Metodikkens betydning for beslutningstaker

En studie med fokus på utviklingen av barrierestyring mot tilsiktede uønskede hendelser

Masteroppgave i risikostyring og sikkerhetsledelse

Vår 2018

Finn Eirik Sørensen

UNIVERSITETET I STAVANGER

MASTERGRADSSTUDIUM I

RISIKOSTYRING OG SIKKERHETSLEDELSE

MASTEROPPGAVE

SEMESTER: Våren 2018

FORFATTER: Finn Eirik Sørensen

VEILEDER: Sissel H. Jore

TITTEL PÅ MASTEROPPGAVE: Metodikkens betydning for beslutningstaker. En studie med fokus på utviklingen av barrierestyring mot tilsiktede uønskede handlinger

---

EMNEORD/STIKKORD: Security, safety, tilsiktede uønskede handlinger, risiko, risikoanalyse, sårbarhetsvurdering, risikostyring, barrierer, barrierestyring, trussel.

SIDETALL: 82

STAVANGER **08 Mai 2018**

DATO/ÅR

Forord

Denne oppgaven representerer slutten på mastergradsutdannelse i Risikostyring og Sikkerhetsledelse ved Universitetet i Stavanger. Det har vært en interessant og lærerik tid som har gitt meg mye ny kunnskap og kompetanse. Men det kjennes godt å kunne sette punktum. Jeg ønsker å takke alle dyktige forelesere og studieadministrasjon for å holde ut med alle mine spørsmål.

Jeg vil også takke min egen arbeidsplass, Statoil og konsernsikring, som har tillatt meg å studere dette emnet som jeg finner så interessant og til tider frustrerende.

Min veileder gjennom denne oppgaven, Sissel H. Jore, tusen takk for støtte og gode råd underveis.

Jeg vil også rette en spesiell takk til min kone, Hilde, for å ha holdt ut med meg gjennom dette studiet og støttet meg hele veien i mål. Nå får du mannen din tilbake.

Oslo, April 2018

Finn Eirik Sørensen

Sammendrag

Ansvaret for security og håndteringen av security risiko i Norge har historisk sett vært forbeholdt politiet eller forsvaret. Men utviklingen i samfunnet, ikke bare i Norge, har endret dette ansvarsforholdet. Vi har gjennom utviklingen fått større mobilitet, vi forflytter oss enklere og raskere fra sted til sted og over landegrenser. Den samme utviklingen har også security og security risiko hatt. Hendelser som terroranslaget i New York i 2001, bombingen av regjeringskvartalet i Oslo i 2011, terrorangrepet mot Charlie Hebdo i Paris i 2015 og gisseltakingen på In Amenas gassanlegget i Algerie i 2013 er bare noen av hendelsene som har ført til et økt fokus på security risiko. Det er ikke lengre et ansvar som er forbeholdt politiet eller forsvaret, det er blitt et allemannseie, et allemannseie som har bidratt til utvikling av forskjellige metodikker for security risikoanalyser. Petroleumssektoren har vært en viktig bidragsyter til sikkerhetsutviklingen og fokuset på security fører naturligvis med seg en utvikling også innenfor security.

Flere av hendelsene over og under den «Arabiske våren» var medvirkende årsaker til at Statoil i 2013 endret metodikken for security risikoanalyser fra kvalitativ metode til en metodikk som i hovedsak er lik metoden funnet i NS 5832. Det er ulike meninger om hvilke metoder og om det er metoder som er mer riktig enn andre. Men basert på egne erfaringer gjorde Statoil endringer i metoden i 2016. Endringene har i hovedsak betydning for sårbarhetsvurderingen og barrierestyringen.

Avhandlingen ser på utviklingen av sårbarhetsvurderingen i perioden 2013 til 2018, betydningen av denne utviklingen og forankringen i selskapets styrende dokumentasjon. For å finne svar på hvordan denne utviklingen har vært er det benyttet en kvalitativ metode og dokumentstudier. Det er analysert 158 scenarioer med tilhørende sårbarhetsanalyser.

Avhandlingens resultater peker på at metodikken i hovedsak har utviklet seg i retning av å bli en reell metodikk for styring av barrierer mot tilsiktede uønskede hendelser enn det tidligere metodikker har vært. Dette gjør den på grunn av den økende informasjon om barrierene, beskrivelser av sammenhengen mellom barrierene og måten de knyttes til scenarioet. Metoden har en forankring i styrende dokumentasjon som gir håndtering av security risiko synlighet i organisasjonen. Metodikken tilrettelegger for beslutningsprosesser hvor «alle» risikoforhold i større grad enn tidligere er beskrevet. Beslutningene blir ikke nødvendigvis enklere, men informasjonsgrunnlaget for beslutning er høyere. Konsekvensene av endringene kan gå ut over den helhetlige sårbarhetsforståelsen og det krever en større bevissthet til viktig

informasjon som tidligere var tilgjengelig i sårbarhetsvurderingen, men som nå er beskrevet under scenarioet.

Figurer og tabeller

Innhold

1 Innledning

16. januar 2013 klokken 05:40 startet væpnede islamister et angrep på gassanlegget In Amenas, Algerie, som varte over fire dager. Angrepet ble ledet av den algeriske islamisten Mokhtar Belmokhtar. Gassanlegget ble drevet som et fellesforetak (joint venture) av the algeriske oljeselskapet Sonatrach, Statoil og BP. Rundt 700 av de neste 800 nasjonale og internasjonale arbeidere ble tatt som gissel i terrorangrepet som varte frem til 19.januar. Algeriske militære styrker brukte to dager på å ta tilbake gassanlegget fra terroristene og terrorhendelsen kostet 40 ansatte fra en rekke land livet (Statoil, 2013).

26.februar beslutter styret i Statoil å granske hendelsen. Den interne granskningsgruppen ble ledet av Torgeir Hagen, tidligere sjef for Etterretningstjenesten. Granskningsgruppen ble gitt mandat til å besvare to hovedspørsmål:

Hva skjedde i In Amenas mellom 16. og 19.januar 2013?

Hvordan kan Statoil lære for å forbedre sikrings- og beredskapshåndteringen?

Resultatet av granskningsgruppens arbeid ble nedfelt i rapporten *«The In Amenas Attack. Report of the investigation into the terrorist attack on In Amenas»* og offentliggjort både via pressekonferanse og på Statoil sin hjemmeside[1].

Ved en hendelse vil det ofte i ettertid være mulig å følge hendelsen tilbake i tid og peke på både årsaker og konsekvens, spesielt når en vet hva som skjedde. I en slik prosess vil det også fort kunne danne seg spørsmål som «hva om?», noe granskningsgruppen også gjorde. De stilte seg spørsmål som «*Hva om barrierene hadde vært sterkere?*», «*Hva om fellesforetaket eller eierne hadde redusert antallet internasjonale før angrepet?*», «*Hva om anlegget ikke hadde blitt stengt ned?*», «*Hva om de sivile vaktene hadde vært bevæpnet?*» og «*Hva om terroristene hadde klart å flytte gislene?*». Granskningsgruppen mener at det ikke er mulig å peke på kun en faktor som årsak og konsekvens, til det er hendelsen for kompleks. De spekulerer heller ikke i alternative scenario eller andre utfall. Men de har «sett» tilbake i tid, både dager, måneder og år forut for hendelsen, for å beskrive i hvilken kontekst beslutninger, ofte vanskelige, har vært tatt. Det er et forsøk på å forklare hva som skjedde[2].

[1] www.statoil.com

[2] The In Amenas Attack. Report of the investigation into the terrorist attack on In Amenas

The investigation team has found no evidence that suggest that Statoil or the In Amenas joint venture were aware of any specific threat to, or had actionable warning of the attack on In Amenas. Nor should companies expect to have so in the future. Therefore, it is important to consider and think through the complications of scenarios where a surprise attack takes place and outer security layers break down[3].

Denne oppgaven handler ikke om In Amenas eller prøver på noen måter å forklare årsakene til terrorhendelser. Oppgaven innleder med terrorhendelsen i In Amenas fordi det er en tilsiktet uønsket hendelse og en hendelse som har hatt betydning for at jeg skriver denne oppgaven. Terrorhendelser har skjedd før, de skjer mens denne oppgaven blir til og vil trolig skje etter at denne oppgaven er ferdig. Innledningen peker i likevel på tema for denne oppgaven og en av granskningsgruppens anbefalinger har vært viktig for formingen av denne oppgaven.

Develop a security risk management system that is dynamic, fit-for-purpose and geared towards action. *It should be an embedded and routine part of the company's regular care business, project planning, and Statoil's decision process for investment projects. A standardized, open and well-defined security risk management methodology will allow both experts and management to have a common understanding of risk, threats and scenarios, and evaluations of these. The objective should be to enable effective and action-oriented discussions, resulting in measures that address the risk at hand.*

[3] *The In Amenas Attack. Report of the investigation into the terrorist attack on In Amenas s.69*

1.2 Motivasjon for valg av oppgave

Innledningen til denne oppgaven er en del av motivasjonen for valg av oppgave. Her vises det til at granskningsgruppen har sett tilbake i tid, dager, måneder og år, for å beskrive i hvilke kontekster beslutninger, ofte vanskelige, har vært tatt. Denne oppgaven omhandler om det grunnlaget vi tar disse ofte vanskelige beslutninger på.

I perioden etter terrorhendelsen i In Amenas ble det gjennomført flere endringer i Statoil for å møte anbefalingene til granskningsgruppen. Jeg er selv ansatt i Statoil og er en del av security organisasjonen. Jeg har derfor både sett og erfart de endringene som Statoil har gått igjennom. Jeg har i den perioden hatt flere roller, både i et forretningsområde, som en del av konsernfunksjonen og leder nå en sektor som er ansvarlig for både å levere security, som en tjeneste, og håndtere security som en risiko. Jeg har i flere av rollene bidratt til de endringene som har vært gjort.

I 2013 endret Statoil metodikken for hvordan security risikoanalyser ble gjennomført. De valgte en standard og gjorde tilpasninger som de mente måtte til for at den skulle passe selskapet. I løpet av en periode på to år ble det høstet erfaringer fra bruken av metoden, som igjen førte til nye endringer i 2016. Endringene i 2016 var i hovedsak basert på egne erfaringer og relatert til sårbarhetsvurderingen, som også er den delen som beslutningene knytter seg til i risikostyringsprosessen. Denne delen av metodikken har blitt videreutviklet også etter 2016.

Jeg ønsker å se nærmere på hvordan beslutningsgrunnlaget for styring av security risiko har endret seg fra 2013 og frem til den metodikken selskapet benytter i dag. Beslutningsgrunnlaget er sårbarhetsvurderingen i metodikken og som ofte blir kalt for barrierestyringen. Det er blant annet på dette grunnlaget beslutningstaker gjør sine vurderinger og valg. Jeg ønsker å se på hva er grunnlaget det tas beslutning på og hvordan har dette utviklet seg? Hvilke konsekvenser eller effekter kan vi se av denne utviklingen? Har denne utviklingen ført til at beslutningene, ikke nødvendigvis blir enklere, men tydeligere?

1.2 Oppgavens problemstilling

For å undersøke om de metodiske endringene har påvirket grunnlaget for de beslutningene som tas gjennom security risikostyringsprosessen har jeg valgt følgende problemstilling for oppgaven:

Hvordan har metoden for styring av barrierer mot tilsiktede uønskede hendelser utviklet seg i selskapet og hvordan er den forankret i styrende dokumentasjon?

For å besvare denne problemstillingen har jeg utledet følgende forskningsspørsmål:

- Hvordan har metoden for styring av barrierer mot tilsiktede uønskede hendelser utviklet seg siden 2013?

Med dette forskningsspørsmålet vil jeg søke å dokumentere utviklingen av sårbarhetsvurderingen og hva som metodisk lå til grunne for beslutninger om styring av security risiko gjennom to tidsperioder. Jeg vil videre søke å finne svar på om det er dekning for den metodiske utviklingen gjennom det teoretiske grunnlaget i oppgaven.

- Hvordan er metodikken forankret og security definert i styrende dokumentasjon?

Med dette forskningsspørsmålet vil jeg søke å finne frem til hvordan både metodikken og definisjonene som benyttes i dag er forankret i styrende dokumentasjon, sett oppimot det teoretiske grunnlaget.

- Hva er konsekvensen av denne utviklingen?

Med dette forskningsspørsmålet søker jeg å finne svar på om de metodiske endringene har endret beslutningsgrunnlaget i security risikostyringsprosessen. Jeg vil også søke å finne svar på om dette har betydning for styring av barrierer mot tilsiktede uønskede handlinger.

