel også innrapporteres fra flere hold. Hvorvidt KPI-ene gir et valid bilde av sikkerhetstilstanden i organisasjonen, er et spørsmål med større usikkerhet. KPI-ene er i stor grad basert på frekvenser og målinger som er etablerte i petroleumsnæringen, på tvers av operatørselskap. En kan argumentere for at validitet avhenger av graden KPI-ene evner å reflektere den reelle sikkerhetstilstanden i organisasjonen. Basert på denne antagelsen vil standardiserte reaktive målinger ha naturlige begrensninger. «Precursor resilience» beskrives som evnen til å monitorere og gripe inn for å raskt korrigere uakseptable tilstander og forhold i en tidlig fase, før det oppstår uakseptabel risiko. En slik form for resiliens vil i stor grad være betinget av indikatorer som tidlig evner å fange opp uønskede forhold og utviklinger. KPI-ene i Lundins HSEQ-plan vil i mindre grad tilrettelegge for en slik praksis, da de i stor grad er standardiserte og reaktive.

Noe som også reflekteres av informant nr. 1: «Vi er ikke så fan av slike rater, da de sier mer om fortiden. Vi prøver å benytte ledende indikatorer. Vi har mest lyst å fjerne selve rate-systemet (KPI), da det ikke sier noe om den reelle sikkerheten» (Informant nr.1).

5.1.2.3 Indikatorer frekvenser og sensitivitet

Disse egenskapene omhandler hvorvidt indikatorene er sensitive nok til å fange forhold av betydning, og hvorvidt indikatorene benyttes ofte nok. KPI-enes sensitivitet vil påvirkes av Lundins relativt lave datamengde sammenlignet med andre operatørselskap og dette vil kunne føre til at enkelthendelser gir større utslag. Hollnagel (2017) trekker også frem spørsmålet om indikatorenes evne til å fange utviklinger og endringer tidlig nok til at de kan korrigeres før de resulterer i uønskede hendelser eller ulykker. KPI-ene er basert på reaktive målinger over tid og det vil derfor kunne diskuteres hvorvidt de evner å fange utviklinger og endringer i et tidlig stadium. Flere informanter påpeker at det finnes flere former for kunnskapsinnhenting som kan betegnes som indikatorbruk. På plattformen Edvard Grieg og på boreriggene er det tilrettelagt for kontinuerlig innsendelse av «Observasjonskort». Observasjonskort er innrapporteringer som kan gjøres både fysisk ved å fylle ut skjemaer som legges i postkasser, eller digitalt på utplasserte PCer. De ansatte oppfordres til å sende inn så mange kort som mulig, og dette er også en bevist strategi. Selv om 60-70 kort per dag innebærer mye irrelevant informasjon, øker dette også sannsynligheten for å fange opp mindre forhold med betydning for sikkerheten. Det gjennomføres daglige morgenmøter i form av videokonferanser hvor gjennomgang av disse observasjonskortene utføres i samråd med operativt ansatte på plattform/borerigg og ansatte onshore. På produksjonsplattformen Edvard Grieg vil driftsavdelingen behandle observasjonskort og legge disse inn i Synergi. På boreriggene er riggeier ansvarlig for håndtering av observasjonskort og systematisering av disse. Selv om Lundin som operatør har påseplikt og er ansvarlig for å påse at riggeier har systemer for innrapportering av HMS-relevante forhold, styres systematiseringen av observasjonskort av riggeier selv. Informant nr. 2 omtaler observasjonskortene som en termometer offshore som også kan fungere som en ledende indikator. Dersom det eksempelvis oppstår mange førstehjelpsskader eller mindre utslipp kan dette være en indikator på forhold som er i ferd med å utvikle seg og som krever en inngripen. Det er allikevel utfordringer knyttet til å monitorere sikkerhet ved å benytte observasjonskort som ledende indikatorer.

Informant nr. 2 understreker hvordan selv ledende indikatorer ofte må utløses av hendelser, og dermed er til dels reaktive eller etterslepene: «Som regel må det være en eller annen hendelse som er målbar, som ikke nødvendigvis er alvorlig, men som gir en indikator på at neste gang kan det gå dårligere» (Informant nr. 2).

Håndteringen og systematiseringen av observasjonskort er et ansvarsområde som tilhører riggeierne, hvor Lundin er ansvarlig for å påse at dette utføres og samtidig innhente kunnskap av betydning. Det kan daglig være mer enn 60 observasjonskort som må håndteres og dette vil derfor kunne være en arena med mye potensial for kunnskapsinnhenting og monitorering. Flere av informantene påpeker imidlertid hvordan majoriteten av kortene omhandler mindre betydelige forhold og trivielle saker som eksempelvis maten om bord. Det fremkommer dermed at det er en utfordring å systematisere denne dataen:

Det skal sies at vi ikke er superflinke til å strukturere denne dataen som kommer inn og bruke det i HMS-arbeidet. En borerigg kan for eksempel få inn 60-70 kort hver dag, og mange av disse er kanskje ikke veldig relevante for HMS-arbeidet, men dersom det for eksempel er 10 som er relevante og omhandler et spesifikt tema, så er vi ikke så flinke til å plukke opp akkurat dette (Informant nr. 2).

På innleide borerigger er det riggeierens egne systemer som skal benyttes for å samle inn og håndtere forhold og hendelser med betydning for sikkerheten. Lundin vil registrere forhold og hendelser med opplevd læreverdi i Lundins eget SIS, Synergi. Saker vil hovedsakelig registreres i Synergi dersom de innebærer oppfølging av riggeier eller en annen innleid tredjepart. Dette gjøres ettersom Synergi som system tillater at man tilegner aksjoner til ansatte som selv må sørge for at de utføres. Trender og mønster i de innregistrerte forholdene må også fanges av HMS-ansvarlige ansatte. «Det er veldig opp til enkeltindividet som faktisk leser kortet hver dag, til å huske at slike hendelser har vi hatt mange av tidligere, og dermed se et mønster.» (Informant nr. 3).

5.1.2.4 Indikatorenes tolkbarhet og organisatorisk støtte

Hollnagel (2017) trekker frem tolkbarhet og organisatorisk støtte som viktige elementer i vurderingen av indikatorer ved hjelp av RAG. Tolkebarhet viser til hvorvidt indikatorene gir mening i seg selv eller om de krever noen form for analyse før de gir mening. Graden av analyse som kreves for å tolke indikatorene vil kunne påvirke indikatorenes nytteverdi som beslutningsgrunnlag. Organisatorisk støtte omhandler ressurstildeling og hensiktsmessig kommunisering av resultater. KPI-ene som benyttes i Lundins HSEQ-plan er etablerte i petroleumsnæringen og gir et sammenligningsgrunnlag med andre operatørselskap.

En problematikk tilknyttet KPI-enes tolkbarhet er datamengde i forhold til andre operatører. Lundin er et lite operatørselskap sammenlignet med de mange aktørene på norsk sokkel. Per april 2019 har Lundin plattformen Edvard Grieg i produksjon, og én aktiv borerigg. Dette utgjør betydelig mindre data sammenlignet med større selskaper som Equinor og ConocoPhillips.

Vår statistikk er mer sårbar ettersom bransjen generelt baserer indikatorer på rater og frekvenser. Dette gir oss lite input sammenlignet med andre selskaper, og gir dermed et dårligere grunnlag for å utføre vurderinger basert på statistikk. En uønsket hendelse vil i større grad slå ut på våre tall, enn hos et større selskap (Informant nr. 1).

Selv om man kan hevde at et mangelfullt datagrunnlag svekker indikatorenes tolkbarhet, vil dette til dels normaliseres ved at uønskede hendelser fordeles på antall arbeidstimer. Problematikken erkjennes også av de ansatte ved HSEQ-avdelingen, noe som også kan sies å være et viktig poeng når indikatorene tolkes internt på avdelingen.

I Lundins HSEQ Plan 2019 presiseres det at progresjon og status på planverket skal gjennomgås og presenteres til ledergruppen LNAS kvartalsvis (LNAS, 2019). Det utføres også en årlig tiltaksverifikasjon hvor man gjennomgår etterlevelse av tiltak fra ca. 5% av sakene fra det forrige året. Disse sakene velges ut på forhånd, før man ser nærmere på hvorvidt tiltak har blitt utført, og om de har hatt ønsket effekt. Informant nr.1 påpeker at graden av tiltaksetterlevelse kan anses som en indikator i seg selv, ettersom den kan si noe om organisasjonens evne til å følge opp uønskede hendelser og forhold. «Tiltaksoppfølging er det beste måten vi kan spore eller verifisere læring. Fravær av lignende hendelser er en målefaktor. Men også på gode resultater på andre indikatorer, slik som ytelsesindikatorer.» (Informant 1). Flere av informantene opplever den årlige management review-gjennomgangen som nyttig da den bidrar til å synliggjøre viktige fokusområder og prioriteringer innad på avdelingen. KPI-ene gjennomgås også for å vurdere det arbeidet som har blitt utført i året som har vært, samtidig som forslag og tilbakemeldinger diskuteres.

5.2 F2) Hvordan benyttes digitale sikkerhetsinformasjonssystemer til systematisering av kunnskap i Lundin Norway?

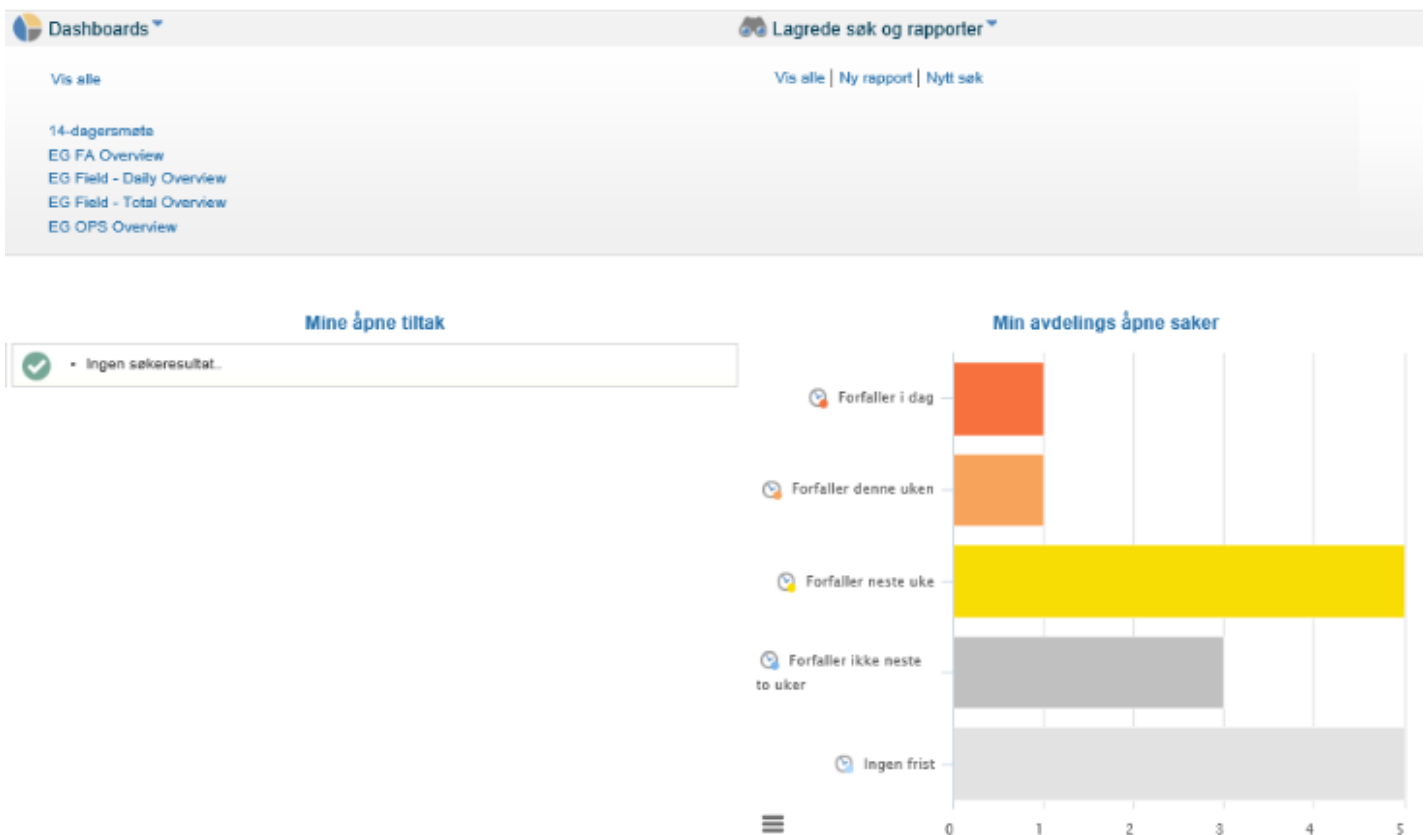
I dette delkapittelet vil det redegjøres for hvordan innsamlet data fra Synergi lagres, kategoriseres og systematiseres i Lundin.

5.2.1 Synergi som verktøy for systematisering av kunnskap

I tråd med teori om SIS benyttes Synergi hovedsakelig til saksbehandling av innrapporterte forhold og hendelser med betydning for sikkerheten i selskapet.

Etter at en sak er opprettet i Synergi vil mulige konsekvenser og alvorlighetsgrad avgjøre hvorvidt rapporten utløser en granskingsprosess internt i Lundin. For at en sak i Synergi skal kunne få status som avsluttet må ansatte signere og lukke tildelte tiltak.

Tildelte tiltak og aksjoner vil være synlig på den enkelte ansattes brukergrensesnitt i Synergi, og det benyttes fargekoder for å signalisere hvilke tiltak som er i ferd med å overstige tidsfrister og som derfor bør prioriteres. Det er også mulig å se forfallende tiltak og aksjoner som er tildelt avdelingen som helhet. Se figur 5-10.



Figur 5-10 Skjermdump av Synergi med eksempel på tiltaksoversikt

For at en sak skal kunne lukkes og bli regnet som avsluttet i Synergi, må tiltakene i saken lukkes og settes som fullført. Når dette er utført blir saken liggende i Synergis database hvor den kan søkes opp i ettertid.

5.2.1.1 Relevans

Aven et al. (2004) beskriver 7 viktige kriterier for et SIS skal fungere i praksis. Flere av disse kriteriene kan anses som relevante i vurderingen av hvordan data systematiseres i Synergi. Kriterie nummer 3 omhandler relevans og informasjonsflyten i et SIS.