1.3 Relevant forskning

Denne oppgaven retter seg mot beslutningsgrunnlaget for styring av barrierer mot tilsiktede uønskede hendelser. Petroleumsvirksomheten i Norge og internasjonalt har vært en viktig bidragsyter til utviklingen av barrierestyring mot safety hendelser, noe det søkene på nett og UiS database etter relevant forskning har vist. Typiske søkeord som har vært benyttet er security, security management, security barrier reseach eller management. I stor grad er det safety relaterte treff, veiledere til standarder for security risikoanalyse eller konsulentselskap som tilbyr tjenester. Men noen av de faglige treffene som ikke inngår i oppgavens teorigrunnlag er:

- The development of an audit technique to assess the quality of safety barrier management (Guldmundur, F., Hale, A., Goossens, L. Betten, J., Duijm, N. J. 2005)
- Mindfullness og teknisk barrieresystem – risikohåndtering i bore- og brønnoperasjoner (M. Nagell, UiS, 2013)
- Den menneskelige faktors betydning i barrierestyring (B. Enehaug, UiS, 2015)
- Security styring i petroleumssektoren (Stålesen, J. S., UiS, 2011)

1.4 Avgrensninger

I min masteroppgave vil jeg fokusere på hvordan sårbarhetsvurderingen i security risikoanalyser mot tilsiktede uønskede hendelser har utviklet seg over tidsperiode 2013 til 2018 i Statoil. I masteroppgaven ser jeg ikke på trusselnivå, konsekvenser eller hva som er risikonivået i Statoil. Oppgaven er derfor heller ikke en studie som sier noe om faktisk risikonivå eller svarer på om security risiko er lavere eller høyere nå enn før. Jeg har videre avgrenser oppgaven og spesielt empirien til kun å omhandle security og vil i teorikapittelet redegjøre for hva som skiller safety og security.

Andre avgrensning er mot selskapets interne ressurser, bemanning, kompetanse og kultur hos dem som utfører eller har utført security risikoanalysene. Dokumentasjon om kunnskap og kompetanse hos dem som faktisk utfører risikoanalysen sier noe om styrken i analysen og er

derfor viktig. Statoil har allerede dokumenterte kompetansekrav[4] til security rådgivere. Min oppfatning er også at dette ville gitt oppgaven mer bredde og gått på bekostning av dybden.

Tredje avgrensing er gjort for å øke åpenheten. Jeg ønsker at denne studien i størst mulig grad skal kunne benyttes av andre og kanskje til videre forskning. For å unngå at oppgaven klausuleres har jeg valgt å ikke identifisere hvilke lokasjoner analysene er gjennomført for, type lokasjon eller region materialet stammer fra. Selv om det er mange i Statoil som håndterer security risiko så er informasjonen gradert begrenset eller konfidensielt.

Fjerde avgrensning har sammenheng med andre avgrensning. Jeg har valgt å kun forholde meg til dokumentene, de skrevne analysene, og ikke personene som har skrevet dem. Ved å kun forholde meg til de skrevne analysene vil andre kunne gjennomføre nettopp samme studie i fremtiden, noe som øker etterprøvbarheten av forskningen. I tillegg vil det være det dokumenterte, de godkjente analysene, som vil være gjenstand for etterprøving ved tilsyn eller en granskning, ikke hva security rådgiveren mente med det denne skrev.

Den siste begrensningen er gjort mot bruken av sannsynlighet (usikkerhet) i security risikoanalyser. Diskusjon rundt bruk av sannsynlighet i security risikovurderinger er for omfattende til å inkludere i denne oppgaven og vil derfor ikke bli inkludert. I tillegg har Egeli (2004) omhandlet dette team i egen masteroppgave, hvor også metodikken Statoil benyttet i 2013 var en del av empirigrunnlaget.

1.5 Oppgavens oppbygging

Kapittel 1 tar for seg innledning, motivasjon for valg av oppgave, formål, relevant forskning, avgrensning og et kort underkapittel om kontekst.

Kapittel 2 gir en kort kontekstbeskrivelse av Petroleumstilsynet

Kapittel 3 beskriver det teoretiske grunnlaget for studiet

Kapittel 4 beskriver de metodiske valgene for undersøkelsesopplegg og vurdering av validitet og reliabilitet

Kapittel 5 presenterer resultatene av datainnhentingen

[4] Insight (Statoil intranett)

Kapittel 6 her drøftes funnene oppimot teori

Kapittel 7 beskriver konklusjon av studiet og anbefaling om videre forskning

2 Kontekst

Petroleumstilsynet (Ptil) har en viktig rolle oppimot petroleumssektoren og som en del av empiri i dette studiet vil jeg benytte Barrierenotatet (Ptil, 2017[5]). Det er derfor hensiktsmessig å gi en kort redegjørelse for Ptil og hvilke lover og regler Olje- og gassaktiviteten i Norge er underlagt.

Petroleumstilsynet er et selvstendig, statlig tilsynsorgan med myndighetsansvar for sikkerhet, beredskap og arbeidsmiljø i petroleumssektoren. De var frem til 1. januar 2004 underlagt Oljedirektoratet. Ptil er underlagt Arbeidsdepartementet og skal føre tilsyn og påse at selskaper i sektoren følger de lover og forskrifter som er fastsatt. Myndighetsansvaret har de gjennom alle faser i sektoren, fra planleggingsprosessen via leteboring, utbygging og drift, til avslutning og fjerning av prosjekt[6]. De viktigste lovene og regelverket:

- Petroleumsloven, hjemler rammene for og de overordnede kravene til sikkerhet I norsk petroleumsvirksomhet.
- Arbeidsmiljøloven som kommer til anvendelse på petroleumsvirksomheten, hjemler de overordnede krav til arbeidsmiljø.

Rammeforskriften[7] fastlegger de grunnleggende sikkerhetskravene til organisering og utførelse av virksomheten.

I tillegg er det gitt mer spesifikke regelverkskrav gjennom *Styringsforskriften* (ibid), at det skal etableres barrierer og hva de skal oppnå. Det er viktig å bemerke at Barrierenotat (Ptil, 2017) verken innfører nye krav eller inngår som en del av petroleumsregelverket, men skal tydeliggjøre hensikten med regelverkskravene.

[5] Prinsipper for barrierestyring i petroleumsvirksomheten
[6] WWW.ptil.no
[7] WWW.ptil.no

3 Teori

3.1 Safety og Security

Både Albrechtsen (2003) og Jore (2016) viser til Securitys manglende akademiske grunnlag. Under den kalde krigen (Jore, 2016) var håndteringen av security risiko ansvaret til politiet eller forsvaret, underforstått at det da heller ikke var utsatt for offentlig eller akademisk granskning eller vurdering. Dette har endret seg og behovet for å forstå begrepene er tydeligere.

I det norske språket har vi ikke ekvivalenter til begrepene safety og security eller ord som enkelt beskriver dem. Safety og security oversettes begge til sikkerhet på norsk. Jore (2016) viser til at håndtering av security risiko ikke lengre kun er en stats ansvar, men også private og offentlige organisasjoner. Det har derfor vokst frem et behov for å skille mellom safety og security i det norske språk. En mer vanlig definisjon er at security defineres som beskyttelse mot tilsiktede uønskede hendelser, mens safety defineres som beskyttelse mot utilsiktede hendelser. Handlingen bak tilsiktede uønskede hendelser er ofte planlagte og de er utført med intensjon slik som kriminalitet, terrorisme og sabotasje. Utilsiktede hendelser ansees som uhell hvor en eller flere personer kan være involvert og som sammen med andre forhold fører til en uønsket hendelse (Albrechtsen, 2003).

Definisjonene over synes enkle og klare, security handler om tilsiktede handlinger, mens safety handler om uhell. Men det finnes flere forskjellige definisjoner på både safety og security (Jore, 2016) og en safety hendelse kan oppstå på grunnlag av en tilsiktet handling (Reason, 1997). I tillegg viser Piètre-Cambacèdès, L. & Chaudet, C. (2010) at betydningen av begrepene safety og security avhenger både av i hvilken sammenheng de brukes og det miljøet de anvendes.

3.1.1 Safety

I enkel forstand betyr safety beskyttelse mot ulykker. De lengste tradisjonene innen safety forskning finner vi i høy-risiko industrier slik som atomkraftverk, shipping, offshore aktivitet innen olje og gass produksjon og transport. Årsaken til en hendelse kan være både teknisk, menneskelig eller organisatorisk. De menneskelige handlingene kan være brudd på lover,

regler og prosedyrer, men de er sjelden eller aldri ondsinnet. Det handler om å beskytte mennesker, miljø, omdømme og verdier mot farer som utgjør en risiko (Albrechtsen, 2003).

Fra et organisatorisk perspektiv er safety risiko veldig forskjellig fra security risiko. Safety risiko kommer av organisasjonens egen aktivitet og risikonivået bestemmes av organisasjonen selv og styres av hva som er tolerabelt for å oppnå økonomisk gevinst i produksjon. Det er organisasjonen selv som er både problemet og løsningen. Safety kan derfor sees på som et relativt teknisk og kontrollerbart problem som organisasjonen selv primærkunnskapen til å håndtere (Jore, 2016).

3.1.2 Security

Security relateres til de utfordringene hvor mennesker handler bevisst og har sin opprinnelse i beskyttelse mot tyveri. I dag dekker feltet alt mellom beskyttelse av mennesker til nasjon, inkludert økonomisk sikkerhet, informasjonssikkerhet, verdier og spionasje. Security handler om beskyttelse mot personer eller gruppers bevisste handlinger for å skaffe seg en gevinst eller påføre mennesker og viktige samfunnsverdier skade. (Albrechtsen, 2003).

Security trusler kan deles inn i eksterne trusler og interne trusler (insider). De eksterne truslene (cyberangrep eller terrorhandling) indikerer en bevisst handling. Eksterne trusler gjør trusselbildet mer kompleks, usikkert og umulig å kontrollere. Det gjør det svært vanskelig å forutsi hvor, når og hvordan en bevisst handling vil skje. I ettertid vil det også kunne være vanskelig å finne de ansvarlige da de bevisst kan unnlate å legge igjen spor. (Albrechtsen, 2003).

Albrechtsen (2003) peker på at årsaken til interne trusler kan være både bevisste og ubevisste handlinger. Dette kompliseres ytterligere av Politiets Sikkerhetstjenestes (PST) åpne trusselvurdering[8] (PST, 2018) hvor de ser en kombinasjon, eksterne trusler som benytter organisasjonens ansatte (innsider), både frivillig og ufrivillig. Denne kompleksiteten gir en enda større usikkerhetsdimensjon. I tillegg til å peke på at security er de truslene som en organisasjon blir eksponert for peker Jore (2016) også på at truslene ikke nødvendigvis er knyttet til verken organisasjonen eller produksjonen. Hun eksemplifiserer dette med terrorisme, hvor hensikten kan være både politisk og økonomisk, hvilket gjør trusselen

[8] PST.no

mindre kontrollerbar. Dersom hensikten er informasjonstyveri er det ikke sikkert at organisasjonen vet om hendelsen.

3.1.3 Likheter mellom safety og security

Albrechtsen (2003) påpeker i sin begrepsavklaring av safety og security at den grunnleggende betydningen er lik, da begrepene tar utgangspunkt i et ønske om beskyttelse mot farer og trusler og å skape trygghet. I safety begrepet vektlegger en *å være beskyttet*, mens i security begrepet vektlegger en *å være fri for fare*. Forskjellen er ikke nødvendigvis enkel å se da det å være beskyttet gir en følelse av å være fri for fare og det å være fri for fare kan bety at en er beskyttet. Derav er den grunnleggende ideen lik for safety og security.

Jore & Egeli (2015) viser til at forskjellen mellom safety og security ofte reflekteres i bruk av forskjellige metodikker, men Piètre-Cambacèdès, L. & Bouissou, M. (2013) peker på at både verktøy og perspektiver innen safety eller security utvikles innen et felt og benyttes i begge. Forsvar i dybden, som ble utviklet og benyttet i militært forsvar, ble deretter benyttet innen atomindustrien og nå også innen IT security.

Piètre-Cambacèdès, L. & Chaudet, C. (2010) viser til at risikokonseptet er utstrakt brukt innen begge feltene. Risikoanalyser, innen safety og security, er basert på liknende faser som involverer trussel analyse (eller fare avhengig av konteksten), sårbarheter (eller svakheter), potensielle konsekvenser og sannsynlighet for at en hendelse skal inntreffe og rangering av risikoer.