Informasjonsflyten må være relevant for beslutningstakere, slik at man unngår en overbelastning med irrelevant informasjon når beslutningsprosesser skal utføres. Synergi fungerer som en database hvor informasjon manuelt må hentes ut ved hjelp av søkefunksjonen i systemet. Ved hendelsesregistrering vil hendelsens alvorlighetsgrad definere saksgangen videre. Dersom rapportens innhold overstiger en gitt poengsum basert på kriterier med hensyn til konsekvenser og alvorlighetsgrad, utløses en intern granskingsprosess. Nøkkelpersoner blir også varslet dersom det oppstår hendelser eller forhold innenfor deres fagområde: «Nøkkelpersoner får umiddelbart tilsendt en epost dersom innrapporteringer innenfor deres område registreres. Disse hendelsene er kriteriedefinert og varsles direkte til teknisk autoritet» (Informant nr. 3).

Nøkkelpersoner i ledergruppen, både i Lundin Norway og i LNAS, mottar automatisk et varsel dersom en alvorlig hendelse har oppstått. Denne beskjednen sendes så raskt som mulig, og har som hensikt å varsle nøkkelpersonell om en pågående hendelse, og samtidig sørge for at nøkkelpersonell ikke lærer om hendelsen fra en tredjepart slik som media. De største utfordringene med hensyn til relevans og informasjonsflyt er utformingen av Synergi som trekkes frem av flere av informantene: Synergi kan i noen tilfeller oppleves som tungvint å bruke. Dette gjelder spesielt i situasjoner hvor ansatte ved ulike avdelinger elektronisk skal signere en sak. Dette må i praksis utføres ved at man åpner saken i Synergi før man videre legger saken inn til en annen avdeling. Denne avdelingen må gjøre det samme etter at de har signert saken for å kunne sende den videre. Det trekkes samtidig frem at dette kan anses som en kvalitetssikring av informasjonen, selv om prosessen oppleves som lite effektiv og logisk av informantene.

En annen utfordring tilknyttet relevans og informasjonsflyt er tilgjengeliggjøring av informasjon. Når en sak opprettes i Synergi foretas det også en vurdering av hvilke brukere som skal ha tilgang til saken. Dette kan oppleves som utfordrende da man ikke kan gi alle tilgang til alle saker, samtidig som man ønsker at nøkkelinformasjon skal nå alle relevante ansatte. Informant nr. 2 oppsummerer utfordringen på følgende måte:

En utfordring er at informasjonen ikke er tilgjengelig for alle, en må ha tilgang for å faktisk kunne gå inn å se. Dette er også en barriere, siden nøkkelinformasjon selvfølgelig burde vært tilgjengelig for alle. Der er lett å sikre at de som har noe å rapportere også har tilgang, men det som 5 personer rapporterer inn kan være relevant for 100 personer. Der har vi en utfordring (Informant nr. 2).

5.2.1.2 Tidsoptimalitet

Som et av flere kriterier for et SIS trekker Aven et al. (2004) og frem tidsoptimalitet. En for langsom informasjonsflyt vil kunne føre til at iverksettelse av tiltak og aksjoner utføres for sent. En konsekvens av dette kan være at risikobildet har endret seg fra den tiden tiltaket opprinnelig ble utarbeidet, og dette kan svekke eller fjerne effekten av tiltaket. Registrering av alvorlige hendelser i Synergi vil som beskrevet føre til automatiske varslinger til tekniske nøkkelpersoner. De største utfordringene tilknyttet tidsoptimalitet beskrives av informant nr. 4 som lukking av tiltak i Synergi og kunnskapsoverføring tilknyttet hendelser som nylig har funnet sted.

Det viktigste med tidsaspektet i denne sammenheng er at potensialet for kunnskapsoverføring er størst rett etter en hendelse har funnet sted. Da er informasjonen fersk og hendelsen fersk i minnet. Går det for lang tid etter en hendelse vil potensialet for læring reduseres. I bransjen har mye utfordringer vært tilknyttet lukking av tiltak eller tiltak som blir stående lenge. Og at det står at alt er fullført når det i realiteten ikke er det (Informant nr. 4).

Disse utfordringene kan sies å samsvare med problematikken fra kriteriet relevans, ettersom tiltak som enten ikke er utført, eller lukket uten å være fullført, vil kunne føre til en opplevd sikkerhetstilstand som ikke samsvarer med virkeligheten: «En person kan oppleve at anbefalingen fra en gransking er meningsløs og derfor gjøre noe helt annet samtidig som han lukker tiltaket. På denne måten kan det oppstå misforståelser i lukke-prosessen, ettersom den ansvarlige ikke har forstått problemstillingen» (Informant nr. 3).

Det kan argumenteres for at denne utfordringen er et resultat av den psykologiske faktoren filter som Aven et al. (2004) presenterer som en sentral faktor i den praktiske bruken av et SIS. Filter som viser til mekanismene som påvirker hvordan informasjon får passere gjennom ulike nivåer vil kunne påvirke informasjonens innhold, samt selve tolkningen av den. Når ansatte videreformidler informasjon vil informasjonen kunne påvirkes av personen som videreformidler og hvorvidt budskapet i informasjonen samsvarer med personens oppfatning av situasjonen. Tidsoptimalitet vil diskuteres videre i relasjon til andre systemer som Lundin benytter for å overføre kunnskap senere i dette kapitlet.

5.2.1.3 Kosteffektivitet

Styringsforskriften (2010) §22 presiserer blant annet at: «Den ansvarlige skal registrere og følge opp avvik fra krav i helse-, miljø- og sikkerhetslovgivningen, deriblant avvik fra interne krav som er av betydning for å oppfylle krav i helse-, miljø- og sikkerhetslovgivningen.» Som operatørselskap er Lundin derfor pålagt å ha systemer for registrering av avvik med hensyn til HMS, altså et SIS. Synergi ble utviklet på 1990-tallet og er i dag godt etablert i Lundin. Ansatte bruker begreper som «Å lage en synergi» når de beskriver rapportering av avvik. En kan på denne måten argumentere for at programvaren i dag inngår som en del av selskapets kultur, og oppleves som akseptert blant mange. På spørsmål om kosteffektiviteten til Synergi som SIS understreker både informant nr. 1 og 3 at Synergi er godt etablert og bidragsgivende, men på ingen måte er fredet i selskapet. «Synergi er ikke noe «state of the art» system. Synergi visualiserer prosesser, men kan i flere tilfeller være tungvint å bruke. Dette gjelder spesielt i situasjoner hvor ansatte ved flere avdelinger skal elektronisk signere samme sak» (Informant nr. 3). Informant nr.1 påpeker også at det finnes alternative løsninger: «Det er jo veldig mange verktøy som kan gjøre det samme, men det har blitt en slags standard. Men vi vurderer kontinuerlig andre leverandører som tilbyr lignende løsninger» (Informant nr. 1).

5.2.2 Granskinger og Synergi

I Lundin utløses interne granskinger av innrapporterte hendelser med alvorlighetsgrad, og konsekvenser som resulterer i en samlet poengsum som overstiger en forhåndsdefinert verdigrænse basert på selskapets risikomatrix. Denne prosessen skjer automatisk i Synergi samtidig som det er mulig å anbefale en gransking underveis i registreringsprosessen.

Klassifisering av hendelse

Linker til guidelines
 Hvordan klassifisere hendelser

	Faktisk alvorlighetsgrad	Potensiell konsekvens	Uavhengige barrierer	
Personskade	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Hydrokarbonlekkasje	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Utsiktede utslipp	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Nedetid	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Materiell skade	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Kostnader	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Annen ytre miljøskade	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Brannbarrierer	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Beregn				Høyeste poengsum <input type="text"/>

Anbefalt videre oppfølging av hendelse

- 1 - Granskning med mandat (>600)
- 2 - Rotårsaksanalyse / Granskning utføres av kontraktør (100-600)
- 3 - Ordinær håndtering i Synergi (<100)

Annen oppfølging bestemt Ja Nei

Kommentar til klassifisering eller oppfølging

Figur 5-11 Skjermdump av Synergi og registrerings skjema for hendelse

Interne granskinger utløses altså av en poengsum og hvorvidt denne overstiger en gitt grense. Avhengig av sakens totale poengsum vil det enten utnevnes en intern granskingsgruppe med mandat for å granske hendelsen, eller så vil man utføre en mindre granskning ved bruk av «5 x Why/Rotårsaksanalyse». Hvorvidt en hendelse skal granskes er en kvalitativ beslutning som utføres av utnevnte ansatte ved HSEQ-avdelingen. I en revisjonsrapport utarbeidet internt i selskapet understrekes det at det også at det foretas granskinger av hendelser hvor poengsummen ikke skulle tilsi at en granskning var nødvendig. Gjentakende hendelser, mindre hendelser eller andre forhold som oppleves som granskingsverdig vil også utløse mindre eller større granskinger basert på kvalitative vurderinger (Lundin Norway, 2018, s. 8).

§ 20 Registrering, undersøkelse og granskning av fare- og ulykkessituasjoner

Den ansvarlige skal sikre at inntrufne fare- og ulykkessituasjoner som kan medføre eller har medført akutt forurensning eller annen skade, blir registrert og undersøkt for å hindre gjentakelse. Situasjoner som opptrer hyppig eller som har stor faktisk eller potensiell konsekvens, skal granskes. Det skal settes kriterier for hvilke situasjoner som skal registreres, undersøkes og granskes, samt settes krav til omfang og organisering. Operatøren skal ha en samlet oversikt over inntrufne fare- og ulykkessituasjoner (Styringsforskriften, 2010, § 20).

Som styringsforskriften (2010) presiserer skal det settes kriterier for hvilke hendelser som skal granskes, og det skal foreligge en oversikt over hendelser i selskapet. I november 2018 satte selskapet ned en kommisjon for å revidere alle interne granskinger i selskapet fra 2015 til og med 2017. Formålet med revisjonen var å vurdere hvorvidt interne granskinger i Lundin har blitt utført på en hensiktsmessig måte og til hvilken grad læring har blitt ivaretatt i etterkant av granskingene. Rapporten konkluderte med at de interne granskingene i selskapet på generell basis utføres på en god måte og at læringsverdien blir ivaretatt. Rapporten fremmet flere anbefalinger med hensyn til videre forbedring av granskingsprosessene. Kommunikasjon av funn var en av anbefalingene som ble fremmet i rapporten og viser til hvordan kommuniseringen av kunnskap fra granskinger ofte er begrenset til toppledelsen og ikke til selskapet som helhet. En annen anbefaling trekker frem tiltaksoppfølging som problematisk, og beskriver hvordan anbefalinger fra granskinger ofte resulterer i anbefalinger som er vanskelig å spore. Det er ønskelig at tiltak som kommer fra granskinger legges inn i Synergi slik at en lettere kan følge opp hvorvidt tiltakene er oppfylt eller ikke. Ofte vil granskinger resultere i generelle anbefalinger uten at dette legges inn som aksjoner/eller tiltak i Synergi (Lundin Norway, 2018, s. 15-16).

Selv om revisjonsrapporten er et internt utarbeidet dokument, med de mulige svakhetene dette måtte innebære, gir det fremdeles en pekepinn på noen av utfordringene som er tilknyttet kunnskapsoverføring fra granskinger. Både revisjonsrapporten og informant nr. 1 - 4 deler en oppfatning om at utfordringene ikke ligger i selve granskingsprosessene, men heller er tilknyttet kunnskapsoverføringen fra selve granskingene: «Dette er blant de største utfordringene i bransjen; Man skriver en rapport, også dabber det av etterpå. Og læring bortfaller. Dette er en kulturgreie» (Informant nr. 1). Informant nr. 1 forklarer videre at det i dag eksisterer en distanse mellom granskingsgruppen og det området som granskes. Det kan argumenteres for at denne distansen bidrar til en fremmedgjøring for personell som befinner seg i den enden som granskes. Dersom ansatte uten direkte innsikt i granskingsprosessene ikke forstår antakelsene og forutsetningene til granskingsgruppens beslutninger, vil dette kunne føre til en manglende forståelse for anbefalinger og resultater fra granskingsprosessene. Dette vil kunne by på utfordringer når tiltak og endringer skal implementeres. Dette er en problematikk som ofte kan oppstå i digitaliseringsprosesser, men som også kan være synlig i andre prosesser (IRIS, 2018, s. 14-15). Informant nr. 1 forklarer at det fremover er ønskelig å involvere ansatte fra området som granskes inn i selve granskingsgruppen, for å redusere distansen mellom disse partene.

Vi ønsker å involvere ansatte fra områder som granskes inn i granskingsgruppen, sånn at de kan bli med å forme aksjoner og stifte eierskap til granskningen. På denne måten kan man i større grad redusere distansen mellom granskingsgruppen og de som granskes/område som granskes. Ofte står det at anbefalinger og tiltak skal i mandat, dette vurderer vi å fjerne, for å involvere de som granskes tidligere. Dette er noe vi har sett at større selskaper har hatt suksess med (Informant nr. 1).

5.2.3 Digitalisering og visualisering av data

Petroleumsnæringen befinner seg i en periode med høyt fokus på effektivitet og kostnader, samtidig som ny teknologi introduseres. Denne perioden kan betegnes som en brytningstid hvor fokuset på utvikling av teknologi er høyt, samtidig som eldre systemer og arbeidsprosesser fortsatt råder (IRIS, 2018, s. 9). Digitalisering beskrives av Unruh og Kiron (2017) som måten forretningsmodeller og prosesser endres for å utnytte digitizing, som videre er definert som prosessen hvor noe analogt konverteres til noe digitalt. I Lundin er også digitizing-prosessen synlig. IHSEQ-plan for 2019 presenteres en rekke hovedaktiviteter for det kommende året (key activities). Informant nr. 1 trekker spesielt frem et av punktene fra listen over aktiviteter:

“14.) Develop a common (LNAS-wide) display/visualization of HSE parameters/results for mandatory use by all LNAS departments.” (LNAS, 2019).

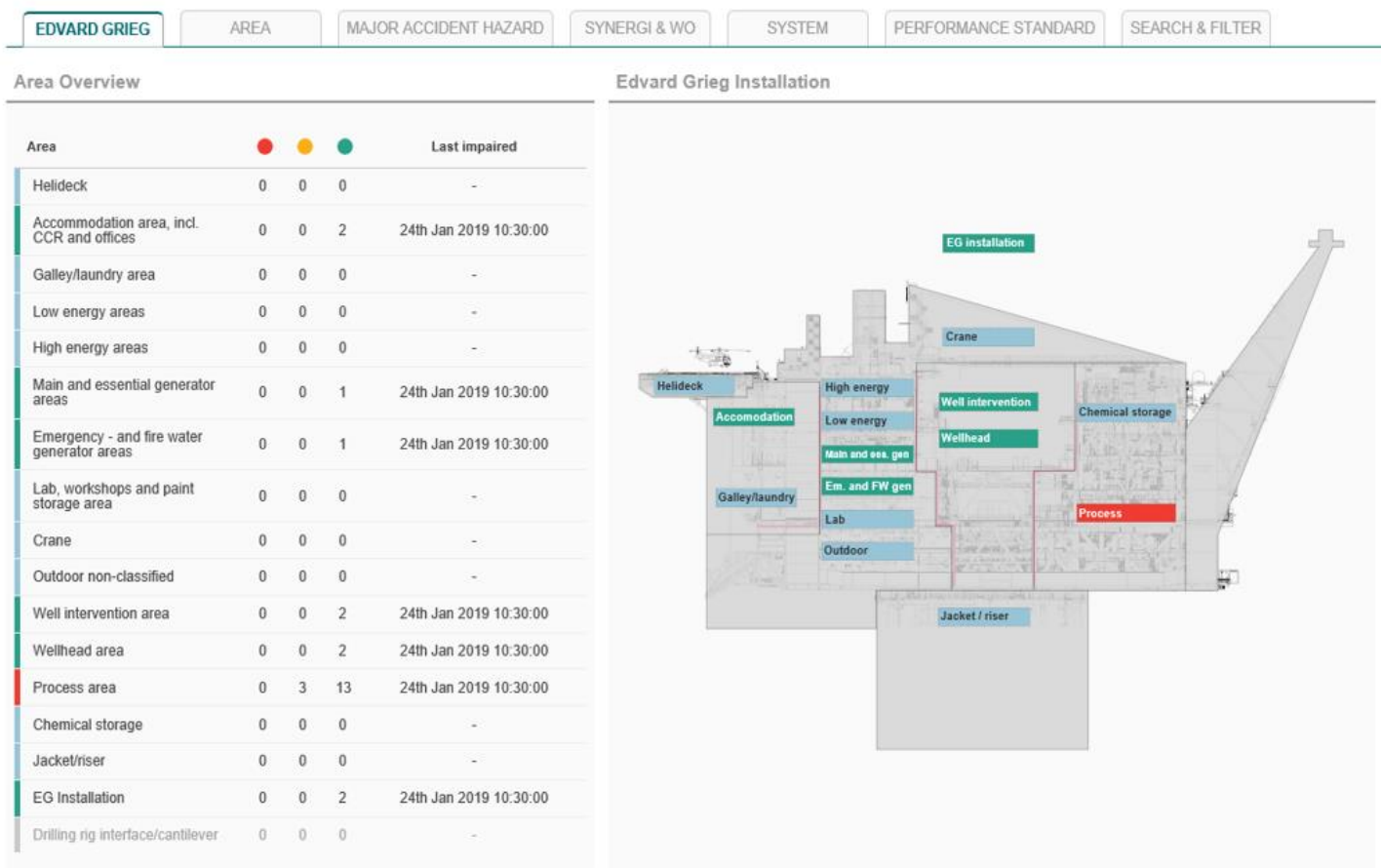
Informant nr. 1 beskriver hvordan det planlegges å sette opp skjermer på avdelingen med statistikk hentet fra Synergi. Denne statistikken vil blant annet basere seg på KPI-tall. Man kan argumentere for at skjermer med avviksfrekvenser og KPI-er må utvikles med varsomhet, da det kan oppstå en differanse mellom de underliggende antagelsene bak informasjonen som visualiseres og hvordan dette tolkes av ansatte.

IRIS (2018) trekker frem hvordan det kan oppstå en fremmedgjøring ved at systemforståelsen til brukerne av systemet svekkes som en direkte konsekvens av digitaliseringen, og med dette kan man få en redusert oversikt over det reelle risikobildet. Dette argumentet får en særlig tyngde når man inkluderer betraktningen til informant nr. 1: «Vi er ikke så fan av slike rater, da de sier mer om fortiden. Vi prøver å benytte ledende indikatorer. Vi har mest lyst å fjerne selve rate-systemet, da det ikke sier noe om den reelle sikkerheten» (Informant nr.1).

5.2.4 Barrierepanelet

Lundin er for tiden i en innkjøringsfase av et nytt digitalt system med navn barrierepanel. Barrierepanelet har som formål å gi en oversikt over status på barrierer med hensyn til storulykker.

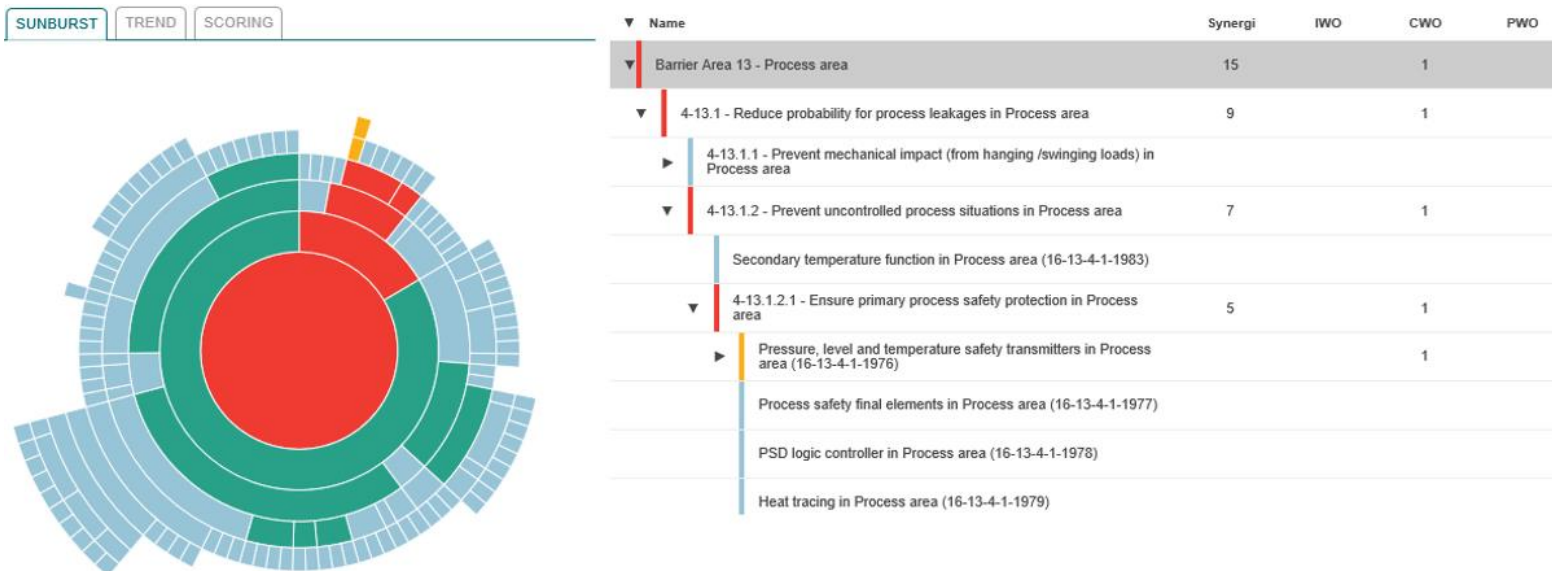
I Styringsforskriften (2010) § 2. Barrierer heter det at: «Det skal være kjent hvilke barrierer som er ute av funksjon eller er svekket. Den ansvarlige skal sette i verk nødvendige tiltak for å rette opp eller kompensere for manglende eller svekkede barrierer». Barrierepanelet er et direkte tilsvarende til denne paragrafen og har som formål å gi en oversikt over barrierestatus på plattformen Edvard Grieg. Denne oversikten skal etter planen støtte drift og ledere både onshore og offshore i planlegging av arbeid og prosjekter. Barrierepanelet har et grensesnitt som gir en visuell oversikt over plattformens sikkerhetsbarrierer og benytter seg av fargekodene rød, gul og grønn. Fargekodene representerer status for de ulike områdene på plattformen, slik som prosessanlegg, lagringsområder, hotell osv. Barrierepanelet gir en oversikt over barrierer og er utarbeidet med hensyn til storulykkesrisiko. Hensikten med systemet er å kunne gi et bilde av statusen på sikkerhetskritiske barrierer på plattformen. Et helhetlig bilde av barrierestatuser på plattformen gir et visuelt oversiktlig bilde av hele plattformen som andre systemer ikke tilbyr. Dette bildet kan gi direkte informasjon til prosjekter i forbindelse med arbeidsplanlegging, ledelsen i Lundin Norway, og øvrig arbeid knyttet til plattformen.



Figur5- 12 Skjermdump av hovedside på barrierepanel

Grensesnittet til systemet er bygd opp av syv faner, hvor første fane gir et oversiktsbilde over plattformen og de ulike områdene med tilhørende status i form av fargekode. Under første fane

visualiseres 16 delområder av plattformen med tilhørende status. Informant nr. 6 beskriver utviklingen av delområdene på følgende måte: «Tidligere var hele plattformen avgrenset til tre delområder, Petroleumstilsynet ga da uttrykk for et ønske om å dele opp plattformen i flere delområder. Dagens oppdeling med 16 delområder gir en mer nøyaktig lokasjon for en endret barrierestatus en tidligere.» (Informant nr. 6). Ved å klikke på de ulike områdene vil en også kunne se en historisk oversikt over statusen til de ulike områdene. Barrierepanelet tillater også at man ser på enkelte barrierer, eller områder av plattformen. Ved å klikke seg inn på et område av plattformen vil man ved hjelp av et «Burst-diagram» få en oversikt over hvilke barrierer som er ute av drift med en visuell forklaring helt ned på komponentnivå, se figur 5-13:



Figur 5-13 Skjermdump av barrierepanelets områdeoversikt

5.2.4.1 Farge og symbolbruk

Informant nr. 6 og 7 erkjenner at fargebruk og betydning av de ulike fargene er en pågående diskusjon på avdelingen. Status på barrierer og områder er i dag kategorisert i fargene blå, grønn, gul og rød. Dersom et område eller en barriere er farget blå, betyr det at det ikke er registrert informasjon om området eller barrieren. Fargen indikerer dermed at området ikke krever direkte oppmerksomhet. Grønn farge indikerer at barrieren er svekket eller ute av funksjon i mer en 72 timer, og dette må håndteres innen 7 dager. Dersom denne tidsfristen overstiges, endres fargen til gul, før den etter 14 dager endres til rød.

En diskusjon i forbindelse med utarbeidelsen av barrierepanelet har vært blant annet bruk av farger, hvor fargen rød i barrierepanelet ikke nødvendigvis har en like akutt betydning som i for eksempel øvrige risikomatriser som brukes i selskapet.

5.2.4.2 Datagrunnlag

Barrierepanelet og status på barrierer baserer seg på data innhentet fra Synergi og Workmate. Workmate er et digitalt system for organisering av arbeidsordrer og utførelse. Workmate fungerer i praksis som en direkte kobling mellom dokumenter og fysisk utstyr. Dersom en arbeidsordre ikke er utført innen en gitt tidsfrist, vil dette utløse krav om risikoanalyser og godkjenning av nedetid på delsystemet. Barrierestatuser vil endre status dersom relevante arbeidsordrer ikke er utført innen sine tidsfrister, eller dersom innrapporterte forhold tilsier en endret status på den aktuelle barrieren. Arbeidsordrer tilknyttes komponenter og utstyr ved bruk av et tag-system. En tag er en unik kode eller nummer for en komponent, og kan sammenlignes med et serienummer. I utarbeidelsen av arbeidsordrer benyttes tags for å beskrive hvilke utstyr eller komponenter som blir berørt av arbeidsorden. Barrierepanelet er som tidligere nevnt oppdelt etter områder og tilhørende sikkerhetsbarrierer, og den videre oppdelingen er kategorisert etter tags som viser til statusen på enkeltkomponenter og utstyr. Innrapporterte forhold er kvalitetssikret i form av gjennomgang og signatur fra nærmeste leder. Samtidig som dette vil kunne medføre noe tidsforsinkelse, og påvirke systemets evne til å gi et sanntidsbilde, er dette også en bevisst avgjørelse. Det er ønskelig å prioritere datagrunnlagets validitet fremfor å prioritere en raskest mulig oppdatering av statusene i systemet.

Det har vært diskusjon rundt dette temaet, men det har vært et bevist valg å legge inn en buffer og en kvalitetssikring av informasjonen. Og på den måten bruke systemet som en oversikt over pågående arbeid og nedetid på delsystemer, og den påfølgende innvirkningen på barrierer mot storulykker. Og ikke som et system for direktestatus (Informant nr. 7).

På denne måten vil man også unngå en direkte overvåking av plattformen, med de konsekvensene dette kan ha på ansatte offshore: «Ting som går galt der ute, må de få lov å fikse uten at 400 folk ser dem over skuldrene. Vi skulle gjerne hatt et direkte system for status også» (Informant nr. 7).