3.1.4 Forskjeller på safety og security

I følge Piètre-Cambacèdès, L. & Chaudet, C. (2010) er det to sentrale forskjeller på safety og security, hvor den første knyttes til intensjonen og den andre knyttes til forholdet mellom systemet og omgivelsene. For security knyttes det en intensjon om å skade, mens safety sees i sammenheng med uønskede hendelser som er tilfeldige og ikke intenderte. Den andre sentrale forskjellen er knyttet til forholdet mellom system og omgivelser, hvor trusselen kommer fra og hvem eller hva den er rettet mot. Det er omgivelsene som skaper security hendelsene, som igjen påvirker systemet, Mens for safety er det systemet som skaper hendelsene, som igjen kan påvirke omgivelsene.

Kriaa et al. (2015) viser til at nettopp trusselens opprinnelse gjør risikovurderingen av safety og security risiko radikalt forskjellige. Security truslene er vanligvis ikke kjent for analytikeren og dekker et svært bredt spekter av mulige scenarier. I analyse av safety risiko vil truslenes egenskaper være mer tilgjengelig for analytikeren og antallet scenarioer som skal hensyn tas vil kunne reduseres, men tilstrekkelig til å bli vurdert som signifikant.

Mens safety truslene vil være relativt stabile over tid og analyse fra tidligere uhell mer pålitelig er security truslene mer uforutsigbare. De er avhengig av flere faktorer, slik som angriperprofil, ferdigheter, motivasjon osv. Dette gjør det vanskeligere i security analyser å vurdere og kvantifisere mulige scenarioer, enn i safety analyser (Kriaa et al. 2015).

Men hvor Piètre-Cambacèdès, L. & Chaudet, C. (2010) peker på intensjon som en sentral forskjell mellom safety og security, trekker Reason (1997) frem en mulig likhet. Videre i Piètre-Cambacèdès, L. & Bouissou, M. (2013) viser de til at en security trussel kan være intelligent, lære av tidligere hendelser, utnytte sårbarheter og gjøre mottiltak både mot aktive og passive barrierer for å oppnå sin intensjon, å skade, noe safety trusler ikke gjør. En security trussel har med andre ord en vilje eller et ønske om å omgå barrierene for å påføre skade, som er intensjonen.

Reason (1997) hevder at årsaken (på individnivå) til organisatoriske ulykker i hovedsak skyldes to årsaker, handlinger feiler i å gå som planlagt og planlagte handlinger oppnår ikke ønsket effekt. Men han legger til en tredje kategori, brudd, når mennesker har en intensjon om å ikke følge safety prosedyrer. Han definerer disse som eksepsjonelle brudd, rutinebrudd og uforsvarlige brudd. Eksepsjonelle brudd er enkelthendelser som skjer i et bestemt sett av omstendigheter, mens rutinebrudd er sedvane og blir en etablert del av en persons oppførsel. Han mener mennesker tar snarveier og unngår safety prosedyrer fordi de oppfattes som en byrde. Uforsvarlige brudd er når en person med intensjon bryter regler og prosedyrer, men intensjon om å skade andre mangler. Reason (1997) peker med andre ord på at i safety hendelser, slik som i security hendelser over, vil det være personer som har en intensjon om å omgå barrierene eller prosedyrene, men intensjon om å påføre skade finnes bare i security hendelsene.

Albrechtsen (2003) påpeker i sin begrepsavklaring at grunntanken bak industriell safety og security er den samme, begge beskytter verdier fra farer og trusler for å skape sikre og trygge forhold. Safety betyr at en beskytter seg på en slik måte at en er utenfor fare, mens security innebærer beskyttelse mot kriminell aktivitet slik at en oppnår trygghetsfølelse.

	Security	Safety
Cause	An incident is most often a result of one person or a group's will	An incident is most often a result of human behavior in combination with the environment
Cause	Often planned actions	Often unplanned
Cause	Criminal acts	Criminal acts (Working Environment Act)
Cause	Mainly malicious acts	Seldom, if ever, malicious
Cause	Mainly deliberate acts with a wish of a wanted output/consequence of the act.	Mainly deliberate acts without a wish of a wanted output and accidental incidents
Threats/Hazards	External and internal human threats	Internal human threats
Threats/Hazards	Threats are not always observable, tangible and proximate	Hazards are observable, tangible and proximate
Loss	Loss is mainly related to physical assets and information	Loss is related to human injuries/death and reliability of industrial assets
Surrounding	Reflects the state of society through its structures, economical situation, law-abidingness and moral	Includes physical and environmental conditions – not only humans and society
Relevance	Relevant for a wide range of Companies	More relevant for the industry and transporting sector
Uncertainty	High degree of *uncertainty* and low degree of knowledge about threats within	

Tabell 1: Viser forskjellene mellom safety og security (Albrechtsen, 2003)

Basert på denne redegjørelsen legger jeg til grunne at security hendelser skjer på grunnlag av en eller flere personers vilje. Det er ofte en planlagt og skadelig handling som kan betegnes som en kriminell handling. I tillegg, og kanskje den mest sentrale faktoren, er den planlagte intensjonen bak handlingen.

Videre, at safety hendelser som regel er tilfeldige ulykker på grunn av uaktsom adferd. De er som regel ikke planlagte, men kan være brudd på regler og prosedyrer. I safety hendelser er det ikke en planlagt intensjon om skade.

3.2 Risikostyring – design eller barrierer

I følge Ptil og Styringsforskriften[9] skal risiko reduseres ved bruk av tekniske, operasjonelle og organisatoriske løsninger som reduserer sannsynligheten for at det skal oppstå skade, feil eller fare- og ulykkessituasjoner. Det skal i tillegg etableres barrierer. Det må bety at når en for eksempel velger en type mekanisk enhet fremfor en annen mekanisk enhet med tilsvarende funksjon, på grunnlag av bedre kvalitet, styrer en risiko gjennom robuste og sikre løsninger, ikke barrierer. Barrierer er noe som kommer i tillegg til den risikoreduserende løsningen en har valg. De skal identifisere tilstander som kan føre til feil, fare- og ulykkessituasjoner, de skal redusere muligheten for at feil, fare- og ulykkessituasjoner oppstår og utvikler seg, samt begrense mulige skader og ulemper.

Det er flere eksempler på at selv om en velger robuste og sikre løsninger og har prosedyrer for operasjoner vil det likevel medføre risiko. Et eldre eksempel er Piper Alfa ulykken i 1988, Olsen m.fl. (2008). Det var flere uheldige hendelser som førte til at konsekvensen ble så stor, men løsningen som på den tiden ble ansett som robust sviktet. Dette førte til store endringer i regler og prosedyrer for petroleumsvirksomheten i Storbritannia. Til tross for endringene, utvikling og fokus i både norsk og internasjonal petroleumsvirksomhet har vi også nyere eksempler. Det finnes eksempler fra norsk sokkel i nærmere tid. Gullfaks C hadde en hendelse som kunne utviklet seg til en ulykke, men som ble avverget[10].

Selv med bruk av robuste og sikre løsninger erfarer vi at ting kan gå galt. Barrierer er svært viktige styringsvariabler i risikostyringen (Aven m.fl. 2004). Det er *"tiltak eller funksjon som er planlagt for å bryte et spesifikt uønsket hendelsesforløp"* (Aven m.fl. 2008).

Reason (1997) viser til at menneskelige feilhandlinger svært ofte er årsaken til uhell. Ved å implementere barrierer økes toleransen for funksjonsfeil eller feilhandlinger (uønsket hendelsesforløp) og kan avbrytes. Reason (1997) konkluderer med at en kombinasjon av tekniske, organisatoriske og operasjonelle barrierer vil gi den beste samlede effekten. Norske

[9] WWW.ptil.no
[10] http://www.ptil.no/bronnsikkerhet/nare-pa-for-gullfaks-c-article7606-825.html

myndigheter har også gjennom Stortingsmelding 12 (2005-2006) «Helse, miljø og sikkerhet i petroleumsvirksomheten» gitt uttrykk for annerkjennelsen av samspillet mellom tekniske, menneskelige og organisatoriske faktorer. Med utgangspunkt i redegjørelsen over legger jeg til grunne at barrierer er tekniske, operasjonelle eller organisatoriske tiltak som, i tillegg til den valgte løsningen, introduseres for å ytterligere styre risiko.

3.3 Hvorfor skjer ulykker?

I følge Aven (2007) handler risikostyring om først å skaffe seg innsikt i risikoforhold for deretter å kunne styre risikoen med de rette tiltakene. En må med andre ord kjenne årsaken til at uønskede situasjoner oppstår før en kan sette inn tiltak. Jore (2016), Albrechtsen (2003) og Schiefloe (2011) peker på manglende forskning og akademisk forankring av security som fagfelt. De peker på forskjellige årsaker, men Schiefloe (2011) mener likevel at kunnskapen om sikkerhet i industriell og annen virksomhet gir oss kunnskapsmessig grunnlag og kan anvendes i forhold til intenderte (tilsiktede uønskede handlinger – security) og ikke-intenderte trusler og hendelser (ulykker – safety). Jeg vil derfor først redegjøre for relevante teoretiske perspektiver for hvorfor uønskede situasjoner oppstår før jeg omhandler barrierer og styring av risiko.

3.3.1 Ulykker må forventes – Normal Accident Theory

Mens Petroleumstilsynet peker på robuste og sikre løsninger for å unngå ulykker viser Perrow (1999) til Normal Accident teorien og hevder at systemulykker før eller siden vil oppstå i komplekse systemer som består av ulike subsystemer, enheter og deler. Han fokuserer på egenskapene ved systemene, ikke den som behandler dem, og kombinasjonen av kompleksitet, gjensidig avhengighet og uforutsette påvirkninger i komplekse systemer skaper systemulykker.

Del er den minste enheten i systemet, for eksempel en pakning i en ventil. Enhet er en samling av deler, for eksempel en motor. Subsystem er en samling enheter, for eksempel et pumpesystem med detektor, motor, slanger osv. Systemet er det totale systemet som pumpesystemet inngår som en del i, for eksempel en gassinstallasjon (Perrow, 1999).

Systemer kan ha komplekse eller lineære interaksjoner og de kan ha tette eller løse koblinger. Komplekse interaksjoner er når komponentene som utgjør et system kan kobles sammen på forskjellige måter og rekkefølger. Koblingene kan være tette eller løse. Lineære interaksjoner er ofte enklere ved at prosessene er synlige og forståelig, men kan likevel ha tette eller løse koblinger. Systemer med komplekse interaksjoner har ifølge Perrow (1999) større sannsynlighet for multiple funksjonsfeil og en designer inn mer redundans som igjen skaper mer kompleksitet. I systemer med tette koblinger, uavhengig om det er komplekse eller lineære interaksjoner, vil en feil umiddelbart forplante seg og påvirke neste kobling.

I komplekse systemer vil mennesker kun ha begrenset forståelse av helheten i systemet og vil derfor heller ikke kunne kontrollere det fullt ut. Selv om det er designet inn barrierer så vil ikke disse fange opp alle ukjente sideeffekter i komplekse system. Den utløsende årsaken kan være forskjellig; feilhandling, uventet ytre påvirkning eller teknisk svikt, men ulykker i komplekse og tett koblet system må en regne med. Det vil da kunne oppstå ikke-forventede koblinger av flere feil, altså ukjente sideeffekter som kan fører til forsterkede viderekoblinger (Perrow, 1999). Han peker videre på at systemer med løse koblinger gir mer fleksibilitet og gjør systemet robust mot uforutsette hendelser.

3.3.2 Menneskeskapte ulykker

Begrepet *menneskeskapte katastrofer* (man-made disasters) og modellen for hvordan menneskeskapte katastrofer utvikles ble introdusert av Turner (1978) og Turner & Pidgeon (1997). Sentralt i dette begrepet står informasjonsflyt, menneskers kulturelle og sosiale samhandling og normer.

Modellen (tre første av seks faser) beskriver hvordan og hvorfor latente feil kan utvikle seg til en katastrofe. Sentralt i årsakskjeden, som muliggjør utviklingen, er en kultur preget av feiltolkninger av signaler, sosial samhandling, misforståelser og informasjonssvikt og utviklingen av uformelle normer og væremåter som kan stride med formelle prosedyrer.

Den *antatte normalsituasjon* (første fase) er baser på eksisterende kunnskap om verden, system og farer eller trusler. På bakgrunn av denne oppfattelsen besluttes regler, prosedyrer og instrukser for hvordan en skal unngå ulykker eller katastrofer. Uheldig konsekvenser, som følge av brudd (*violations*) på regler og prosedyrer i denne fasen fører ikke nødvendigvis til en kulturendring, snarere en bekreftelse på behovet for de gjeldende regler og prosedyrer.