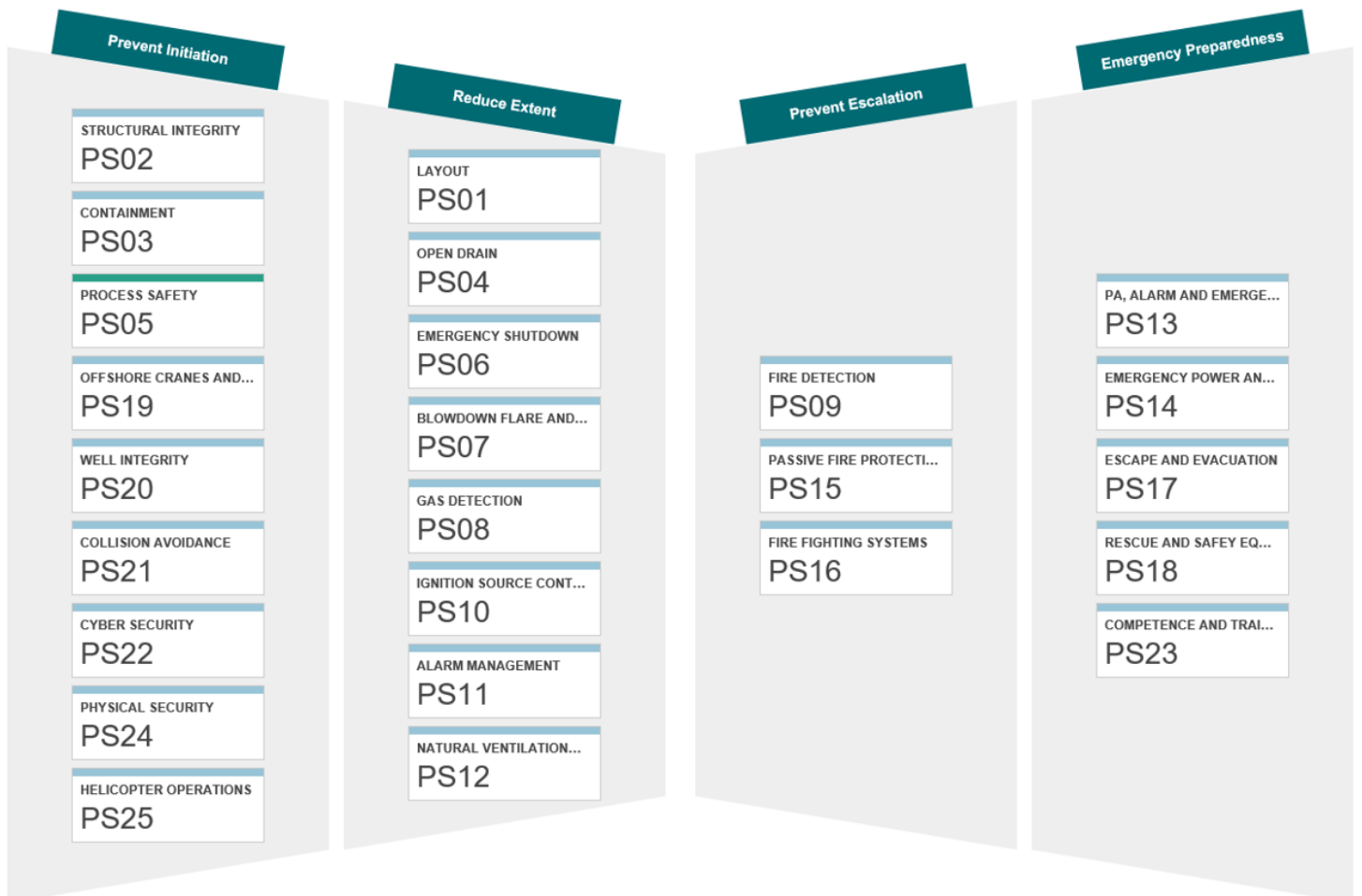
Barrierepanelet har også en mer direkte tilknytning til risikostyring enn andre oversiktssystemer. Honeywell Asset Sentinel, forkortet til SAS, er et digitalt system som viser status til komponenter.

Informant nr. 6 og 7 påpeker at dette systemet ikke gir en direkte oversikt over risiko, men at det planlegges å integrere dette systemet under en egen fane på barrierepanelet. I denne prosessen er det viktig å visualisere dette på en måte som tydeliggjør at komponenters status ikke har samme risikobetydning som barrierestatuser: «Dersom man deaktiverer gassdetektorer og lignende arbeid, trenger ikke dette å være direkte knyttet til økt risiko» (Informant nr. 7). I motsetning til den reaktive naturen i Lundins KPI-er, representerer barrierepanelet den mer proaktive delen av sikkerhetsarbeidet ifølge informant nr. 2:

Synergi er noe vi bruker for å måle temperaturen, men det er jo mer reaktivt. Vi har ingen leading indicators som vi legger inn i Synergi. Systemet er jo hendelsesbasert risikostyring. Du kan si at vi har synergi i det ene enden og barrierepanelet i den andre enden. På barrierepanelet er vi mer proaktive og prøver å se hvordan vi kan hindre hendelser i å oppstå (Informant nr. 2).

Barrierepanelet har en egen fane hvor barrierene er plassert i en «bow tie-modell» for å kunne visualisere konsekvensene av bortfallet til én eller flere barrierer. Et interessant aspekt ved «Bow-tie modellen» er at den uønskede hendelsen er plassert på venstre side i modellen, noe som innebærer et større antall konsekvensreducerende barrierer på høyre siden i modellen, sammenlignet med antallet risikoreducerende barrierene på venstre siden av modellen. Se figur 5-14.

Informant nr. 6 trekker frem at denne løsningen er utarbeidet i samråd med Petroleumstilsynet, og ble ansett som mest hensiktsmessig



Figur 5-14 Skjermdump av Bow-Tie i barrierepanelet

Barrierepanelet har også en egen fane hvor sikkerhetsbarrierene er kategorisert etter hendelser med storulykkepotensial. Det er to kategoriseringer av arbeidsordrer i WorkMate som benyttes som et direkte datagrunnlag i barrierepanelet. PWO er en forkortelse for Preventive Work Orders, og innebærer planlagte arbeidsordrer slik som rutinemessig vedlikeholdsarbeid på komponenter og utstyr på plattformen.

CWO er en forkortelse for Corrective Work Orders og er arbeidsordrer som er utløst av behov for arbeid utover rutinemessig vedlikeholdsarbeid. Slike korrektive arbeidsordrer kan eksempelvis være feil på systemer, komponenter eller utstyr som krever at en iverksetter tiltak for å utbedre det aktuelle området.



Figur 5-15 Skjermdump av kategoriseringer etter storulykker i barrierepanelet

Under fanen som kategoriserer barrierene med hensyn til storulykker er panelet visualisert etter ulike bokser som representerer ulike typer ulykker. Kategoriene er visualisert ved hjelp av bokser og symboler, og inneholder egne felt hvor antall synergisaker, utløpte PWO og utløpte CWO er visualisert.

5.2.4.3 Kan barrierepanelet benyttes til monitorering?

Hollnagel (2017) vektlegger at det er sentralt å spørre seg om hva som monitoreres og hvorfor. Dette stiller igjen grunnleggende spørsmål om prioriteringer, ressurstildelinger og hvilke data en ønsker å innhente. Indikatorer som monitoreres kan kategoriseres som ledende indikatorer og etterslepene indikatorer (Hollnagel, 2017, s. 18). Hos Lundin betegnes barrierepanelet som et monitoreringsverktøy med ledende indikatorer, ettersom barrierepanelet gir muligheten til å ta høyde for konsekvensene av nedetid på barrierer før de resulterer i en økt risikotilstand. Det er også her interessant å trekke frem Informant nr. 6 som understreker hvordan barrierepanelet representerer den proaktive delen av sikkerhetsstyringen i Lundin: «Du kan si at vi har synergi i det ene enden og barrierepanelet i den andre enden. På barrierepanelet er vi mer proaktive og prøver å se hvordan vi kan hindre hendelser i å oppstå» (Informant nr. 6).

Både informant nr. 6 og 7 poengterer at barrierepanelet ikke gir et sanntidsbilde og at det derfor ikke skal benyttes som første kilde til informasjon. Sentrale beslutningstakere skal dermed være kjent med barrierebortfall før dette blir synlig på barrierepanelet: «Betydelige forsinkelser i systemet gjør at systemet ikke gir et sanntidsbilde uansett. Dette er et innforstått faktum med systemet» (Informant nr. 7). Som følge av at barrierebortfall må overstige 72 timer før det synliggjøres på barrierepanelet, eksisterer det betydelige forsinkelser som medfører en begrensning i systemets monitoreringsevne. Dette er også et etablert faktum blant ansatte, og barrierepanelet skal derfor ikke være første kilde til barrierestatus, men heller fungere som en oversikt over nedetid på barrierer. Denne informasjonen vil også kunne bidra til å visualisere sårbarheter som oppstår av nedetiden til ulike barrierer i kombinasjon med hverandre.

Barrierepanelet er visualisert ved hjelp av farger og symbolbruk på tv-skjermer plassert strategisk på avdelingen. Barrierepanelet er dermed synlig for alle på avdelingen til alle tidspunkt. Selv om det av flere informanter understrekes at barrierepanelet ikke skal være en første kilde til informasjon, vil man også kunne argumentere for at visualiseringen kan misforstås og skape en falsk trygghet. Digitalisering kan som kjent ha positive effekter på effektiviseringer av prosesser i HMS-arbeidet, og det vil samtidig kunne oppstå en fare for at ansattes systemforståelse svekkes som en konsekvens. Dersom de underliggende antagelsene og forutsetningene som ligger bak systemene blir mindre synlig, risikerer en at beslutningstakere får en begrenset systemforståelse, og en redusert oversikt over det reelle sårbarhetsbildet og en fremmedgjøring (IRIS, 2018, s. 14-15). På bakgrunn av dette kan man argumentere for at barrierepanelets funksjon er avhengig av brukernes kunnskap og at det derfor må tildeles ressurser på å ivareta ansattes systemforståelse. Lundin er et relativt lite operatørselskap med korte beslutningsveier og relativt få ansatte. Man kan argumentere for at dette faktumet spiller til fordel i prosesser hvor man introduserer nye systemer, ettersom færre ansatte medfører færre muligheter for misforståelse og færre personer som skal opplæres. Aven et al. (2004) beskriver informasjonsfilter som en psykologisk faktor som påvirker informasjonsflyt. Disse filtrene beskrives som avgjørende for hvordan enkeltpersoner tolker og videreformidler informasjon, og hvordan selve informasjonen påvirkes av dette. I lys av slike faktorer vil man kunne hevde at Lundins størrelse er en fordel, som en følge av at informasjon passerer færre ledd. Samtidig er det viktig å være bevisst på fallgruver som fremmedgjøring, og hvordan slike fenomener kan ha store konsekvenser dersom de får utvikle seg over tid.

Carr (2014) trekker frem hvordan fenomenet «Automation bias» som følge av digitaliseringsprosesser tidligere har vært avgjørende i flyulykker. Ved Automation bias oppstår en form for kunstig tillit til resultatene som systemene produserer, hvor brukerne oppfatter data som korrekt ettersom det er produsert av en maskin. Carr understreker også hvordan gevinsten i form av effektivisering fra automatisering og digitalisering til dels må betales av tap av menneskelig intuisjon i systemene (IRIS, 2018, s. 42). Ettersom det eksisterer betydelige forsinkelser i barrierepanelets datagrunnlag, gir panelet heller ikke et sanntidsbilde. For at en barriere skal få fargen rød, kreves det at nedetiden overstiger 14 dager. I denne perioden vil ansatte som ser på barrierepanelet kunne miste opplevelsen av at den aktuelle barrieren faktisk er ute av drift, og det vil kunne oppstå en falsk trygghet. Det er derfor sentralt med en ivaretagelse av kompetansen til ansatte som benytter barrierepanelet som informasjonsgrunnlag. Til syvende og sist vil en skjerm med farger og symboler påvirke opplevd risiko, selv om man er kjent med strukturen til datagrunnlaget bak systemet.

5.3 F3) Hvordan distribueres kunnskap fra digitale sikkerhetsinformasjonssystemer i Lundin Norway?

Dette forskningsspørsmålet har som formål å besvare hvordan kunnskap fra det digitale SIS-et Synergi distribueres til relevante deler av organisasjonen. I denne forskningsspørsmålet vil det i liten grad fokuseres på møtevirksomhet eller andre fora hvor kunnskap deles gjennom sosiale interaksjoner. Dette er også viktige arenaer for deling av kunnskap, men anses her som mindre relevant da studien omhandler standardiserte digitale systemer og hvordan de tilrettelegger for kunnskapsoverføring.

5.3.1 Lessons Learned

I Lundin er Lessons Learned, heretter forkortet til LL, den etablerte digitale distribusjonsformen for kunnskapsoverføring i forbindelse med HMS-arbeid. Lessons Learned, eller «onepager» er betegnelsen på dokumenter som beskriver hvilken kunnskap som burde videreføres i etterkant av hendelser, revisjoner, eller andre situasjoner. Informant nr. 3 beskriver LL/Onepagere som etablert i næringen, og som en populær distribusjonsform som følge av at dokumentet er kort og fungerer som et sammendrag av viktig kunnskap en ønsker å videreføre:

En LL skal være en veldig kondensert versjon av hva som har skjedd og hva som bør læres fra det. Og det er egentlig essensen i det. Vi forsøker å legge ved noen bilder også, sånn at det er lett å forstå hva som har skjedd. Dokumentet skal være veldig oppsummerende sånn at det kan sendes ut uten ytterligere tilleggsinformasjon. Det skal være såpass lettforståelig (Informant nr. 2).



LL-dokumenter benyttes i Lundin på hovedsakelig tre fagområder: Prosjekter, eksterne tilrådinger fra Petroleumstilsynet, og i HMS-sammenheng.

Kunnskapsoverføring i form av LL-dokumenter har en noe annen struktur innenfor prosjekter, og brukes der til videreføring av kunnskap som ikke nødvendigvis omhandler sikkerhet, men informasjon fra vellykkede referansebrønner o.l. i forbindelse med boring. Et interessant aspekt i bruken av LL i forbindelse med prosjekter, er at avdelingen i stor grad benytter LL til å videreføre kunnskap fra hendelser med både positivt og negativt utfall. Informant nr. 5 påpeker også at HMS-LL benyttes i prosjekter: «Ved utarbeidelse av prosjekter vil man også inkludere HMS-LL- fra tidligere prosjektet dersom det anses som hensiktsmessig.» (Informant nr. 5). En kan allikevel inkludere lessons learned fra tidligere prosjekter i prosjektprofilen.»

Dette kapitlet er avgrenset til struktur og distribusjon av LL med tilknytning til HMS. LL er i praksis en PDF-fil som kort beskriver kunnskap en ønsker å videreføre på en enkel og konkret måte. I Lundin benyttes en mal for LL-dokumenter med følgende struktur (se figur 5-16).

Lessons Learned – One Pager

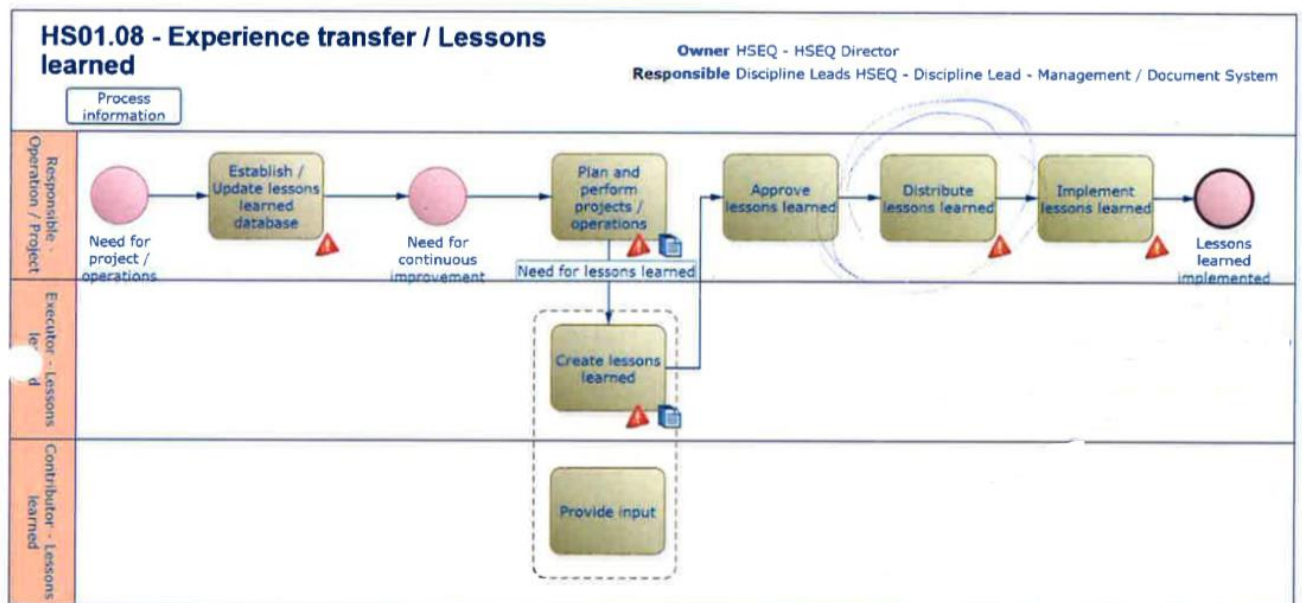
[tittel]

<p>Saksbeskrivelse:</p> <ul style="list-style-type: none"> [Beskriv pågående aktiviteter] [Hvor på installasjonen?] [Hvem/Hvor mange var involvert?] [Hvilke strakstiltak ble iverksatt?] <p>Faktisk konsekvens:</p> <ul style="list-style-type: none"> [Ved behov; beskrivelse av faktisk konsekvens] . <p>Potensiell konsekvens:</p> <ul style="list-style-type: none"> [Vurdering av risiko/tapspotensial. Hva kunne skjedd under marginalt endrede omstendigheter?] . . <p>Årsaker:</p> <ul style="list-style-type: none"> [Beskrivelse av årsaker til hendelsen; Bruk gjerne MTO-metodikk] . . <p>Lessons learned:</p> <ul style="list-style-type: none"> 	<p>Nøkkelinformasjon</p> <p>Lokasjon: [plattform, modul]</p> <p>Dato:</p> <p>Synergi #:</p>	<table border="1"> <thead> <tr> <th colspan="3">Granskning</th> </tr> </thead> <tbody> <tr> <td>N/A</td> <td>Pågår</td> <td>Fullført</td> </tr> <tr> <td></td> <td></td> <td></td> </tr> </tbody> </table>	Granskning			N/A	Pågår	Fullført			
	Granskning										
N/A	Pågår	Fullført									
	<ul style="list-style-type: none"> Klikk på ikon for å legge til bilde 										
	<ul style="list-style-type: none"> Klikk på ikon for å legge til bilde 										

Figur 5-16 Mal Leassons Learned dokument

Malen er utarbeidet etter hva som anses som mest hensiktsmessig i form av informasjon å inkludere, uten at det foreligger noen spesiell metodikk som ligger bak utarbeidelsen av dokumentet. Dersom LL-dokumentet er tilknyttet en sak i Synergi skal det være en direkte lenke til Synergi-saken i LL-dokumentet. Saksbehandlinger i Lundin kan resultere i tiltak som å opprette og distribuere LL i etterkant av saksbehandlingen. LL-dokumenter kan også inneholde beskrivelser som krever at man oppretter en sak i Synergi før den behandles etter saksgangen i Synergis struktur. LL og Synergi er på denne måten nært koblet, og en kan beskrive LL som en distribusjonsmetode for kunnskap fra Synergisaker.

I prosessverktøyet APOS ligger det en overordnet prosessbeskrivelse av saksgangen i forbindelse med utarbeidelse og distribusjon av LL. Informant nr. 3 erkjenner samtidig at denne prosessbeskrivelsen først og fremst er overordnet: «Prosessbeskrivelse i APOS er overordnet og legger ingen føringer for hvordan LL skal kommuniseres. Dette er opp til de enkelte prosjektene, og epost er den løsningen som oftest blir brukt, med de naturlige svakhetene dette innebærer» (Informant nr. 3).



Figur 5-17 Prosessbeskrivelse for utarbeidelse og distribusjon av Lessons Learned

Som følge av at LL er en etablert metode for kunnskapsoverføring i petroleumsnæringen, vil også ulike selskap systematisere LL-dokumenter på ulike måter. I Lundin eksisterer det ingen egen programvare for håndtering og distribusjon av LL-dokumenter, og det er først og fremst Microsoft Word, Excel og intern epost som benyttes.

Informant nr 5. understreker problematikken rundt dette: «Manko på prosedyrer knyttet til dokumentstyring har lenge vært en utfordring hos oss. Dette har blitt noe bedre, men det oppleves fortsatt som mangelfullt ift. mange systemer, og det er mye bruk av mapper og Excel-filer.» (Informant nr. 5).

LL vil i praksis utarbeides når sakseier opplever at det er hensiktsmessig å utarbeide og distribuere LL på bakgrunn av sakens innhold og verdi. Sakseier vil også da avgjøre hvem som skal få tilsendt epost med LL-dokumentet. Både informant nr. 1, 2 og 3 beskriver at epostdistribusjonen som i dag praktiseres har flere utfordringer. Epost er en kommunikasjonsmetode som også har svakheter i seg selv, ettersom eposter kan forsvinne i mengden, ikke nå fram, eller bli fanget av eposttjenerens eget søppelfilter. Mangelen på formaliserte prosedyrer for når LL skal utarbeides og for hvem det skal sendes til, medfører også at man legger stor tillit til sakseiers vurderingsevne i enkeltsaker:

LL sendes kun ut via epost, men det har vi egentlig ikke noe superbra system. Han som skriver LL sender jo ut til de personene som han føler det er fornuftig å sende til, basert på at kunnskapen skal spres ut til de som har behov for den (Informant nr. 3).

Som følge av svakhetene i dagens distribusjonsmetode har det ved flere tilfeller blitt vurdert å benytte distribusjonssystemer fra tredjeparter, uten at dette har ført til noe videre avgjørelser. Et eksempel på et slikt system er nettportalen lessonlearned.no som fungerer som en database for LL fra prosjekter, utstyr og andre områder tilknyttet oljeutvinning. En annen utfordring tilknyttet kunnskapsoverføring er eksterne LL. Eksterne LL betegnes som LL-dokumenter fra andre selskaper, leverandører og tredjeparter. Lundins tilgang til eksternt kunnskap begrenses til dels av selskapets størrelse, og informant nr. 1, 2 og 3 opplever at det mottas få eksterne LL-dokumenter: «Vi mottar få eksterne LL i Lundin. Dette kan være problematisk som følge av organisasjonen er begrenset i størrelse og antageligvis går glipp av en del relevant i bransjen» (Informant nr. 3). Som et forsøk på å øke antall innkommende LL fra eksterne kilder har det blitt opprettet en egen epostadresse som man forsøker å sende ut til eksterne aktører. Dette har som formål å øke antall eksterne LL slik at Lundin blir mer inkludert og oppdatert på hva som skjer i næringen. Samtidig opplever de ansatte at antallet innkommende LL er for lavt, og sitter med et inntrykk av at det potensielt er mye kunnskap som Lundin ikke evner å fange opp.

5.3.2 Synergi som distribusjonsverktøy

I tråd med betegnelsen til Aven et al. (2004) er Synergi i praksis et digitalt SIS basert på en reaktiv styringsløype-struktur hvor avvik kontinuerlig korrigeres i forsøk på å øke sikkerhetstilstanden i selskapet. I vurderingen av Synergis evne til å tilgjengeliggjøre informasjon er det derfor hensiktsmessig å se på hvordan Synergis struktur legger til rette for informasjonsuthenting. Som en følge av Synergis struktur tilbyr systemet en form for reaktiv loggføring av hendelser og forhold som allerede har funnet sted. Statistisk sett er det mulig å hente data om type hendelse/forhold, alvorlighetsgrad og frekvenser fordelt etter datoer. Ettersom databasen i Synergi ikke inneholder andre variabler som eksempelvis eksponeringstid, er det ikke mulig å hente ut videre analyser av datagrunnlaget. Dette må gjøres ved å manuelt hente ut statistikk fra Synergi, før det deretter analyseres andre steder.

Informant nr. 4 erkjenner at kategoriseringer i Synergi har vært diskutert over tid, da det er en utfordring å utarbeide et sett med kategorier som er representativt for alle former for hendelser og forhold. Som en viktig psykologisk faktor beskrevet som «Organisatoriske rammebetingelser og struktur» understreker Aven et al. (2004) hvordan hensiktsmessige kategoriseringer er en viktig faktor for informasjonsflyten i et SIS (Aven et al., 2004, s. 136). Kategoriene har også betydning for den videre saksgangen, da forskjellige personer er ansvarlig for forskjellige områder. Kategoriseringen påvirker også registreringen av informasjonen og tilgjengeligheten når saker skal søkes opp i ettertid. Det utføres i dag et pågående arbeid med å videreutvikle et sett med kategorier som effektivt evner å fange opp ulike former for hendelser og forhold i Lundin. Man kan argumentere for at en mer hensiktsmessig kategoriinndeling hadde bidratt til å redusere de utfordringene som i dag gjør det vanskelig å søke opp tidligere hendelser i Synergi. Tilgjengelighet er også et viktig kriterium for et SIS, ettersom et «SIS må kunne generere informasjon som er tilgjengelig til brukerne av systemet på en oversiktlig og lettvisning måte» (Aven et al., 2004, s.136).

Det er veldig mye informasjon som går inn i Synergi, men det er som et sort hull fordi det er vanskelig å finne tilbake til det. Et annet problem er at informasjonen ikke er tilgjengelig for alle, en må ha en bruker for å faktisk kunne gå inn å se. Dette er en barriere, siden nøkkelinformasjon selvfølgelig burde vært tilgjengelig for alle (Informant nr. 2).

Man kan argumentere for at et SIS burde være brukervennlig samtidig som lagret data må være tilgjengelig uavhengig av datamengde som befinner seg i databasen.

Som informant nr. 2 påpeker er det mye informasjon som ligger lagret i Synergi, og mye av dette kan anses som irrelevant for sikkerhetsstyringen i Lundin. På den andre siden kan man argumentere for at dette er en prioriteringssak hvor man heller ønsker for mye enn for lite registrert informasjon. Det vil allikevel være viktig at et SIS er brukervennlig og at brukerne må besitte en kompetanse til å hente frem den informasjonen de ønsker. Dette er en utfordring med dagens utforming av Synergi: «Likevel er det vanskelig å få tak i all informasjon, for du må ha en viss kunnskap om hvordan verktøyet fungerer for å kunne sette opp søk for å finne informasjon. Der er synergi litt gammeldags» (Informant nr. 1).

Basert på informantens utsagn er det grunn til å tro at Synergi har et brukergrensesnitt som gjør det vanskelig å søke etter tidligere saker og data. Hvorvidt løsningen på denne utfordringen er å øke ansattes kompetanse eller å utføre strukturelle endringer i Synergi, kan diskuteres. Et rimelig argument kan allikevel være at et SIS skal være intuitivt og at en slik egenskap vil kunne ha positive virkninger på flere områder, i form av opplæring, effektivitet og generell bruk av systemet i selskapet. Carr (2014) påpeker hvordan gevinsten av effektivisering fra automatisering og digitalisering til dels må betales av tap av menneskelig intuisjon i systemene (IRIS, 2018, s. 42). Dette argumentet kan belyse effekten av den stadige utviklingen av digitale systemer, samtidig som denne problematikken er å anse som en utfordring og ikke en hindring. Få personer vil hevde at et digitalt SIS fungerer godt om det ikke er brukervennlig, uavhengig av andre egenskaper.

En annen utfordring med hensyn til henting og vurdering av tidligere saker i Synergi er tilknyttet verifisering av lukkede tiltak og saker. Når eksempelvis en granskingsrapport ferdigstilles vil tiltak/aksjoner legges inn i Synergi og deretter tilegnes ulike ansatte med relevante ansvarsområder. Enkeltpersoner vil da være ansvarlig for å lukke tildelt aksjoner/tiltak, uten at det foreligger krav om å gjøre seg kjent med saken. Det vil i disse tilfeller være sakseier som er ansvarlig for å verifisere at tiltak og aksjoner er gjennomført på tiltenkt måte.

Dette er en konsekvens av måten Synergi er strukturert på. En får tilsendt epost som sier at en har fått tildelt et tiltak, og en kan jo da klikke seg inn i saken og lese alt, men enkelte vil jo heller bare lese det tildelte tiltaket og fokusere på hva som må gjøres for å få lukket det. Det foreligger ingen krav om at en må gjøre seg kjent med saken. Så det er jo stort rom her for å gjøre ting annerledes enn det som var opprinnelig tiltenkt i utformingen av tiltaket. I praksis kan personen lukke tiltaket uten å ha gjort noe som helst, for eksempel dersom han syntes tiltaket er meningsløst. Men det vil være eieren av saken som er ansvarlig for at tiltakene har blitt utført på en hensiktsmessig måte som sakseier (Informant nr. 2).

Selv om Synergi er et SIS med reaktiv struktur, er det ikke dermed sagt at datagrunnlaget ikke kan benyttes til ledende indikatorer. Hvorvidt dette utføres i praksis hos Lundin, og til hvilken grad av validitet vi finner i de ledende indikatorene kan diskuteres. Informant nr. 1 forteller at Lundin er opptatt av å bruke ledende indikatorer, men understreker at det viktigste er at indikatoren faktisk er målbar:

Det viktigste når vi definerer en indikator er at det må være målbart. Vi måler risikonivået veldig konkret, og vi forsøker å unngå et reaktivt fokus bare på hendelser. Ledende indikatorer må fokusere på risikoanalyser. Et eksempel på dette er å se hvorvidt det er forskjell på risikonivå over tid. Vi ser blant annet på utviklinger i fra vernerunder og endringer over tid (Informant nr. 1).