Inkubasjonsstadiet (andre fase) er tidsrommet hvor informasjonssvikt og feiltolkninger utviklers seg. En kjede av avvikende hendelser, fra det som ble vurdert i første fase til å være gjeldende virkelighetsoppfattelse, får utvikle seg og akkumuleres uten at det oppdages. Men i den grad hendelsene blir oppdaget blir de gjerne misforstått og håndtert ut i fra hvordan verden, system og farer eller trusler ble definert i første fase. Dette kan igjen føre til ytterligere misforståelse og at de dypere eller latente problemene ikke oppdages. Inkubasjonsstadiet kan strekke seg over lengre perioder og år.

Den *utløsende hendelsen* (tredje fase). Hendelsen fremstår da gjerne som uventet fordi en ikke vet når eller hvor hendelsen vil inntreffe eller fordi det er en hendelse som ikke har skjedd før. Turner & Pidgeon (1997) påpeker at informasjon er tilgjengelig i organisasjon, men at den ofte er oversett eller misforstått. Turner (1978) mener at denne type ulykker, som utvikler seg gjennom en kjede av hendelser, potensielt kunne vært forhindret. Men informasjon og signaler fra latente feil og hendelser, i gråsonen av vår definisjon og oppfattelse av hvordan denne type hendelser utvikler seg, feiltolkes og dermed muliggjøres.

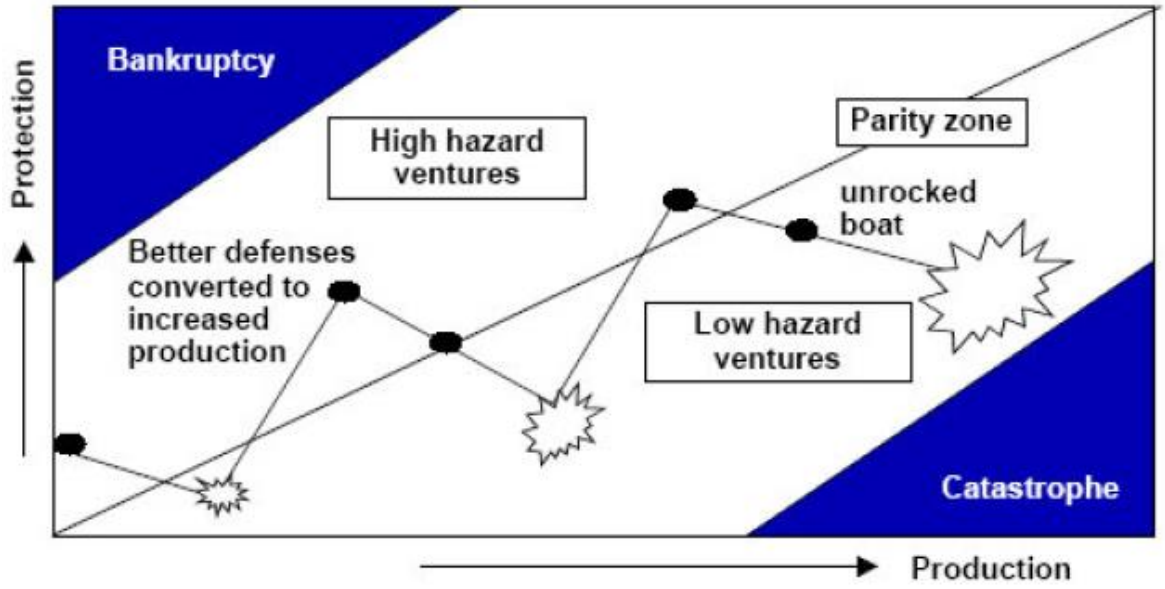
Turner (1978) bruker i tillegg begrepene «failure of foresight» og «The decoy problem». Det første knytter han til inkubasjonsstadiet, når mennesket eller organisasjon ikke er i stand til å forutsi de avvik som akkumuleres i inkubasjonsstadiet. Vår oppfattelse med virkeligheten stemmer med andre ord ikke. Men i den grad vi oppfatter problemer, misforstått eller ikke, tar dette gjerne fokuset vekk fra de virkelige og underliggende feil som faktisk kan lede til en større ulykke, noe han kaller «The decoy problem».

3.3.3 Organisatoriske ulykker og menneskelige feilhandlinger

I følge Aven (2007) må en ha innsikt i risikoforhold for å kunne styre risikoen. Formålet med risikostyringen er «å sikre den riktige balansen mellom det å utvikle og skape verdier, og det å unngå ulykker, skader og tap» (Aven, 2007, s. 5). Reason (1997) viser til at nettopp denne balansen kan være vanskelig da en må balansere mellom produksjon og beskyttelse, to områder, hvor det ene (produksjon) gjerne er mer forstått enn det andre. Produksjon er konkret, direkte og skaper ressurser, mens beskyttelse er mer indirekte og fravær av hendelse er kun en indikasjon på god beskyttelse. I en organisasjon er sjelden eller aldri disse likestilte og det oppstår konflikt i hva som skal prioriteres.

Reason (1997) visualiserer denne problemstillingen med figuren «The unrocked boat» (figur 1) som viser livssyklusen til en hypotetisk organisasjon. I utgangspunktet er det en fornuftig balansering mellom produksjon og beskyttelse. Men etter hvert som kravet om effektivitet treffer organisasjon, på grunn av ny teknologi eller konkurranse, tas det snarveier og safety-marginene minimeres helt til det skjer en mindre hendelse. Slike mindre hendelser fører til en forbedring av beskyttelsen, men som igjen minimeres på grunn av en hendelsesfri periode, nye krav om effektivisering, og til slutt inntreffer det en katastrofal hendelse.

Forbedringer av beskyttelsen er ofte introdusert rett etter en hendelse, nettopp for å sikre at slike hendelser ikke skjer igjen. Men ofte vil ledelsen og produksjonslinjen, over tid, adoptere slike forbedringer av beskyttelsen inn i grunnlaget og argumentasjon for økt og raskere produksjon som igjen fører til mindre marginer og nye hendelser (Reason, 1997). Han peker videre på tidsaspektet, uten hendelser, som en viktig faktor. Produksjon og effektivitet økes på bekostning av beskyttelse og safety-marginene i perioder med fravær av hendelser. En «glemmer» det en ikke erfarer ofte og investeringer i effektiv beskyttelse og vedlikehold reduseres, som igjen reduserer integriteten i eksisterende beskyttelse.



Figur 1. The unrocked boat, Reason (1997)

I sin beskrivelse av årsaker til organisatoriske ulykker skiller Reason (1997) mellom aktive feil og latente forhold. Det er mennesker som designer og konstruerer, produserer, vedlikeholder og opererer komplekse systemer. Det bør derfor ikke være noe overraskelse at

mennesker er involvert i alle organisatoriske ulykker. Men, han mener det likevel er viktig å skulle mellom aktive feil og latente forhold. Aktive feil er de handlinger vi mennesker gjør som gir en umiddelbar uønsket effekt eller hendelse. De latente forholdene er systemfeil, som enkeltindividet ikke kontrollerer, slik som organisatoriske faktorer, design- og produksjonsfeil eller forhold på arbeidsplassen.

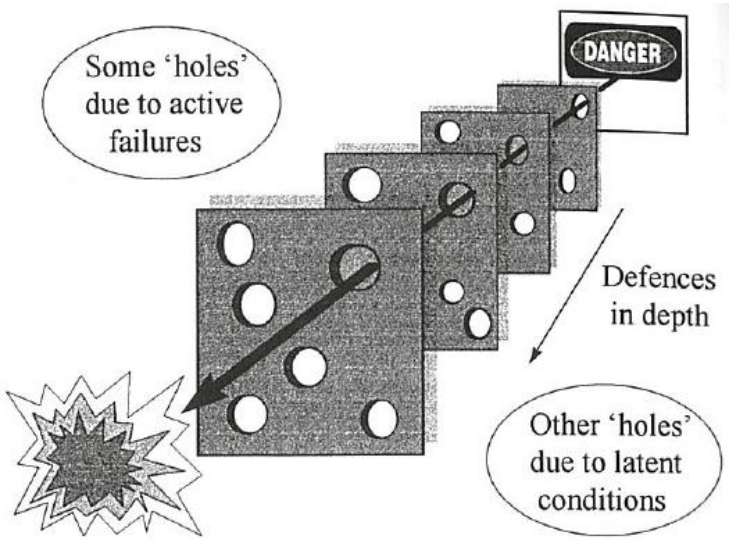
Aktive feil skjer i den skarpe enden av en organisasjon og kan deles inn i tre kategorier. Den første kategorien aktive feilen er slurv eller glipp og derav gjennomføres ikke handlingen slik det var planlagt at den skulle gjennomføres. Den andre kategorien aktive feilen er når en tror at en handler riktig, men handler feil på grunn av manglende kunnskap, forståelse eller kompetanse. Den siste kategorien aktive feilen er når en bevisst bryter prosedyrer, instrukser eller regler. Reason (1997) definerer aktive feil som planlagte handlinger som feiler i å oppnå den ønskede effekten, uten innblanding av uforutsette hendelser.

De latente forholdene er systemfeil, knyttet til det øvre sjiktet i en organisasjon, relatert til produksjon, kontrakter og til regulatorisk og statlig byrå (Reason, 1997). Latente forhold kan være designfeil, manglende kvalitet i tilsyn, manglende trening og opplæring eller ubrukelige prosedyrer. En viktig forskjell mellom aktive feil og latente betingelser blir derfor tidsaspektet. Aktive feil vil føre til en umiddelbar hendelse, mens latente betingelser kan være tilstede over lengre tidsperioder uten at de oppdages. Reason (1997) deler de organisatoriske faktorene inn i følgende:

- **Safety spesifikke faktorer**: Hendelses- og ulykkesrapportering, styrende safety dokumentasjon og beredskapsressurser og prosedyrer.
- **Ledelsesfaktorer**: Endringsledelse, ledelse og administrasjon, kommunikasjon, ansettelse og innplassering i organisasjon, innkjøpskontroll og prioriteringer mellom produksjon og beskyttelse.
- **Tekniske faktorer**: Vedlikeholdsstyring, grad av automatisering, menneske og system grensesnitt, tekniske kontroller, design og maskinvare.
- **Prosessuelle faktorer**: Standarder, regler, instrukser, administrativ kontroll og operasjonelle prosedyrer.
- **Trening**: Formell og uformell metode, treningsressurser, kunnskap og kompetanse oppimot krav.

Reason (1997) visualiserer sammenhengen mellom aktive feil og latente betingelser med «Sveitserostmodellen» (figur 2). Ostelagene er forsvaret og barrierene, som kan være

organisatoriske, operasjonelle og tekniske. Lagene i forsvaret kan sees på som dynamiske og i konstant bevegelse. Hullene i lagene, skapt av de latente betingelsene, vil derfor hele tiden endre posisjon. Det er når hullene i forsvaret synkroniseres, ikke nødvendigvis i tid, at de latente betingelser blir de bakenforliggende årsakene som muliggjør aktive feil og ulykker.



Figur 2: Swiss cheese model (Reason, 1997)

3.4 Kan ulykker unngås?

På lik linje med at det er forskjellige teoretiske perspektiver for hvorfor ulykker oppstår og hvorvidt de kan unngås, er det forskjellige teorier, perspektiver og beskrivelse av hvordan en via organisasjonsdesign, overlappende tiltak og gjennom beskrivelse og utvelgelse av de riktige barrierene kan redusere risiko. Jeg vil derfor redegjøre for noen jeg mener er relevant for denne oppgaven. Flere vil er knyttet til teoriene over, men ikke nødvendigvis alle.

3.4.1 Ulykker må forventes – Normal Accident Theory

Den organisatoriske barrieretenkningen for kontroll av systemet og beslutningsmodell ved hendelser avhenger i hvordan systemet er sammensatt. I systemer (komplekse interaksjoner) med løse koblinger, hvor en feil ikke umiddelbart påvirker neste komponent, vil det kunne være rom for å håndtere en feil før den utvikler seg. I slike tilfeller bør kontroll og beslutningsmodell være desentralisert. Det gir den lokale operatøren mulighet og myndighet til å undersøke og håndtere hendelsen (Perrow, 1999).

Den sentraliserte kontroll og beslutningsmodellen mener Perrow (1999) passer best i tett koblede systemer og i lineære interaksjoner, da feil oppstår i forventede rekkefølger og i rask rekkefølge. Operatøren vil ha liten tid til å vurdere situasjon og håndteringen må derfor være forhåndsplanlagt og sentralisert styrt (Perrow, 1999).

Perrow (1999) mener at begge modellene vil fungere på systemer som er løst koblet og lineære interaksjoner, men at systemer som preges av tett koblede og komplekse interaksjoner vil skape konflikt mellom de to modellene.