Denne praktiske bruken av ledende indikatorer eksemplifiseres av informant nr. 2 som beskriver hvordan mindre hendelser uten betydelige konsekvenser benyttes som kilder for kunnskap:

Har du mange lekkasjer på riggen som ikke går til sjø, men fanges opp på dekk så er også dette et tegn eller en indikator på at neste gang vil lekkasjen kanskje gå ut i sjøen istedenfor. Så du prøver hele tiden å følge opp slike hendelser som går bra. Men vi er nok ikke så flinke til å ha indikatorer som er enda mer ledende da. Som regel må det være en eller annen hendelse som er målbar, som ikke nødvendigvis er alvorlig, men som gir en indikator på at neste gang kan det gå dårligere. Men dette er jo også en etterslepene indikator ettersom det er en reaktiv reaksjon, men vi prøver jo å bruke de observasjonene vi får inn daglig som ledende indikator (Informant nr. 2).

Lundin benytter seg av mindre betydelige uønskede hendelser og endringer i kvantitative risikoanalyser som datagrunnlag for ledende indikatorer. Man kan argumentere for at slike indikatorer faller under Reiman & Pietikäinens (2012) betegnelse på outcome indicators. Outcome indicators måler midlertidige sluttresultater fra kontinuerlige prosesser og aktiviteter, som i Lundin utgjør resultater fra operative prosesser offshore. En svakhet i benyttelsen av slike data til å vurdere sikkerhetsnivå i organisasjonen er at de ikke nødvendigvis representerer det reelle sikkerhetsnivået i organisasjonen (Reiman & Pietikäinen, 2012, s. 1998).

Uønskede hendelser og historisk ytelsesdata vil naturligvis kunne være gode kilder til kunnskap om sikkerhet, samtidig som et lavt antall eller fravær av uønskede hendelser ikke være synonymt med høy sikkerhet. Et fravær av uønskede hendelser kan for eksempel være et resultat av tilfeldigheter og ikke en høy sikkerhetstilstand.

Hollnagel (2017) trekker frem læring som en aktivitet som må skje i det daglige og ikke være begrenset til hendelser med negativt utfall (Hollnagel, 2017, s. 64).

En kan argumentere for at dette også er praksis i Lundin, da det forsøkes å dra kunnskap fra uønskede hendelser uten betydelige negative konsekvenser. I større prosjekter benyttes LL-dokumenter til å videreføre kunnskap om blant annet referansebrønner og hva som har vært vellykket i arbeidet, uten at dette har en direkte tilknytning til sikkerhet. Hvorvidt Lundin evner å bevisst trekke sikkerhetskunnskap fra daglige hendelser er derfor vanskelig å konkludere. Informant nr. 4 trekker frem følgende:

Oppsummeringer av kampanjer og øvelser blir plukket opp og tatt med i neste planlegging. Vi kan ikke bli overrasket over at ting går bra. Vi må ha en strukturell tilnærming til det som går bra. Det oppleves derfor som mer hensiktsmessig å lære av det som går galt (Informant nr. 4).

Man kan argumentere for at det er mulig å trekke mye kunnskap fra hendelser som går bra og at dette også kan benyttes som ledende indikatorer for å predikere endringer i sikkerhetstilstanden. Dersom man også evner å fange opp ytelsesendringer fra hendelser med positive utfall vil en, i teorien, ha en større database å hente kunnskap fra. Dette støttes også av «Precursor Resilience»-perspektivet, som beskriver et systems evne til å monitorere forhold i et system og evnen til å gripe inn å korrigere dersom det oppstår uakseptable forhold (Pettersen, 2019, s. 52). For at en slik tilnærming skal kunne være effektiv det samtidig være viktig at denne kunnskapen blir benyttet og kommunisert til riktige aktører i organisasjonen. Informant nr. 2 trekker frem følgende betraktninger tilknyttet kommunikasjon av ledende indikatorer:

Proaktive indikatorer kan være litt vanskeligere å kommunisere, ettersom de er mindre intuitive. Har du snublet og brekt en fot så er det en veldig håndgripelig greie å ta tak i, men å eksempelvis presentere skadestatistikk basert på potensiale til en hendelse vil skape mer rom for diskusjon (Informant nr. 2).

Det er tydelig at Lundin som selskap besitter flere perspektiver på sikkerhetsstyring og HMS som samsvarer med moderne faglitteratur og betraktninger. Fokuset på ledende indikatorer og monitorering av sikkerhetsnivået i organisasjonen er tydelig en høy prioritet.

Digitaliseringens effekter er også synlig i den stadige utviklingen av de digitale systemene som benyttes i HMS-arbeidet, ikke bare i Lundin, men på tvers av petroleumsnæringen. Samtidig kan man hevde at det eksisterer et gap mellom systemenes formål og det praktiserende arbeidet som utføres. Aller tydeligst er kanskje kommunikasjonen av kunnskap. Det er få utfordringer tilknyttet registrering av hendelser i Synergi, samtidig oppleves det som utfordrende å hente ut denne kunnskapen i ettertid som følge av systemets utforming. Dette kan igjen føre utfordringer både ved sporing av tiltak og kunnskapsoverføring i selskapet. Distribueringen av LL-dokumenter er også et område med rom for forbedringer, ettersom kommuniseringen av LL i dag foregår via epost. Det er også enkelte uklareheter tilknyttet distribueringslister og beslutninger over hvem som bør få tilsendt et LL-dokument. Digitaliseringen er i dag synlig hos Lundin med introduksjonen av barrierepanelet og visualisering av nøkkeltall på skjermer. Denne formen for effektivisering vil være avhengig av pålitelige systemer for behandling av kunnskap, og det bør derfor brukes ressurser på å utvikle så intuitive systemer som mulig. Digitalisering, vekst, og dynamiske omgivelser i bransjen vil kunne møtes av en proaktiv og resilient sikkerhetsstyring hvor man benytter tilgjengelig kunnskap for å hele tiden være forberedt på det utenkelige. Kanskje kan fokus på resiliens og bruk av verktøy fra RE være bidragsgivende i dette arbeidet. Som følge av at prosjektet i stor grad er teoretiske forankret i arbeidet til Erik Hollnagel, ble det ansett som bidragsgivende å kontakte Hollnagel for å høre hvilke tanker han har om arbeidet med resiliens, sikkerhet og digitalisering i et operatørselskap. Hollnagel bidro med følgende betraktninger i sammenheng med dette prosjektet: «Digitaliseringen gjør det stadig vanskeligere å forstå hvordan arbeidsprosesser og funksjoner henger sammen og påvirker hverandre. Det vil kreve at vi hele tiden utvikler bedre metoder, modeller, og teorier. Behovet for metoder som RAG vil derfor stige i årene fremover» (E. Hollnagel, personlig kommunikasjon, 22.04.2019). Økende kompleksitet i organisasjoner som følge av digitalisering vil kunne medføre utfordringer til den tradisjonelle tilnærmingen til sikkerhetsstyring. En fremtidsrettet sikkerhetsstyring med fokus på egenskaper som vektlegges i RE vil derfor kunne være bidragsgivende. Det er ikke nødvendigvis visuelle systemer som bidrar til en synlig sikkerhetstilstand, men evnen å fange opp nødvendig kunnskap på et nødvendig tidspunkt. Hollnagel (2009) beskriver ved hjelp av ETTO-prinsippet hvordan beslutninger i det daglige arbeidet hele tiden er en avveie mellom effektivitet og nøyaktighet. Dette gjør seg spesielt synlig i sikkerhetsarbeid, hvor effektivitet ofte reduseres helt til sikkerhetsmål er nådd (Hollnagel, 2009, s. 15) Tradisjonelle kvantitative målsetninger for sikkerhetsarbeidet vil kunne medføre et for stort fokus på fraværet av hendelser, i motsetning til et fokus på den reelle sikkerhetstilstanden i organisasjonen.

Det bør derfor utarbeides målsetninger som ikke er direkte tilknyttet kvantitative målinger, men heller setter søkelys på hvordan sikkerhet påvirkes av de prosessene som skjer i det daglige. Kunnskapsoverføring burde derfor også skje i det daglige, og ikke være isolert til de unike uønskede hendelsene som tilhører sjeldenhetene.

7.0 Konklusjon

I dette prosjektet var formålet å belyse hvordan digitale sikkerhetsinformasjonssystemer i Lundin kan bidra til resiliens i selskapet. Steen & Aven (2011) beskriver RE som sikkerhetslitteraturens motsvar til organisasjoners økende kompleksitet og utvikling som følge av blant annet digitaliseringen. Resiliens betegnes av Hollnagel (2017) som et uttrykk for et systems ytelse under forventede og uforventede forhold, og kan derfor hevdes å være et mål for sikkerhet som skiller seg fra annen litteratur. Som en følge av dette og begrepets økende bruk innenfor moderne sikkerhetslitteratur, benyttes resiliens i dette prosjektet som en form for idealmål for sikkerhet. Det er samtidig viktig å poengtere at resiliens ikke nødvendigvis er synonymt med høy sikkerhet; i dette prosjektet anses teorien som verdifull da den tilbyr nye perspektiver på sikkerhetsstyring som kan bidra til å fange forhold som tidligere ikke har blitt viet oppmerksomhet.

For å kunne besvare prosjektets problemstilling var det nødvendig å kartlegge hvilke digitale systemer som benyttes til håndtering av sikkerhetsinformasjon i Lundin. For å kunne besvare hvorvidt disse systemene besitter egenskaper som kan bidra til resiliens i selskapet var det nødvendig å kartlegge systemenes struktur, utforming og praktiske bruk. Et digitalt sikkerhetsinformasjonssystem har som formål å videreføre og fremme kunnskapsoverføring med betydning for selskapets sikkerhetsstyring. Det ble derfor nødvendig å kartlegge hvilke kilder til kunnskap som benyttes i det digitale SIS-et og hvordan systemene benyttes til monitorering. Videre ble det etter forskningsspørsmålenes oppdeling vurdert som hensiktsmessig å kartlegge hvordan innhentet informasjon blir systematisert og distribuert. Denne oppdelingen av forskningsspørsmålene oppleves som dekkende for funksjonene og kunnskapens livsløp i et SIS.

Lundin har i dag et høyt fokus på sikkerhet, noe som synliggjøres i målsetninger og planverk. Det utføres kontinuerlig diskusjoner om hvordan ny teknologi og digitale løsninger kan bidra i HSE-arbeidet. Dette er også synlig i HSEQ-planen for 2019, hvor det trekkes frem at skjermer med visualisering av nøkkeltall og progresjoner skal installeres på avdelingene. På avdelingen høres man også hvordan begreper som «ledende indikatorer» og «HMS-2» flittig blir brukt og trukket frem. HMS-2 brukes i Lundin som betegnelsen på «Safety 2» og arbeidet med å lære fra hendelser uten negative utfall.

Disse begrepene har sitt opphav i RE og kan sies å være synlige tegn på at denne litteraturen er i ferd med å få fotfeste i et moderne operatørselskap, og kan sies å være en viktig forutsetning i veien mot resiliens.

Lundins evne til å monitorere og innhente kunnskap med betydning for sikkerhet er i dag begrenset til de rammene som de digitale systemene setter. Synergi fungerer i dag som en database hvor mye informasjon tilføres, samtidig som det eksisterer utfordringer ved å hente ut informasjon som oppleves som relevant for sikkerhetsarbeidet. Synergis manglende evne til å produsere statistikk eller automatiske varslinger kan diskuteres som en mulig svakhet eller et ledd i kvalitetssikringen av informasjon. Rådata fra Synergi hentes i dag ut manuelt før det benyttes i rater og analyser, og på denne måten vil enkelte ansatte ha et stort ansvar for å oppdage uønskede trender eller utviklinger. Hvorvidt dette er en svakhet eller styrke vil kunne hevdes å være betinget av selskapets størrelse og datamengde, og bør være et fokusområde i årene som kommer, med tanke på selskapets vekst. Prosjektets funn tyder på en utstrakt bruk av reaktive outcome indikatorer, både i form av KPI-er og i det daglige HMS-arbeidet. Dette må kunne sies å være et område med forbedringspotensial. Ledende indikatorer kan være et nyttig verktøy som kan bidra til å fange kunnskap og dermed være et viktig steg i veien mot resiliens, men er samtidig ikke et absolutt krav innenfor RE-litteratur. Verdien av å øke andelen av ledende indikatorer må allikevel ikke avfeies, da dette i stor grad kan styrke selskapets evne til å fange opp utviklinger og endringer i sikkerhetstilstanden før dette når et uakseptabelt nivå, i tråd «Precursor Resilience».

Synergi er i dag et etablert system i Lundin og i petroleumsnæringen generelt. Selv om Synergi i stor grad er etablert og akseptert er det også utfordringer tilknyttet prosesser i daglige HMS-arbeidet. Det oppleves som tungvint å signere tiltak som utført i Synergi, ettersom saker med tiltak tilegnet ulike avdelinger manuelt må sendes frem og tilbake mellom avdelinger. Saker og tiltak blir i enkelte tilfeller stående som åpen uten at dette oppdages umiddelbart. Det hviler også et stort ansvar på ansatte som får tildelt tiltak, da tiltak kan lukkes uten at de i praksis er utført. Den årlige tiltaksverifikasjonen er heller ikke dimensjonert til å gjennomgå alle tiltak og saker fra det forbigående året. Det vil være naturlig å diskutere hvorvidt dagens kvalitetssikring av tiltak- og sakslukking er tilstrekkelig, ettersom man med dagens system risikerer at saker og tiltak blir stående som åpen og at mulige risikoforhold får utvikle seg.

Utfordringene rundt tiltak- og sakslukking i Synergi er også synlig i etterkant av interne granskinger. Interne granskinger vil ofte resultere i anbefalinger hvor etterlevelse er vanskelig å måle; eksempelvis vil noen anbefalinger ikke legges inn som tiltak i Synergi. Dette gjør det vanskelig å måle etterlevelse av selve tiltaket og den ønskede effekten. Systematiseringen av kunnskap utføres også ved hjelp av andre digitale systemer, hvor barrierepanelet er det nyeste i rekken. Barrierepanelet eksemplifiserer hvordan digitale løsninger kan benyttes til å systematisere kunnskap på en måte som tilsynelatende styrker arbeidet med HSE.

Barrierepanelet tilfører sikkerhetsarbeidet i Lundin en proaktiv dimensjon som gir muligheten til å predikere hvordan nedetid på barrierer vil påvirke risikobilde med hensynet til storulykker. Barrierepanelet vil utvilsomt kunne regnes som et viktig bidrag i arbeidet med sikkerhet, samtidig som det også kan medføre utfordringer knyttet til fremmedgjøring blant de ansatte. Det bør derfor tildeles ressurser til ivaretagelse av ansattes kompetanse og bruk av barrierepanelet, slik at panelet ikke blir en kilde til misforståelser og kunstig trygghet. Dagens indikatorbruk i Lundin representerer i stor grad et selskap som setter sikkerhet høyt, samtidig som man er opptatt av moderne utviklinger som fremkommer i sikkerhetslitteraturen.

Samtidig må begreper og holdninger transformeres til handlinger og systemer som tilrettelegger for resiliens og høy sikkerhet i et selskap i vekst.

Distribuering av kunnskap ble valgt som tredje og siste forskningsspørsmål, og tar sikte på å redegjøre for hvordan kunnskap fra Synergi distribueres og benyttes i sikkerhetsstyringen. Selv om Lundin har systemer som evner å samle inn og systematisere kunnskap om sikkerhetsrelevante forhold, vil dette være til liten nytte dersom man mangler prosedyrer og rutiner for å distribuere denne kunnskapen til viktige beslutningstakere og ansatte. Dette forskningsspørsmålet tar også sikte på å besvare en praktisk dimensjon i arbeidet rundt kunnskapsoverføring, da øvrige systemer kan etterleve forskrifter uten at man bruker kunnskapen som systemene tilgjengeliggjør. Denne studien har avdekket flere forbedringsområder i Lundins organisering av LL-dokumenter. Det er flere svakheter i dagens organisering hvor epost benyttes som kommunikasjonsform. Mange ansatte mottar daglig store mengder utstrakt bruk av office» epost hvor LL-dokumenter risikerer å forsvinne i mengden, om de ikke heller blir fanget av søppelfiltre eller lignende. Det er også manglende formelle retningslinjer som konkretiserer hvilke ansatte som skal motta hvilke dokumenter. Man kan spørre seg om prioriteringer av visualiserte systemer, slik som barrierepanelet og skjermer med KPI-tall, overensstemmer med å prioritere sikkerhet når det eksisterer betydelige mangler

omkring kommunikasjon av LL-dokumenter og kunnskap fra forhold og hendelser. Det er viktig at beslutningstakere som ønsker å ivareta en sikkerhetsfokusert ressursprioritering ikke ser seg blind på digitaliseringens effektivitet, men evner å se systemenes samlede effekt i forhold til organisasjonens behov. Det vil derfor anbefales at Lundin tydeliggjør sine retningslinjer rundt utsendelse av LL-dokumenter, både med hensyn til mottakslistene og systemer for organisering av LL-dokumentene. En utstrakt bruk av Microsoft Office basert på ad-hoc løsninger er også et område som bør vies oppmerksomhet i tiden fremover, kanskje er det mulig å sammenslå flere av dagens prosesser inn i et system. En konkret anbefaling vil kunne være å integrere LL-distribusjon inn i Synergi, slik at en dermed kan kvalitetssikre organiseringen i større grad.

Dette prosjektet har hatt som formål å belyse hvordan perspektiver fra RE kan belyse kunnskapsoverføring i et moderne operatørselskap, for å se hvorvidt etablerte prosesser samsvarer med RE. Som påpekt av Hollnagel gjør digitaliseringen det stadig vanskeligere å forstå hvordan arbeidsprosesser og funksjoner henger sammen og påvirker hverandre. Det er derfor et økende behov for å utvikle bedre metoder, modeller og teorier som evner å følge den raske utviklingen som følge av digitalisering. Basert på denne antakelsen vil behovet for metoder som RAG stige de neste årene. Digitaliseringens effekter er synlig både i petroleumsnæringen generelt, og i Lundin. For at digitaliseringens konsekvenser skal kunne utnyttes i sikkerhetsarbeidet de neste årene, er det viktig at man vier oppmerksomhet til den økte kompleksiteten digitaliseringen også kan medføre. Introduksjonen av forenklete visualiseringer av komplekse prosesser vil kunne effektivisere arbeidet med sikkerhet, samtidig som man risikerer å miste oversikten over de antakelsene og prosessene som skjuler seg bak systemene. Hollnagel (2009) beskriver ved hjelp av ETTO-prinsippet hvordan beslutninger i det daglige arbeidet hele tiden er en avveie mellom effektivitet og nøyaktighet. Dette gjør seg spesielt synlig i sikkerhetsarbeid, hvor effektivitet ofte reduseres helt til sikkerhetsmål er nådd (Hollnagel, 2009, s. 15). Det er viktig at Lundin som selskap derfor ikke vier for mye oppmerksomhet mot rigide og kvantitative sikkerhetsmål og visualiseringer, men heller fokuserer på sikkerhet som en dynamisk tilstand som påvirkes av en rekke organisatoriske faktorer. Denne tilstanden må kontinuerlig vedlikeholdes og prioriteres. En av de viktigste faktorene for det videre arbeidet med sikkerhet i Lundin er kommunikasjon og distribusjon av viktig kunnskap. Etersom sikkerhet påvirkes av hele organisasjonen er det også viktig at sentral sikkerhetsinformasjon kommuniseres til hele organisasjonen, og at de digitale systemene også bidrar til at denne informasjonen tilgjengeliggjøres og distribueres. Dette samsvarer også med

formålene til verktøy som RAG. Dersom Lundin i større grad ønsker å implementere RE i sin sikkerhetsstyring, vil denne studien kunne være bidragsgivende og fungere som en kartlegging av delprosesser som inngår i RE. Dagens digitale sikkerhetsinformasjonssystemer bidrar til resiliens i den grad de oppfyller delkrav slik som bruk av ledende indikatorer og kunnskapshenting fra hendelser uten negative utfall, selv om dette innebærer utfordringer i praksis. Det er samtidig en stor forskjell på å ha systemer som kan bidra til resiliens og det å ha resiliens. Det er derfor viktig å videreutvikle dagens systemer, og i større grad vektlegge hvordan sikkerhet ikke bare er et fravær av hendelser, men en dynamisk tilstand som krever overblikk og oppmerksomhet fra hele organisasjonen hver dag.

8.0 Forslag til videre forskning

Dette prosjektet har avgrenset seg til hvordan perspektiver fra RE kan benyttes til å vurdere systemer og praksis med hensyn til kunnskapsoverføring. Et utdrag av RAG-modellen har også blitt benyttet til å belyse monitoreringsprosesser i Lundin, men dette har vært gjort uten å vurdere hele organisasjonens potensiale for resiliens. Det ville ha vært interessant å utføre en større analyse ved hjelp av RAG-modellen i sin helhet, for å forsøke å kartlegge alle egenskapene som inngår i RAG-modellen, og dermed vurdere hvorvidt Lundin besitter egenskaper som kreves for å være resilient. Denne analysen vil også kunne belyse kunnskapsoverføringen fra et større perspektiv, og vil kunne belyse eventuelle konsekvenser av dagens utfordringer tilknyttet systemer for kommunikasjon av sikkerhetsrelevant informasjon i selskapet. En slik studie kunne inkludert flere avdelinger og ansatte med operative stillinger offshore, og dermed fanget et større bilde av kunnskapsoverføringen i Lundin.

I en forskningsartikkel produsert av Sintef introduseres en metode for å utvikle tidlige varslingsindikatorer basert på RE. Metoden baserer seg på tre hoveddeler, hvor man stegvis utvikler suksessindikatorer basert på egenskaper som sammen utgjør resiliens. Videre utvikles underindikatorer for å kunne måle etterlevelse av suksessindikatorene. Denne fagartikkelen illustrerer at det er mulig å utvikle et sett med indikatorer som tidlig kan varsle og fange opp utviklinger, før de får lov til å utvikle seg til farlige forhold. Dette inkluderer også utforutsette forhold (Øien, Massaiu, Tinmannsvik & Størseth, 2010, s. 1) Det anbefales at Lundin i større grad integrerer denne metodikken i det fremtidige arbeidet med sikkerhet. En slik metodikk vil kunne bidra til å videreutvikle eksisterende indikatorer som brukes i dag. Et slikt prosjekt kan bidra til å gjøre selskapet som helhet mer forbered på å takle forhold og risiko som man vet at man kjenner til, men også de skjulte farene man ikke vet at man ikke kjenner til. De sorte svanene.

Litteraturliste

- Aven, T., Boyesen, M., Njå, O., Olsen, K., & Sandve, K. (2004). *Samfunnssikkerhet*. Oslo: Universitetsforlaget.
- Bartnes, M., (2013). *Resilience – fra safety til security* . Hentet fra <https://infosec.sintef.no/informasjonssikkerhet/2013/01/resilience-fra-safety-til-security/>
- Blaikie, N. (2010). *Designing social research : The logic of anticipation* (2nd ed.). Cambridge: Polity Press.
- Dixon, N, M., (1999). *The Organizational Learning Cycle* (2. utg.). Hampshire, England: Gower Publishing Limited.
- DNV GL. (2019A). *A test of resilience: the outlook for the oil and gas industry in 2019*. Hentet fra http://images.e.dnvgl.com/Web/DNVGL/%7Bc86f4852-e559-432f-b2ed-03a47af527fc%7D_DNV_GL_Industry_Outlook_Report_2019_-_A_test_of_resilience.pdf?utm_campaign=OG_GLOB_19Q2_PROM_2019-IndustryOutlook-Report-download-confirmation-email-R2&utm_medium=email&utm_source=Eloqua&elqTrackId=7ccffa0c706e4060aa684c2218de8e8c&elq=749a3c4167f34656b65f74a6e06ab712&elqaid=10842&elqat=1&elqCampaignId=
- DNV GL. (2019B). *How does Synergi Life work?* Hentet 05.04.2019 fra <https://www.dnvgl.com/software/software-services/how-does-synergi-life-work.html>
- Endresen, R. (2015) *Lundin Petroleum - The Most Successful Explorer*. Hentet fra <https://www.nord24.no/svenske-lundin-jakter-stort-funn-i-nytt-omrade/s/5-32-49558>
- Engen, O, A, H., (2017). *Helse, arbeidsmiljø og sikkerhet i petroleumsvirksomheten*. Rapport fra partssammensatt arbeidsgruppe. Hentet 27.03.2019, fra URL <https://www.regjeringen.no/contentassets/0a217a1b53a84a5b877bc526d67a5c5f/helse-arbeidsmiljo-og-sikkerhet-i-petroleumsvirksomheten.pdf>

- Engen, O., Kruke, B., Lindøe, P., Olsen, K., Pettersen, O., & Pettersen, Kenneth Arne. (2016). *Perspektiver på samfunnssikkerhet*. Oslo: Cappelen Damm akademisk.
- Gressgård, L., Melberg, K., Risdal, M., Tømmerås Selvik, J., & Østgaard Skotnes, R., IRIS. (2018). *Digitalisering i petroleumsnæringen* (7303019) Hentet fra <https://www.ptil.no/contentassets/50e7e658ebfa4bf2b52a8f94ef52a2ce/digitalisering-i-petroleumsnaringen.pdf>
- Holling, C. S. (1973). *Resilience and stability of ecological systems*. Annual Review of Ecology and Systematics, 4, 1–23.
- Hollnagel E., Wears R.L. and Braithwaite J. (2015). *From Safety-I to Safety-II: A White Paper. The Resilient Health Care Net*: Published simultaneously by the University of Southern Denmark, University of Florida, USA, and Macquarie University, Australia
- Hollnagel, E. (2009). *The ETTO principle: Efficiency-thoroughness trade-off : Why things that go right sometimes go wrong*. Burlington, Vt: Ashgate.
- Hollnagel, E. (2017). *Safety-II in Practice: Developing the Resilience Potentials*. Routledge.
- Jacobsen, D. (2015). *Hvordan gjennomføre undersøkelser?: Innføring i samfunnsvitenskapelig metode* (3. utg. ed.). Oslo: Cappelen Damm akademisk
- LNAS (2019) *LNAS HSEQ Plan 2019* (002561). Hentet fra internt nettverk
- Lundin (Hentet 05.04.2019) *Et moderne oljeeventyr i Nordsjøen*. Hentet fra: <https://www.lundin-norway.no/2019/04/05/et-moderne-oljeeventyr-i-nordsjoen/>
- Lundin Norway (2018). *Audit Report - Execution and learning from investigations* (006380). Hentet fra internt nettverk
- Lundin Norway. (Hentet 12.03.2019) *Johan Sverdrup*. Hentet fra: <https://www.lundin-norway.no/2017/02/02/johan-sverdrup/>
- Lundin Petroleum. (Hentet 08.03.2019) *Historie*. Hentet fra: <https://www.lundin-petroleum.com/sv/om-oss/historik/page/2/>

- Nonaka, I., & Takeuchi, H., (1995). *The knowledge-creating company: how Japanese companies create the dynamics of innovation*. New York: Oxford University Press.
- Norsk Petroleum. (Hentet 10.05.2019) *Selskapets reserver per felt ved årsskiftet*. Hentet fra <https://www.norskpetroleum.no/fakta/selskap-utvinningstillatelse/lundin-norway-as/>
- Petroleumstilsynet. (2013). *En bok om læring*. Hentet fra https://www.ptil.no/contentassets/17aa07f6f5e44e4a91244835509bb70e/laring_shefte_lavopplost-norsk.pdf
- Pettersen, K, G., (2019) *Precursor Resilience in Practice – An Organizational Response to Weak Signals*. In: Wiig S., Fahlbruch B. (eds) *Exploring Resilience*. SpringerBriefs in Applied Sciences and Technology. Springer, Cham
- Rammeforskriften. (2010). *Forskrift om helse, miljø og sikkerhet i petroleumsvirksomheten og på enkelte landanlegg*. (FOR-2010-02-12-158). Hentet fra <https://lovdata.no/dokument/SF/forskrift/2010-02-12-158>
- Reason, J. (1997). *Managing the risks of organizational accidents*. Aldershot: Ashgate
- Reiman, T. & Pietikäinen, E. (2012). *Leading indicators of system safety – Monitoring and driving the organizational safety potential*. *Safety Science*, 50 (10), 1993-2000. <https://doi.org/10.1016/j.ssci.2011.07.015>.
- Reuters. *Lundin in article*. Forsidebilde. Hentet (15.05 2019) fra <https://www.reuters.com/media-campaign/brandfeatures/business-debate-gg/lundin-in-article.jpg>
- Ringdal, K. (2018). *Enhet og mangfold : Samfunnsvitenskapelig forskning og kvantitativ metode* (4. utg. ed.). Bergen: Fagbokforlaget.
- Rosness, R., SINTEF (2010). *Organisational Accidents and Resilient Organisations: Six Perspectives*. Revision 2. (SINTEF A17034). Hentet fra https://www.sintef.no/globalassets/upload/teknologi_og_samfunn/sikkerhet-og-palitelighet/rapporter/sintef-a17034-organisational-accidents-and-resilience-organisations-six-perspectives.-revision-2.pdf