I tillegg til de operasjonelle barrierene i form av operasjonsprosedyrer, standarder for handlinger i normal drift, ved indikasjon på feil eller når feil eller ulykker bekreftes deles de tekniske barrierene inn i to grupper. Kontrollene som varsler operatørene om feilfunksjon eller uønsket tilstand og de tekniske innretningene som skal forhindre en hendelse. Kontrollene kan være varsellys som blinker eller begynner å lyse, alarmer eller automatiserte kontroller som stenger ned eller starter en prosess for å reversere en feil. Tekniske barrierene som fysisk segregering av delsystemer, redundans ved dobling av komponenter for å unngå stans og ventiler som skal forhindre en uønsket reversering av prosesser ved feil i systemet (Perrow, 1999).

3.4.2 Menneskeskapte ulykker

Pidgeon & O`Leary (2000) viser til Turners modell for menneskeskapte katastrofer som poengterer at hendelser og farer som har mindre variasjoner fra organisasjonens oppfattelse, som vist til tidligere, er vanskelig å håndtere i inkubasjonsstadiet. For å forhindre ulykker poengterer de viktigheten av å ikke bare fokusere på de farene som faller innen rammen av organisasjonens godt definerte oppfattelse av farer og utvikling av dem, men også utenfor rammen. En viktig tilnærming blir da å ikke la seg begrense av det som har vært, men bruke fantasien til å «se» hva som kan skje i fremtiden. De viser til hvordan denne prosessen ble lagt til rette i forbindelse med opplæringen av Amerikanske brannmenn i den føderale skogbruk tjenesten. Prosessen består i syv «råd» for hvordan en legger til rette for og sikrer tenkning utenfor satte rammer.

(i) En må forsøke å tenke på det en frykter mest skal skje
(ii) Prosessen må legges til rette for å oppnå varierte synsvinkler
(iii) Tenk «hva om?» om potensielle farer

(iv) Ingen verst tenkelige utfall kan utelukkes
(v) Glem eller se vekk fra antakelser om hvordan oppgaver har vært håndtert tidligere
(vi) Nye identifiserte sikkerhetshendelser vil nødvendigvis ikke være mulig å beskrive klart og tydelig, da de er nye, og varians eller tvetydighet må tillates.
(vii) En må tvinge seg selv til å fullføre den visuelle tankerekken av en nestenulykke som utvikler seg til en ulykke

Pidgeon & O`Leary (2000) viser til ulykken med atomkraftverket Tsjernobyl og peker på det kulturelle aspektet for å forhindre menneskeskapte ulykker. De mener en god safety-kultur reflekteres av og kan promoteres med følgende:

1. Safety-forpliktelse fra senior ledelse
2. Alle har et ansvar (*shared care and concern*) for farer og til å fokusere på konsekvensen de kan ha for mennesker
3. Realistiske og fleksible normer og regler knytte til farer; og
4. Kontinuerlig refleksjon over praksis gjennom overvåking, analyse og systemer for tilbakemelding (organisatorisk læring).

3.4.3 Organisatoriske ulykker og menneskelige feilhandlinger

I følge Reason (1997) er nasjonale kulturer basert på felles oppfattelse av verdier, mens en organisasjonskultur blir formet av felles praksis. En god safety kultur kan konstrueres sosialt ved å identifisere og produsere de essensielle komponentene og sette dem sammen til en helhet. En *rapporterende* kultur, en *rettferdig* kultur, en *fleksibel* kultur og en *lærende* kultur, er fire kritiske underkomponenter han har identifisert som beskrivende for en god safety kultur. En god safety kultur kan med andre ord ikke sees på som kun en enhet. Det er en kollektiv læringsprosess hvor det er et samspill mellom elementene, felles måte å tenke, styre og utføre. En sterk kultur er når alle lag i en organisasjon deler de samme mål og verdier, og er basert på forpliktelse, kompetanse og bevissthet. Kulturen får tilstedeværelse i organisasjonen som én helhet og er en organisatorisk barriere som skal forhindre utrygge eller potensielt farlige handlinger som kan skape uønskede hendelser. Han peker i tillegg på redundans som et viktig element, både i kulturperspektivet og tekniske. Redundans i kulturperspektivet kan skapes ved åpenhet, hvor ansatte rådfører seg med hverandre før en

oppgave og/eller beslutning tas. Formålet er å øke kunnskapsgrunnlaget forut for utøvelsen og muligheten til å korrigere.

I tillegg til kultur, som en organisatorisk barriere, viser Reason (1997) til «forsvar-i-dybden». Forsvar i dybden, som prinsipp for risikostyring, ble opprinnelig utviklet i militære sammenhenger (Piètre-Cambacèdès & Bouissou, 2011). Det ble deretter tatt i bruk innen atomkraft og datasikring før det også ble benyttet innen fysisk sikring.
Reason (1997) benytter beskrivelsen forsvar (*defences*) som må tolkes som noe mer enn bare en enkel barriere, da han henviser til barrierer i forsvaret. Han mener forsvaret kan kategoriseres både ut i fra hvilken funksjon de har eller ut i fra måte de oppnår denne funksjonen på. Selv om forsvarets funksjoner er universelle vil måten det er implementert på kunne variere fra organisasjoner, basert på den operasjonelle faren i hver organisasjon. Han mener alle forsvar er designet til å oppnå en eller flere av de følgende funksjonene:

- Det skal skape forståelse og bevissthet til de lokale farene og truslene.
- Det skal gi en klar og tydelig veiledning for safe operasjon
- Det skal gi alarmer og varsel dersom fare eller trusler er nært forestående
- Det skal gjenopprette systemet til en sikker tilstand etter en unormal situasjon
- Det skal være et skille (en eller flere barrierer) mellom farer og potensielle tap (verdi)
- Det skal kontaminere eller eliminere faren dersom den unnslipper barriere over
- Det skal gi tid og rom til rømming og redning dersom kontaminering ikke fungerer

I følge Reason (1997) gir listen over en implisitt forståelse av forsvar i dybden. En rekke lag av beskyttelse, etter hverandre, som alle er klar til å beskytte dersom laget foran bryter sammen. Når forsvaret som skal skape forståelse, bevissthet og prosedyremessig veiledning feiler skal alarmer og varsel gjøre dem oppmerksom på faren slik at systemoperatører kan gjenopprette sikker tilstand. Dersom dette ikke er mulig å oppnå skal fysiske barrierer skille og beskytte mellom fare og potensielt tap (verdi), mens andre forsvar skal kontaminere og eliminere faren. Dersom alle forsvar og barrierer feiler skal evakuering og redningstiltak benyttes, som en del av forsvaret.

Det er nettopp dette mangfoldet av overlappende og gjensidig støttende forsvar som gjøre komplekse teknologiske systemer, slik som atomkraftverk og moderne fly, sikre mot enkeltfeil fra mennesker eller teknikk. Funksjonene i forsvaret oppnås, vanligvis, gjennom en blanding av «harde» og «myke» tiltak. «Harde» tiltak kan være automatiserte sikkerhetstiltak, fysiske barrierer, alarmer og varslere, sperrer (sluser), nøkler, personlig beskyttelsesutstyr og

svakheter som er designet for å knekke, slik som sikringer og sikkerhetspinner på flymotorer. «Myke» tiltak beskriver han (Reason, 1997) avhengig av papir og mennesker. Det er de skrevne lover og regler, samt overvåking av dem, instrukser og prosedyrer, trening, øvelse og orienteringer, administrativ kontroll (arbeidstillatelse etc.), lisenser og sertifikater. Han trekker frem tilsyn som et kritisk tiltak og da spesielt ovenfor operatører i kontrollsystemer som har høy grad av automatisering. Han legger til at forsvar i dybden har også har ulempen med at systemet blir enda mer kompleks og uoversiktlig. Konsekvensen av dette er omhandlet tidligere i oppgaven.

3.4.4 Høypålitelige organisasjoner – High Reliability Organizations

På midten av åttitallet lanserte Todd LaPorte, Gene Rochlin og Karlene Roberts prosjektet *High Reliability Organizations* (HRO) ved universitetet Berkeley (Bourrier, 2011). Prosjektet ansees som opprinnelsen til *High Reliability* teorien. LaPorte & Consolini (1991) viser til, gjennom studie av komplekse og potensielt ulykkes-utsatte organisasjoner i artikkel "*Working in Practice but Not in Theory*", at disse kan opererer i lang tid uten at alvorlige ulykker oppstår. I sitt arbeid studerte de blant annet systemer for kontroll av flytrafikk, hangarskip og komplekse elektrisitetssystemer.

I følge Aven m.fl. (2004) er HRO et perspektiv som har et optimistisk syn på forebygging av ulykker og styring av risiko da utgangspunktet er at ulykker i høyteknologiske systemer kan forebygges. Teorien tar utgangspunkt i at ved å designe organisasjonen riktig er «fullstendig» sikre operasjoner er mulig, selv med komplisert teknologi og stort risikopotensiale. En viktig forutsetning er at det er mulig å utvikle pålitelige systemer baser på upålitelige enkeltkomponenter. Organisasjonen må hele tiden ha fokus på sikkerhet og pålitelighet gjennom desentralisert styring, sterk organisasjonskultur og kontinuerlig læring. Menneskelige feil og svakheter kan kompenseres gjennom å konstruere en tilstrekkelig pålitelig og sikker organisasjon. For å oppnå en tilstrekkelig pålitelig og sikker organisasjon er følgende betingelser nødvendig:

- *Sikkerhet og pålitelighet har høyeste prioritet,* må være forankret hos både formelle og uformelle ledere. Mål om høy sikkerhet og pålitelighet må gjennomsyre hele organisasjonen.

- *Redundans øker sikkerheten.* Duplikasjoner, overlapp og reservesystemer er nødvendig for å kompensere for eventuelle feil, og kan gi pålitelige systemer av upålitelige komponenter.
- *Desentralisert styring, sterk organisasjonskultur og kontinuerlig læring* er viktig. Desentralisert beslutningstaking øker muligheten for raks, fleksible og lokalt tilpasset reaksjon på uventede hendelser. En sterk organisasjonskultur som setter pålitelighet høyt kan øke sikkerheten ved at alle på lavt nivå reagerer likt og riktig på unormale situasjoner. Kontinuerlig øvelse, trening og simulering gir høy pålitelighet. Redundans i organisasjon betyr også at de ansatte *skal* ha forskjeller med hensyn til kultur, opplæring og bakgrunn. Det øker sannsynligheten for at feil og fare som ikke blir oppdaget av en person, kan oppdages av en annen. Den vektlegger også at kolleger kan rådføre seg med hverandre og korrigere hverandre.
- *Organisatorisk læring* gjennom prøving, feiling og simuleringer, og i tillegg av tidligere ulykker er effektivt.

Men ifølge Weick & Sutcliffe (2007) har ikke High Reliability organisasjoner bare er en unik struktur, de tenker og handler forskjellig fra andre organisasjoner. De bruker uttrykket «mindfulness», som sier noe om hele organisasjonens fokus. Alle i organisasjonen har et kontinuerlig fokus på helheten, sammenhenger og er oppmerksomme på indikasjoner på feil og fare. Kompetansen i organisasjon er dynamiske og nye erfaringer adopteres hele tiden inn i organisasjon. De fremhever fem sentrale egenskaper ved HRO:

1. *Fokus på feil*: For å forhindre ulykker må organisasjon hele tiden ha fokus på feil og tidlige signaler på mulig feil. Dette inkluderer å rapportere alle avvik og forsømmelser.
2. *Motvilje til å forenkle fortolkninger*: Organisasjonen motstår tilbøyeligheten til å forenkle virkeligheten ved å benytte for få eller for enkle indikatorer på tilstanden. Høyteknologiske systemer er kompleks og uforutsigbar og det kreves derfor et komplett og nyansert bilde for å forstå.
3. *Sensitivitet ovenfor operasjoner*: Systemer er ikke statisk og lineær, men dynamisk, og fokuset bør derfor være på det operasjonelle.
4. *Forpliktelse til motstandsdyktighet (resilience)*: Organisasjonen håndterer feil, før de får alvorlige konsekvenser, og opprettholder produktivitet. Organisasjonene er ikke feilfri, men de håndterer dem før de utvikles eller kommer ut av kontroll.

5. *Desentralisert beslutningstaking*: Myndigheten til å ta beslutning i kritiske situasjoner kan raskt skifte fra sentralisert til desentralisert, altså dem nærmest eller i situasjonen. En er da ikke avhengig av tillatelse fra noen høyere opp i organisasjonen.

3.5 Barrierestyringen

I de foregående kapitlene er det redegjort for teori som er relevant for å forstå hvorfor organisasjoner som har forsvar og barrierer mot ulykker og farer likevel blir utsatt for uønskede hendelser. I tillegg har vi sett på tilnærminger og perspektiver på hvordan risiko kan styres via organisasjonsdesign og overlappende forsvar og barrierer. I dette siste kapitlet går jeg nærmere inn på hva som bør synliggjøres om barrierene for å sette dem inn i det totale bildet av risikostyringen.