- Skre, I.B. (2018). *resiliens*. I *Store norske leksikon*. Hentet 02.03.2019 fra <https://snl.no/resiliens>
- Standard Norge. (2012). *Samfunnssikkerhet - Beskyttelse mot tilsiktede uønskede handlinger – Terminologi (NS 5830:2012)*.
- Steen, R., & Aven, T. (2011). *A risk perspective suitable for resilience engineering*. *Safety Science*, 49(2), 292-297. Hentet fra <https://www.sciencedirect.com/science/article/pii/S0925753510002237>
- Styringsforskriften. (2010). *Forskrift om styring og opplysningsplikt i petroleumsvirksomheten og på enkelte landanlegg (FOR-2010-04-29-611)* Hentet fra <https://lovdata.no/dokument/SF/forskrift/2010-04-29-611?q=styringsforskriften>
- Thagaard, T. (2018). *Systematikk og innlevelse: En innføring i kvalitative metoder* (5. utg. ed.). Bergen: Fagbokforlag
- Thomas, M.J., (2012). *A Systematic Review of the Effectiveness of Safety Management Systems (AR-2011-148)*. Hentet fra https://www.atsb.gov.au/media/4053559/xr2011002_final.pdf
- Tinmannsvik, R, K. SINTEF. (2011) *Deepwater Horizon-ulykken: Årsaker, lærepunkter og forbedringstiltak for norsk sokkel (SINTEF A19148)*. Hentet fra https://www.sintef.no/globalassets/upload/konsern/media/deepwater-horizon---sintef_23.06.11.pdf
- Unruh, G., Kiron, D. (2017). *Digital Transformation on Purpose*. MIT Sloan Management Review. Hentet 12.04.19 fra <https://sloanreview.mit.edu/article/digital-transformation-on-purpose/>
- Øien, K., Massaiu, S., Tinmannsvik, R, K., & Størseth, F. (2010). *Development of Early Warning Indicators based on Resilience Engineering*. 10th International Conference on Probabilistic Safety Assessment and Management 2010, PSAM 2010. 3.

Lundin HSEQ, Key Performance Indicators for 2019:

Topic	KPI	Description	Indikatorotype
Working environment	Work related illness cases	The target is related to the number of possible work-related illnesses reported to the authorities by LNAS' Occupational medicine physician according to regulatory provisions.	- Kvantitativ - Etterslepende - Outcome indicator
Serious incidents	Serious Incident Frequency	A Serious Incident defines as an incident with high actual and/or potential HSE consequence (Consequence area = red).	
Serious incidents	Serious Accident Frequency	A Serious Incident defined as an incident with high actual HSE consequence (Consequence area = red).	
Serious incidents	Perfect HSE Day	A Perfect HSE Day is defined as a day without recordable	- Kvantitativ - Etterslepende

		injuries, dropped objects or recordable spills.	- Drive indicator
Personnel Injuries	Total Recordable Injury Frequency	TRIF includes Medical Treatment Injuries, Restricted Work Injuries, Lost Time Injuries and Fatalities.	- Kvantitativ - Etterslepene - Outcome indicator
Dropped objects	Dropped objects > 40J outside secured area	Dropped objects directly to sea not included	
Process safety	Loss of Primary Containment Tier 1 incidents		
Spills and discharges	Unplanned discharges	All authority notifiable discharges to sea (all spills above 10 000L yellow chemicals, 10L red/black chemicals).	
Quality	No. of overdue actions in Synergi classified as yellow or red criticality	All actions classified with yellow and red category shall be closed within the set deadlines.	
Quality	Action verification for yellow and red incidents	Verify effect of implemented actions. To be monitored and verified quarterly by each department.	

Security	Course Completion	Percentage of all personnel with access to LNAS IT systems that has completed relevant courses launched.	<ul style="list-style-type: none"> - Kvantitativ - Ledende - Monitor indicator
Security	No. of security incidents that exploited known vulnerabilities	We have some known vulnerabilities within our IT systems and access to our facilities. The aim of the KPI is to measure incidents where these vulnerabilities are exploited.	<ul style="list-style-type: none"> - Kvantitativ - Etterslepende - Drive indicator
Security	No. of security incidents that resulted in damage, compromise or loss to the organizations assets, functions or stakeholders	Security incidents with actual consequences	
Emergency Preparedness	Completion of Emergency Response training	Percentage of training and exercises performed according to established plans.	<ul style="list-style-type: none"> - Kvantitativ - Etterslepende - Drive indicator
Emergency Preparedness	Notification of emergency response situations	The no. of actual and potential emergency situations that is notified	<ul style="list-style-type: none"> - Kvantitativ - Etterslepende - Outcome indicator

Vedlegg 2

Intervjuguide for opphold 1 av 2

Kort introduksjon om forskningsprosjektet:

Resilience engineering er et nyere fagfelt som forsøker å besvare et økende behov for nye metoder for sikkerhetsstyring, på bakgrunn av sosio-tekniske systemers økende kompleksitet. Resiliens er definert som en organisasjons evne til å operere under forventede og uventede forhold. Innenfor resilience engineering er det flere byggesteiner som må ligge til rette for at en organisasjon skal kunne være resilient. Informasjonsbehandling (monitorering) er en sentral egenskap eller byggestein. Dette forskningsprosjektet har derfor som formål å se hvordan digitale sikkerhetsinformasjonssystemer i et suksessfullt operatørselskap benyttes til sikkerhetsstyring og til hvilken grad systemene og prosessene er i tråd med byggeklossene fra «resilience engineering». Det er herunder interessant å se på hvordan funksjoner som indikatorer, struktur, og informasjonsflyt fungerer i praksis, og hvordan dette legger et grunnlag for Kunnskapsoverføring

«Hvordan bidrar digitale sikkerhetsinformasjonssystemer til resiliens i Lundin Norway?»

Foreløpige forskningsspørsmål;

F1) Hvordan kan perspektiver på resiliens benyttes i digitale sikkerhetsinformasjonssystemer i Lundin Norway?

F2) Hvordan benyttes indikatorer i digitale sikkerhetsinformasjonssystemer i Lundin Norway?

F3) Hvordan systematiseres og distribueres kunnskap fra digitale sikkerhetsinformasjonssystemer?

Synergi
- Informering om forskningsprosjektet og prosjektets formål
Informantens bakgrunn og erfaring
- Hva er din nåværende stilling og hvor lenge har du hatt den?
- Hva inngår i dine arbeidsoppgaver?
- Hvilken utdanning og arbeidserfaring har du?
Begrepsavklaringer

<ul style="list-style-type: none"> - Hva legger du i begrepene resiliens og robusthet innenfor sikkerhetsstyring? - Hva legger du i begrepet sikkerhetsinformasjonssystem? - Hva legger du i indikatorer?
Informantens tilknytning til sikkerhetsinformasjonssystemer
<ul style="list-style-type: none"> - Hvilke systemer benytter Lundin for behandling av sikkerhetsrelevant informasjon? - Hva er formålene til disse systemene? - I hvor stor grad benytter du disse systemene for avviks- og hendelsesrapportering i din hverdag?
Systemenes tilgjengelighet
<ul style="list-style-type: none"> - Hvem kan registrere forhold og hendelser i systemet? - Hvem har tilgang til informasjon i systemene? - Opplever du systemet som oversiktlig og lett å bruke?
Tidsoptimalitet
<ul style="list-style-type: none"> - Hvordan opplever du informasjonsflyten i systemet med hensyn til tid? - Hvilken rolle spiller fargekodene med hensyn til tid?
Kosteffektivitet
<ul style="list-style-type: none"> - Opplever du at det er et reelt behov for systemet, med hensyn til ressursbruken? - Hvis nei, hvilke alternative løsninger kunne en vurdert?
Forståelig og akseptert
<ul style="list-style-type: none"> - Hvordan opplever du det generelle synet på dagens SIS er i organisasjonen? - Opplever du at ansatte i operative og øvrige stillinger aksepterer systemet og ser behovet for det?
Insentivstruktur
<ul style="list-style-type: none"> - Hvordan opplever du at belønninger og sanksjoner påvirker innrapportering av hendelser og forhold? - Hvordan rolle spiller anonymitet i innrapportering av hendelser?
Monitorering og indikatorbruk
<ul style="list-style-type: none"> - Hvordan benyttes informasjon i SIS som indikatorer? - Hvordan kan informasjon i systemene benyttes som indikatorer for sikkerhetstilstander? - Benyttes informasjon fra systemene til å måle trender og sikkerhetsnivå over tid? - Er det mulig å registrere forhold som ikke er knyttet til uønskede hendelser og forhold? - Gir indikatorene mening i seg selv, eller krever de videre analyse? - Finnes det indikatorer i systemene, eller benyttes informasjonen til å danne indikatorer/analyser? - Hvordan verifiseres disse indikatorene? - Hvordan er indikatorene utviklet? - Hvordan revideres og gjennomgås indikatorene? - Finnes det retningslinjer for hvor ofte indikatorene skal gjennomgås eller revideres? - Benyttes det etterslepe eller ledende indikatorer? - Er indikatorene reaktive i form av måling av statistikk og historiske tall? - Finnes det indikatorer som forsøker å predikere fremtiden? - Har indikatorenes validitet blitt etablert? - Er indikatorer utviklet på bakgrunn av effektivitet eller grundighet? - Er indikatorene tilstrekkelig sensitive? Fanger de opp endringer og utviklinger tidlig nok? - Dersom indikatorer indikerer en uakseptabel sikkerhetstilstand, hvordan varsles dette? - Må noen logge inn i systemet og sjekke, eller vil systemet varsle selv dersom en indikator er indikerer en uakseptabel tilstand? - Hvor ofte måles indikatorene, hva sier rutinene? - Finnes det etablerte inspeksjonsrutiner av indikatorene? Er disse prosessene tilegnet nok ressurser? - Kommuniseres data fra indikatorene til riktige personer, og hva brukes den til?

Vedlegg 3

Intervjuguide for opphold 2 av 2

Kort introduksjon om forskningsprosjektet:

Resilience engineering er et nyere fagfelt som forsøker å besvare et økende behov for nye metoder for sikkerhetsstyring, på bakgrunn av sosio-tekniske systemers økende kompleksitet. Resiliens er definert som en organisasjons evne til å operere under forventede og uventede forhold. Innenfor resilience engineering er det flere byggesteiner som må ligge til rette for at en organisasjon skal kunne være resilient. Informasjonsbehandling (monitorering) er en sentral egenskap eller byggestein. Dette forskningsprosjektet har derfor som formål å se hvordan digitale sikkerhetsinformasjonssystemer i et suksessfullt operatørselskap benyttes til kunnskapsoverføring og til hvilken grad systemene og prosessene er i tråd med byggeklossene fra «resilience engineering». Det er herunder interessant å se på hvordan funksjoner som indikatorbruk, struktur, og informasjonsflyt fungerer i praksis, og hvordan dette legger et grunnlag for Kunnskapsoverføring

«Hvordan bidrar digitale sikkerhetsinformasjonssystemer til resiliens i Lundin Norway?»

Foreløpige forskningsspørsmål;

F1) Hvordan benyttes digitale sikkerhetsinformasjonssystemer til monitorering av sikkerhet i Lundin Norway?

F2) Hvordan benyttes digitale sikkerhetsinformasjonssystemer til systematisering av kunnskap i Lundin Norway?

F3) Hvordan benyttes digitale sikkerhetsinformasjonssystemer til distribusjon av kunnskap fra digitale sikkerhetsinformasjonssystemer?

Intervjuguide
Lundins monitoreringsevne i lys av RAG – Evne til å samle inn kunnskap
<ul style="list-style-type: none">- Hvor viktig opplever du kunnskapsoverføring som for HMS-arbeidet?- Hvor tilgjengelig er historisk statistikk i synergi?- I hvilken grad opplever du at Synergi kan benyttes til å monitorere sikkerhetstilstanden i Lundin Norway?

- Hvordan kan statistikk og data fra Synergi brukes som indikatorer for sikkerheten i organisasjonen?
- Hvor valid er i så fall disse indikatorene? Gir de et reelt og gyldig bilde av tilstanden i Lundin?
- Opplever du at synergi som system gir muligheten til å tidlig oppdage negative trender/utviklinger?
- Opplever du at det er forhold som ikke fanges av Synergi?
- Hvordan vil statistikk kunne utløse aksjoner og tiltak?
- Hvordan påvirker tolkningsprosesser av statistikk fra Synergi HMS-arbeidet?
- Hvordan benyttes ledende indikatorer?
- Hvordan benyttes reaktive indikatorer?

Sikkerhetsinformasjonssystemer og struktur – Evne til å behandle og distribuere kunnskap

- Hvordan påvirker tidsaspektet kunnskapsoverføring fra saker og granskinger i synergi?
- I hvilken grad er det mulig å spore læring? Fra kontraktørers granskinger?
- Hvem har tilgang til saker i Synergi?
- Er Synergi etablert og kollektiv akseptert i organisasjonen?
- Opplever dagens utforming av Synergi som effektiv?
- Hvilke saker/forhold utløser LL?
- Hvem er ansvarlig for utarbeidelse av LL?
- Hvem skal få tilsendt LL?
- Kunne dette vært integrert i Synergi?
- Hva anser du som de største utfordringene tilknyttet kunnskapsoverføring de neste årene?

Digitalisering og psykologiske faktorer – systemenes nytte i praksis

- Tas det høyde for misforståelser som kan oppstå som følge av forenklete visualiseringer, farge- og symbolbruk?
- Hvor viktig er det at brukerne av systemer forstår hvilke underliggende antagelser systemet er bygd opp av?
- **Attribusjon;** I hvilken grad tas det høyde for attribusjon med hensyn til inhabilitet i granskinger og behandling av forhold og hendelser?
- **Insentivstruktur;** Hvordan innvirkning har sanksjoner og belønninger med hensyn til innrapporteringen av hendelser og forhold? Finnes det utfordringer knyttet til dette?
- **Filter;** Hvordan påvirker informasjonsflyt og kvalitetssikring innholdet i rapporter og data? Vil ledere og personer med tilknytting til hendelser og forhold kunne endre innholdet for egen vinning?
- Hvordan tror du digitalisering vil påvirke sikkerhetsarbeidet i årene fremover?