I følge Aven (2007) handler risikostyring om balansen mellom det å utforske muligheter og det å unngå tap og skade. For å finne denne balansen og styre risikoen må en derfor skaffe seg innsikt i risikoforhold og årsaker, for deretter å finne de riktige tiltakene. Hvilken metode som skal benyttes for å finne de riktige risikoforholdene innen security risiko er ikke omforent, verken nasjonalt eller internasjonalt, som FFI-rapport 2015/00923[11] viser til. I rapporten konkluderer de videre med at følgende kjennetegn går igjen i en god tilnærming: *«den(i) er strukturert, (ii) har en arbeidsgruppe med bred kompetanse, (iii) kartlegger kunnskapsstyrken, (iv) er basert på systemforståelse og er konkret, (v) har et helhetlig perspektiv, (vi) kommuniserer risiko og usikkerhet samt (vii) er gjennomsiktig, sporbar og etterprøvbar».* Aven (2007) mener videre at «*med risikostyring forstås alle tiltak og aktiviteter som gjøres for å styre risiko*».

Aven m.fl. (2004) beskriver at det i petroleumsindustrien er vanlig å skille mellom sikkerhetstiltak og beredskap. Sikkerhetstiltak er de tiltak som gjennom en risikoanalyse allerede er implementert for å hindre at en inntrådt faresituasjon utvikler seg til en ulykkessituasjon, eller som hindrer eller reduserer skadevirkningene av inntrådte ulykkessituasjoner. Tiltakene kan beskrives som beredskapsbarrierer eller bare barrierer, men de skiller seg fra de tiltak som planlegges implementert under ledelse av en mobilisert beredskapsorganisasjon.

[11] Risikovurdering for tilsiktede uønskede handlinger

Risikostyringen starter allerede i planleggingsfasen hvor barrierene velges, dimensjoneres og bygges inn, og i driftsfasen hvor barrierene holdes ved like, videreutvikles og forbedres. Overvåking av barrierene er viktig da endringer i en barrieres ytelse endrer risikonivået. Aven m.fl. (2004) skiller mellom *aktive* og *passive* barrierer. De *aktive* barrierene krever en ekstern aktivering, manuell eller automatisk, mens de *passive* er helt uavhengig ekstern styring eller aktivisering.

De (Aven m.fl., 2004) benytter **ytelse** som overordnet begrep for å beskrive den totale godheten eller effekten av barrierene eller tiltakene. Grunnlaget for den totale godheten eller effekten kommer av en vurdering av barrierenes *pålitelighet*, *effektivitet* og *sårbarhet*, og med det mener de:

Pålitelighet – om barrieren virker ved behov. Her vurderer en enhetens evne til å utføre den tiltenkte funksjonen barrieren har. Barrieren kan testes gjennom drift eller ved tester og det antall ganger barrieren virker gir et uttrykk for observert eller målt pålitelighet. Når pålitelighet vurderes antas det at barrieren ikke er ødelagt som følge av ulykkessituasjon.

Effektivitet – kapasitet og tid, gitt at den fungerer. Beskrivelsen og målingen av en barrieres effektivitet kan variere avhengig av funksjonalitet og det antas at den ikke ødelegges som følge av ulykkessituasjonen i det denne oppstår. Effektivitet kan være et mål på tid det tar før deteksjon, tid en brannvegg opprettholder funksjonen sin eller kapasitet til en eksplosjonsvegg. Det kan i tillegg inneholde en sannsynlighetsparameter, for eksempel sannsynligheten for at et gitt antall personer møter innenfor en gitt tid for mønstring av et brannlag.

Sårbarhet – beskriver grad av svekkelse eller bortfall av barrieren gitt ulykkeshendelsen. Sårbarheten kan også omtales som robusthet og uttrykkes kvalitativt eller kvantitativt. Det er en beskrivelse av eller et mål på barrierens evne til å opprettholde sin funksjon når den utsettes for påkjenninger.

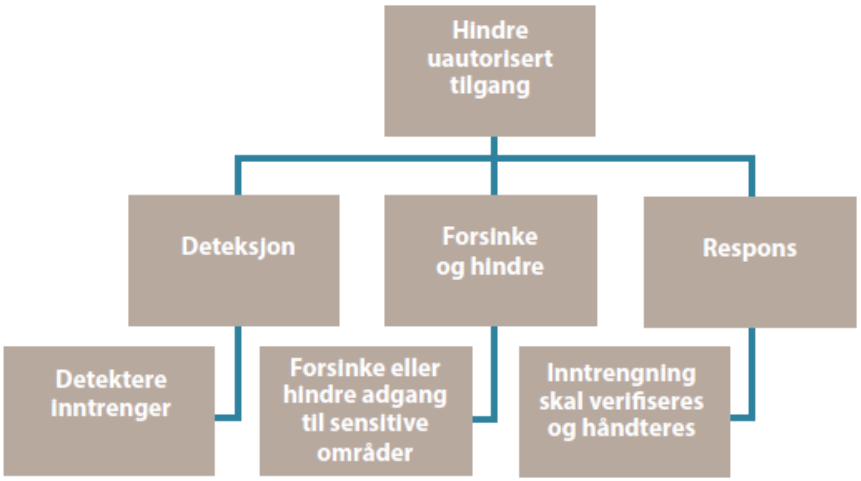
Petroleumstilsynet uttrykte[12] så sent som i 2017 bekymring for selskapers forståelse av barrierer og krav. Gitt Petroleumstilsynets rolle (ibid) oppimot petroleumssektoren, også med tanke på kunnskapsdeling og erfaring, er det naturlig å inkludere «Barrierenotatet 2017» (Ptil, 2017) som beskriver «Prinsipper for barrierestyring i petroleumsvirksomheten» (heretter

[12] www.ptil.no

omtalt som barrierenotatet). Ptil er tydelig på at det er et notat, som ikke innfører noe krav, men at det er en faglig knytning til styringsforskriftens §5 om barrierer og relaterte regelverkskrav. Det er verd å merke seg at Ptil, på lik linje med Schiefloe (2011), gjennom barrierenotatet eksplisitt mener at kunnskapen og prinsipper om industriell sikkerhet og risikostyring kan anvendes i forhold til intenderte handlinger (tilsiktede uønskede handlinger – security). Ptil benytter *sikring* om security og *sikkerhet* om safety for å skille begrepene i barrierenotatet og har i tillegg inkludert et eget vedlegg med utfyllende informasjon og eksempler om sikring. Her fremgår det at sikringshendelser defineres inn som feil, fare- og ulykkessituasjoner. Bruke av prinsippene for barrierestyring fra barrierenotatet, også for sikingshendelser, mener de kan bidrar til en mer systematisk tilnærming til identifisering, etablering og vedlikehold av sikringsbarrierene.

En viktig presisering i barrierenotatet (Ptil, 2017) er at risikostyringen, også med tanke på sikringsrisiko, starter allerede i planleggingen av et anlegg eller en innretning. Dersom en i planleggingen utformer bygg og rom på en slik måte at en enten skjuler eller vanskeliggjør tilgang til sensitive eller «sårbare» rom vil en kunne redusere sikringsrisiko igjennom design. De trekker også barrierestyringen inn, som en integrert del, av den totale risikostyringen i en organisasjon.

Ptil (2017) beskriver et sikringssystem, med en barrierefunksjon baser på en risikovurdering, som bestående av flere delsystemer med delfunksjoner og peker på lik linjen med Reason (1997) på samspillet mellom tekniske-, operasjonelle- og organisatoriske barrierer for å oppnå et sikringssystems barrierefunksjon. Det er derfor viktig å beskrive de forskjellige delsystemenes barrieredelfunksjoner som skal støtte opp under det totale systemets barrierefunksjon og risikoreduksjon. Ved å strukturere et barrieresystems i henhold til den totale barrierefunksjon og barrieredelfunksjoner i undersystemer vil skape en tydelighet hvor en enkelt kan vurdere systemets totale funksjon og hvilke underfunksjoner som vil være mer kritisk enn andre. Barrieredelfunksjoner kan for eksempel være deteksjon, forsinkelse eller respons, som vist i figur 3.



Figur 3. Barrierefunksjon og delfunksjoner for sikringssystem (Ptil, 2017)

I følge Ptil (2017) handler barrierestyring om mer enn bare å beskrive hvilke funksjoner og delfunksjoner et sikringssystem er bygd opp av. Barrierestyring handler om at en systematisk og kontinuerlig sikrer at de nødvendige barrierene er tilstede og kan oppfylle den funksjonen de er satt til. For å kunne sikre at barrierene oppfyller den funksjonen de er satt til må vi beskrive hva dette er. Alle skjønner at et overvåkningskamera overvåker, men hvis det skal kunne overvåke døgnet rundt må det også kunne «se» om natten. Det må derfor settes noen krav til teknikken i kameraet for at det skal klare dette. Ptil kaller dette ytelseskrav og tilsvarende krav vil en kunne sette på organisatoriske og operasjonelle barrierer.

I tillegg vil alle tre barrieretypene (tekniske, operasjonelle og organisatoriske) påvirkes av forskjellige interne og eksterne faktorer. Vær og vind, søvn, trening, fysisk form og kvaliteten i prosedyrer er noen interne og eksterne faktorer som kan påvirke en barrieres kvalitet og ytelse. Ptil (2017) påpeker viktigheten av de ytelsespåvirkende faktorene da de kobler denne informasjonen sammen med behovet for vedlikehold. Det må lages en plan for vedlikeholdet av barriereelementene slik at en sikrer det totale systemets barrierefunksjon til enhver tid. I tillegg må dette sees oppimot produsenter og leverandørers dokumenterte vedlikeholdsbehov og krav.

Figur 4. Totaloversikt over sikringssystem (Ptil, 2017)

Ut ifra dette (Ptil, 2017) blir følgende faktorer viktig å synliggjøre for å ivareta en god styring av sikringsbarrierer:

Barrierefunksjon – beskrivelse av sikringssystemets totale funksjon: For eksempel å hindre uautorisert tilgang.

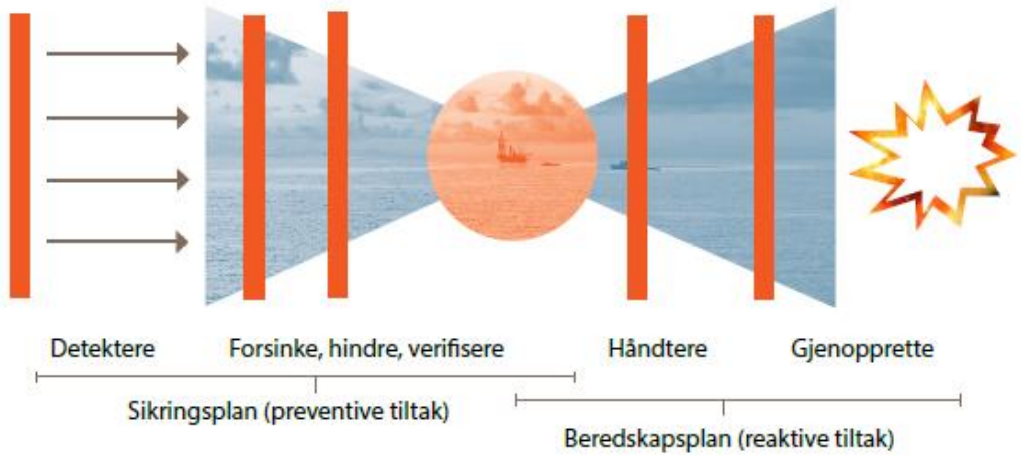
Barriereelement – beskriver de tekniske, operasjonelle eller organisatoriske tiltakene eller løsningene som inngår i sikringssystemet. Tiltakene eller løsningene kan for eksempel være skilt, overvåkingskamera, sensorer, porter og prosedyrer.

Barrieredelfunksjoner – beskriver barriereelementenes delfunksjoner for å oppnå systemets totale funksjon. Slike delfunksjoner kan, ut ifra barrierenotatet være, avskrekking, deteksjon, verifikasjon, forsinkelse, hindre, håndtere og gjenopprette.

Ytelseskrav – beskriver de kravene som er satt til de forskjellige barriereelementene. Etterprøvbare krav til elementene som skal sikre deres funksjon. Slike krav kan være graden deteksjon et kamera eller en sensor skal oppnå 24/7, faglig kompetansenivå på operatører og vakter eller tidskrav og utførelse i henhold til tid.

Ytelsespåvirkende faktorer – beskriver hva som kan påvirke barriereelementene og svekke ytelsen og derav systemets totale funksjonalitet. Dette kan være værforhold, innstilling og justering av utstyr, søvn, trening og fysisk form eller prosedyrer.

Prinsippskissen (Ptil, 2017) for sikringsbarrierer skiller mellom proaktive tiltak og reaktive tiltak, og plasserer dem henholdsvis i Sikringsplan og Beredskapsplan. Men til tross for denne delingen visualiserer og signaliserer skissen også en tydelig sammenheng mellom sikring og beredskap. Det som gjennom sikringsrisikoanalysen er identifisert og laget barrierer mot på venstre side er det samme som beredskap må kunne håndtere på høyre side. Det må derfor tolkes som en tydelig sammenheng mellom sikring og beredskap.



Figur 5. Prinsippskisse for barrierer anvendt på sikring

3.6 Oppsummering av teori

Denne oppgaven ser på hvordan styringen av barrierer mot tilsiktede uønskede hendelser har utviklet seg i Statoil og hva er konsekvensene eller resultatene av denne utviklingen.

Majoriteten av forskning på hvorfor uønskede hendelser skjer, om og hvordan dette kan forhindres har i hovedsak sin opprinnelse innen fagfeltet safety. Men ifølge Schiefloe (2011) er dette relevant kunnskap og kan anvendes i forhold til security og intenderte handlinger (tilsiktede uønskede hendelser).

Det teoretiske bidraget i denne oppgaven er derfor hentet fra den samme konteksten, safety, og med formål om å se dette oppimot utviklingen i Statoil og hvordan dette kan bidra til den videre utviklingen av barrierestyring mot tilsiktede uønskede hendelser.

Barrierer, ut i fra det teoretiske bidraget, er noe ekstra og i tillegg til det som skal til for at et system skal kunne fungere. Risiko i systemet styres gjennom konstruksjon, valg av komponenter i og sammensetning av systemet, mens barrierer er noe som kommer utpå det igjen. Det kan være organisatoriske barrierer, ofte i form av krav og overordnede føringer gjennom styrende dokumentasjon, tekniske barrierer i form av en innretning eller mennesker kan være barrierer i form av vakthold.

I lys av dette teoretiske bidraget søker jeg i denne oppgaven å forske på styringen av barrierer, dette noe ekstra.

4 Metode

I følge Jacobsen (2015) er hensikten med forskning å frambringe gyldig og troverdig kunnskap om virkeligheten. Vitenskapelig metode er strategien eller planen for hvordan en går frem for å oppnå gyldig og troverdig kunnskap. Jeg vil i dette kapittelet redegjøre for de valgene jeg har gjort og den metoden jeg har benyttet i denne studien for å besvare problemstillingen.

4.1 Valg av problemstilling

Valg av problemstilling har vært en lang prosess. Den startet samtidig med dette studiet som jeg nå er i avslutningen av. Jeg har lenge hatt interesse for analyse og har jobbet med «*operativ kriminalanalyse*», hvor formålet er å støtte beslutningstaker i etterforskning av kriminalsaker med stor informasjonsmengde. Parallelt med dette studiet har jeg også bidratt inn i prosessen med å utvikle både styringssystem og metodikk for security risikoanalyser. Denne utviklingen har fortsatt etter at jeg sluttet i den avdelingen som har ansvar for utviklingen, men interessen min for dette er fortsatt sterk og fagfeltet synes jeg er interessant. En tanke om å skrive om dette har derfor hele tiden vært tilstede, men vinklingen av problemstillingen synes jeg har vært vanskelig. Flere vinklinger og problemstillinger har vært testet og forkastet. Det har vært viktig for meg å velge et tema som ikke medførte at oppgaven ble klausulert. Men etter flere diskusjoner, både med meg selv og andre, ble en problemstilling formulert. Den har på en måte «*vært tilgjengelig*» for meg siden før jeg startet i Statoil. Jeg leste nemlig granskningsrapporten[13] i forbindelse med at jeg søkte på den første stillingen min i selskapet. En av anbefalingene, som vist til i innledningen, var at selskapet måtte utvikle styringssystemet. Problemformuleringen ble derfor etterhvert til følgende: *Hvordan har metoden for styring av barrierer mot tilsiktede uønskede hendelser utviklet seg i selskapet og hvordan er den forankret i styrende dokumentasjon?* Hensikten med problemstillingen er å gå i dybden for å finne ut om og eventuelt hvordan utviklingen kan påvirke selskapets evne og mulighet til å styre barrierer mot tilsiktede uønskede hendelser. Dette er en eksplorerende problemstilling (Jacobsen, 2015).

[13] The In Amenas Attack. Report of the investigation into the terrorist attack on In Amenas

4.2 Undersøkelsesdesign og metodevalg

Intensive undersøkelsesdesign er velegnet for å belyse problemstillinger der interessen ligger i å gå i dybden på få enheter (5-10 enheter). Intensive undersøkelsesdesign gir muligheten for å få frem detaljer og nyanser i enhetene, mens *ekstensive* undersøkelsesdesign søker breddekunnskap (Jacobsen, 2015). Jeg har valgt et *intensivt* undersøkelsesdesign. Årsaken til dette er at jeg ønsker å undersøke metodikken som lå til grunne i forskjellige tidsperioder og få frem mest mulig detaljer om selve metodikken. Deretter ønsker jeg å gå i dybden på et mindre antall security risikoanalyser for de samme periodene og få frem mest mulig detaljer om hvordan barrierer mot tilsiktede uønskede hendelser (terror) er beskrevet i disse. Begge delene peker på et *intensivt* undersøkelsesdesign. Når jeg har valgt et *intensivt* design og avgrenset studien til en trusselaktør så er jeg klar over at dette medfører at den statistiske generaliseringen blir liten, men at den teoretiske generaliseringen blir større. Dette er avveininger og valg som jeg har vært nødt til å gjøre på grunn av egen ressursbruk.

Forholdet mellom kvalitative og kvantitative studier i samfunnsvitenskapen er omdiskutert, spesielt i debatten om positivismen, men ifølge Grønmo (2004) refererer begrepene kvalitativ og kvantitativ først og fremst til egenskaper ved de data som samles inn og analyseres. Grovt og enkelt kan data som uttrykkes i rene tall eller andre mengdeenheter karakteriseres som kvantitative. Mens data som ikke uttrykkes på denne måten vil være kvalitative data.

I dette studiet har jeg valgt å benytte kvalitativ metode. Grunnlaget for dette valget er at jeg ønsker å få frem detaljene og nyansene mellom de forskjellige metodikkene og bruken i forskjellige perioder. I tillegg gir den kvalitative metoden meg større fleksibilitet til å gjøre endringer underveis, spesielt med tanke på problemstilling. Kvalitative metoder er i tillegg ressurskrevende og er årsaken til at jeg har begrenset antall undersøkte enheter og avgrenset mot trusselen som kalles terror i enhetene jeg undersøkte.

4.3 Undersøkelsesopplegg

Valget av undersøkelsesopplegg for en studie kan være utfordrende. I følge Jacobsen (2015) er det umulig å svare på hvilken metode som er best å benytte, *induktiv*, *deduktiv* eller *abduktiv*. Det handler i større grad om at alle metoder har styrker og svakheter og en må finne den som passer best for sin forskning. Formålet med dette studiet er ikke å skape ny teori, men å undersøke hvordan utviklingen av styringssystemet har forbedret barrierestyringen.

Security har hatt et stort fokus i selskapet som har ført til en. Teorigrunnlaget i denne oppgaven og kunnskapen om både fokuset og utviklingen har skapt en del forventninger om hvordan virkeligheten ser ut, empirien samles derfor inn for å se om denne oppfattelsen stemmer med virkeligheten. Det er derfor benyttet en deduktiv metode.

Jacobsen (2015) påpeker at det aldri vil være mulig å velge det perfekte undersøkelsesopplegget, noe jeg har erfart i dette studiet. Jeg ønsket å undersøke hvordan én metodikk har endret seg, noe som tilsier en *tidsseriestudie*. Men samtidig ønsket jeg å undersøke bruken av metodikken, hvordan ble barrierer beskrevet i metodikken og i flere eksempler innen en og samme periode, noe som tilsier *tverrsnittstudier*. Undersøkelsesopplegget består derfor av begge deler. Første delen er en *tidsseriestudie* for å undersøke og beskrive hvordan metodikken har endret seg. I den andre delen har jeg benyttet et *tverrsnitts* studie for å undersøke og beskrive resultatet av metodikken i de forskjellige periodene.

4.4 Valg av kilder

I følge Jacobsen (2015) er det i hovedsak fire forskjellige metoder for innsamling av kvalitative åpen data. Det *individuelle åpne intervjuet*, *fokusgruppeintervju*, *observasjon* og *dokumentundersøkelse*. Jeg har valgt dokumentundersøkelse. Grunnlaget for dette valget er sammensatt. For det første er det metodikkens utvikling jeg undersøker og den er dokumentert gjennom styrende dokumentasjon, veiledninger og maler. I tillegg ønsker jeg å se på resultatet av bruken av metodikken, nå og tidligere, som også tilsier dokumentundersøkelse. Når det har vært et så stort fokus på security i selskapet over så lang tid er det naturlig at det er en kunnskapsmessig utvikling og modning i selskapet. En ren dokumentundersøkelse vil da ikke redegjøre for om resultatet er kun på grunn av en bedring i metodikken eller om resultatet er bedre på grunn av utvikling og modning hos de ansatte. Dette er en svakhet som taler mot en ren dokumentundersøkelse, men samtidig ser vi de ansatte som en mer dynamisk gruppe som i større grad en tidligere bytter stillinger. Men på den andre siden så vil en oppgave med en ren dokumentundersøkelse i større grad kunne avdekke metodiske svakheter da disse ikke blir kompensert av kunnskapsstyrken til den som utfører oppgaven. I tillegg vil jeg, kun ved å forholde meg til dokumenter, kunne gå i dybden og ha «nærhet» uten å risikere påvirkning av intervjuobjekter. Jeg mener dette gjør studien mer objektiv og troverdig. I en ren dokumentundersøkelse vil en også sikre at det er den

informasjonen som metodikken frembringer, og som vil være gjenstand for undersøkelse og granskning etter en hendelse, som vurderes og ikke hva den som har gjennomført vurderingen måtte mene med det denne skrev.

Informasjon jeg baserer dette studiet på er *primærdata* og i utgangspunktet fra en *førstehåndskilde*. Primærdata (Jacobsen, 2015) innebærer at det er forskeren som samler inn opplysningene for første gang. Førstehåndskilde betyr at personen som har skrevet informasjonen observerte dette selv. Det er et krav i styringssystemet[14] at den som gjennomfører analysene skal være fysisk på lokasjon, noe som også er praksis og informasjonen som er skrevet om barrierene er derfor i utgangspunktet fra en førstehåndskilde som har observert dette selv. Men det vil likevel være noe informasjon som ikke er observerbart i en vurdering og som igjen innhentes fra andre. Dette gjør at deler av primærdata i grunnlaget er fra *andrehåndskilder* og kanskje *tredjehåndskilder*. Dette vil ikke kunne avklare eller kontrollere, men igjen er det avveininger som er gjort da dokumentanalyse ble valgt. Men når det er valgt dokumentanalyse er det med viten om at dette kan påvirke studiet ved at ikke all informasjon jeg underveis ser jeg kunne trengt er tilstede.

4.5 Utvalg av kilder

En av de største utfordringene knyttet til dokumentstudier er utsiling av kilder i forkant av undersøkelsen (Jacobsen, 2015, s. 188). Når jeg først har valgt dokumentundersøkelse i denne oppgaven så styrer dette valget mye av utvelgelsen av kilder. Naturlige kilder som må være med er styrende dokumentasjon som beskriver krav til utførelse, involvering, frekvens, prosess og som gir veiledning. Dette er tilgjengelig i ARIS[15] sammen med maler og andre beskrivelser. Denne dokumentasjon har allerede vært gjenstand for en form for siling, men som sannsynligvis har mindre betydning for denne oppgaven. Når dokumentasjonen i styringssystemet ble skrevet er det noen som har bestemt hva som skal skrives og dermed silt informasjon. I tillegg må all styrende dokumentasjon sendes ut på høring og tilbakemelding fra høringen kan føre til nye endringer og fjerning av informasjon. All styrende dokumentasjon har vært utsatt for en form for siling, men jeg mener at det er av mindre betydning. For det er den godkjente styrende dokumentasjonen jeg ønsker å undersøke, ikke

[14] ARIS: Systemet for styrende dokumentasjon (Insight: Statoil intranett)
[15] ARIS: Systemet for styrende dokumentasjon (Insight: Statoil intranett)

hva som ble tenkt og sagt i forkant. Det er ikke en situasjon som er dokumentert og silt gjennom flere ledd slik som i eksemplet i Jacobsen (2015, s. 188, figur 9.3). Styrende dokumentasjon er tilgjengelig for alle ansatte og dermed også for meg. Det vil derfor ikke være en siling av hva jeg har tilgang til, men det vil være en siling i form av hva jeg velger å ta med. Jeg mener dette vil være den første *viktige* silingen som må dokumenteres i beskrivelsen av metode. Jeg har tilgang til all styrende dokumentasjon, som beskrevet over, men jeg kommer til å gjøre et utvalg av hva jeg mener er viktig for oppgaven og dermed siler informasjon.

Security risikoanalysene som er gjennomført vil også være en naturlig del av datagrunnlaget da jeg vil undersøke resultatet av bruken av metodikken. Disse analysene vil være utsatt for en type siling som er beskrevet i Jacobsen (2015, s. 188) og av forskjellige personer. Informasjonsgrunnlaget i selve vurderingen er utsatt for siling i flere ledd. Noen har laget en trusselvurdering som er grunnlaget for vurderingen og her er det gjort en siling av hva som ble tatt med. Den som har gjennomført vurderingen har igjen gjort et utvalg fra trusselvurderingen. Det er ikke hele vurderingen som er gjenstand for undersøkelse i denne oppgaven, men det er likevel viktig å påpeke denne silingen da informasjonen til slutt er grunnlaget for barrierestyringen som er grunnlaget for oppgaven. Men også innen barrierebeskrivelsene vil dokumentasjonen være utsatt for siling, som jeg har vært innom ovenfor under beskrivelse av type kilder til informasjonen. Den som har skrevet vurderingen vil sile informasjon da det ikke vil være mulig å beskrive alt denne ser og oppfatter. I tillegg har det vært en siling av informasjon da det er andre som også bidrar med informasjon om barrierene. Det kan med andre ord være forskjell mellom den faktiske situasjonen og hva som er valgt tatt med i vurderingen. Dette kan selvsagt være en ulempe med tanke på styringen av barrierene. Det vil også kunne påvirke resultatet i denne oppgaven ved at manglende beskrivelser og dokumentasjon, på grunn av siling, gir et bedre eller et dårligere bilde av situasjon enn det den faktisk er.

Jacobsen (2015) viser til kvalitetsvurdering av kilden og at dette i utgangspunktet knytter seg til *kunnskap* og *kompetanse* hos den som har skrevet informasjonen. Jeg har avgrenset studiet fra å vurdere kompetanse i det utførende leddet. Dette som en naturlig begrensning av studiet, men også fordi Statoil har kompetansekrav[16] til alle som skal gjennomføre de analysene jeg benytter i utvalget. Men i det utvalget jeg benytter vil det være forskjellige personer som har

[16] ARIS: Systemet for styrende dokumentasjon (Insight: Statoil intranett)

gjennomført de forskjellige analysene og jeg vil da få datagrunnlag produsert av personer med forskjellig kompetanse. Jeg vil derfor måtte gjøre en vurdering av kvaliteten i datagrunnlaget, hvorvidt det har den kvaliteten som trengs for å besvare forskningsspørsmålene. Dette må igjen betraktes som en siling av forskeren.

Det å analysere alle security risikoanalysene som Statoil har vil være en for omfattende oppgave, men samtidig må det analyseres mange nok til at funnene er gyldige og troverdige. Jacobsen (2015) viser til *metning* som kan tolkes til at man stopper videre datainnsamling når ny innsamling ikke lengre gir noe nytt. For denne oppgaven må *metning* vurderes på to forskjellige måter. Mye av datagrunnlaget er ikke gjentakende beskrivelser av sitasjoner. Det finnes bare en utgave å studere, slik som styrende dokumentasjon. Men disse er igjen inndelt i funksjonsområder, slik som security, safety og beredskap[17]. For dette området av empirien må metning tolkes som at jeg stopper når andre systemer ikke gir informasjon eller ny informasjon om temaet. For security risikoanalysene vil jeg få det antallet jeg selv definerer jeg har behov for. Behovet vil derfor fortløpende bli vurdert og kommunisert ut ifra hvorvidt nye analyser gir ny informasjon.

4.6 Analyseprosessen

I følge Jacobsen (2015) må kompleksiteten i datagrunnlaget reduseres ved at informasjonen forenkles og struktureres. Dette skal for å skape en oversikt som gjør at det er mulig å trekke noe fornuftig ut av informasjonsmengden. Han beskriver videre, i hovedsak to metoder for analyse, *innholdsanalyse* og p*rosessanalyse*. Jeg har valg å benytte innholdsanalyse da jeg mener at informasjon i datagrunnlaget kan reduseres til noen overordnede og meningsfylte kategorier. Ved å sammenstille datamaterialet kan en deretter peke på mønstre, regulariteter, spesielle avvik og underliggende årsaker. Han deler den kvalitative analyseprosessen inn i fire deler:

- Dokumentere: I denne fasen beskrives og, til en viss grad, systematiseres datamaterialet.
- Utforske: Her gjør forskeren seg kjent med materialet og gjør en usystematisk leting etter forhold som «*trer fram fra*» dataene.

[17] ARIS: Systemet for styrende dokumentasjon (Insight: Statoil intranett)

- Systematisering og kategorisering: Dataene struktureres etter kategorier som kan være team, hendelser, steder og tidspunkter. Det er forskerens kriterier som bestemmer struktureringen.
- Sammenbinde: I denne fasen trekkes forbindelsene og sammenhengene mellom de ulike kategoriene.

Jacobsen (2015) beskriver i hovedsak to former for kategorisering; *åpen koding – syklus koding* og *aksial koding* eller *andre-syklus*. Den første formen tar utgangspunkt i data i teksten og en samler den teksten som likner hverandre eller omhandler det samme og kaller det en kategori. Slik bygges det opp flere kategorier og deretter mindre grupper. I den andre formen er det undersøkeren som lager kategoriene, uten at disse nødvendigvis finnes i teksten, og etter at den første analysen er gjennomført. Jeg har kombinert disse metodene i analyseprosessen.

Jeg tok utgangspunkt i forskningsspørsmålene og i den første delen benyttet jeg *åpen koding*. Her ble kategoriene til på bakgrunn av en samling av tekst fra datagrunnlaget som bestod av styrende dokumentasjon, prosesser, krav og veiledninger, i tillegg til selve malen for security risikoanalyser. I den andre delen, siste forskningsspørsmål, benyttet jeg *aksial koding*. Grunnlaget for å benytte *aksial koding* til å besvare siste forskningsspørsmål var at jeg nå hadde en oversikt over teorigrunnlaget og datagrunnlaget som gjorde at jeg mener jeg kunne sette opp de kategoriene som måtte til for å hente ut den informasjonen som var interessant oppimot forskningsspørsmålet. Jacobsen (2015) beskriver det forholdsvis lille skillet mellom planlegging, gjennomføring og analyse som en av styrkene med kvalitativ metode. Hvordan datagrunnlaget skulle analyseres har vært i tankene mine mens jeg skrev teorien og har derfor trolig også påvirket hvordan jeg skrev teorien. Min oppfattelse er at den analytiske prosessen har pågått i hele prosessen med å skrive denne oppgaven.

Jeg har fulgt analyseprosessen beskrevet over (Jacobsen, 2015) men siden jeg benyttet to forskjellige metoder for koding består den totale analysen av tre deler. Første del, *dokumenteringsfasen*, er felles for begge. Her ble datagrunnlaget delt inn i beskrivende mapper avhengig om det var styrende dokumentasjon, prosesser, krav, veiledere, security risikoanalyser og i henhold til tidsperiode.

I denne fasen leste jeg også store deler av datagrunnlaget, noe som dro ned skillet til neste fase, *utforskningen*. Både gjennom denne fasen og neste fase, *systematisering* og *kategorisering*, ble det benyttet *åpen koding* knyttet oppimot de første

forskningsspørsmålene. Informasjon i kategoriene ble deretter knyttet sammen (sammenbindingen), men i henhold til sin tidsperiode, for deretter å se de to tidsperiodene oppimot hverandre.

For å besvare det siste forskningsspørsmålet, som baserer seg i stor grad på ferdig utfylte security risikoanalyser, ble de samme fasene gjennomgått. Men metoden skiller seg ved at jeg benyttet *aksial koding*. I tillegg er metodikkene i de to tidsperiodene strukturmessig forskjellige og datagrunnlaget måtte derfor i tillegg omstruktureres og samles. Jeg benyttet i større grad teks-graving (Jacobsen, 2015) til å utforske og samle teks i henhold til kategori.

4.7 Validitet

Studiets validitet betinger, ifølge Jacobsen (2015), at en kritisk drøfter kvaliteten i metoden når en skal vurdere om konklusjonene er gyldige og til å stole på. Han viser til at intern gyldighet handler om hvorvidt en har fått tak i det en ønsket og videre at den eksterne gyldigheten handler om hvorvidt funnene kan generaliseres og gjelde for andre enn dem som faktisk er undersøkt.

Den *interne gyldigheten* i dette studiet vil indikeres av hvorvidt de riktige dataene er samlet inn. Det har vært benyttet *primærdata* i dette studiet og begrensningene i tilgangen har kun vært styrt av egne ressurser og tid. Jeg mener dette styrker den interne gyldigheten, men samtidig vil begrensninger i egne ressurser og tid også kunne påvirke gyldigheten ved at kun et begrenset antall kilder har vært mulig å undersøke.

Ekstern gyldighet i dette studiet indikeres hvorvidt funnene kan overføres til de enhetene som ikke har vært undersøkt og Jacobsen (2015) peker på at jo flere enheter som undersøkes, jo større sannsynlighet er det for at man kan generalisere. Dette studiet baserer seg på 12 enheter, men som til sammen har 158 scenarioer og sårbarhetsvurderinger som alle har vært undersøkt og analysert. Funnene i analysene mener jeg er så entydige at dette styrker sannsynligheten for at en kan generalisere funnene.

4.8 Reliabilitet

Grønmo (2004) knytter reliabiliteten til datamaterialets pålitelighet og at reliabiliteten er høy hvis undersøkelsesopplegget og datainnsamlingen gi pålitelig data. Han mener at dersom en

får identisk data, ved bruk det samme undersøkelsesopplegget ved ulike innsamlinger, så er det et uttrykk for pålitelighet. Reliabiliteten er et uttrykk for hvor stort samsvar det er mellom datasettene for slike gjentatte datainnsamlinger. Jacobsen (2015) peker på om det er trekk ved selve undersøkelsen som har skapt de resultatene en har kommet frem til. I dette legger han at undersøkelsesopplegget, datainnsamlingen og analysen kan ha påvirket resultatet. Han viser også til slurv og unøyaktig nedtegning og analyse av data som en mulig trussel mot troverdigheten av studiet.

I dette studiet er det benyttet selskapets styrende dokumentasjon, noe er offentlig tilgjengelig på nett, mens andre ting ligger åpent på det interne nettverket. Det finnes kun en utgave, noe som gjør at andre forskere vil få nøyaktig det samme datamaterialet ved å gjenta datainnsamlingen. Videre er det benyttet internt graderte dokumenter, security risikoanalyser, men som er sentralt lagret i selskapet. Her vil også andre forskere kunne få tilgang til nøyaktig det samme datamaterialet ved gjentakelse av undersøkelsesopplegget. Datamaterialet som er analysert er primærdata som er elektronisk kopiert over i nytt format for å struktureres, men uten at teksten har vært endret, noe jeg mener styrker troverdigheten i datamaterialet. Men analysene og resultatet baserer seg på mine kategorier, min kategorisering og min tolkning av data for kategorisering. Kategoriseringen av den originale informasjonen ble gjort i Excel. Dette gjorde det mulig både å filtrere på informasjon samt går tilbake og verifisere mot det originale materialet, men min tolkning av tekstenes betydning vil selvsagt kunne bli tolket av andre på en annen måte. Dersom en annen forsker benytter samme datagrunnlag antar jeg at denne vil kunne komme frem til tilsvarende resultat.

4.9 Styrker og svakheter

Styrken ved dette studiet mener jeg ligger i datagrunnlaget. Utvalget består av 12 enheter, noe som virker å være innenfor rammen av hva som er vanlig i kvalitative undersøkelsesopplegg. Men det er analyser og kategorisert informasjon fra 158 scenarioer og sårbarhetsanalyser, noe jeg mener er en styrke. I tillegg er det benyttet datakilder som beskriver hvordan metodene skulle benyttes, noe jeg mener også er en styrke.

Svakheter med studien mener jeg er at det ikke har vært benyttet informanter. Det kunne vært benyttet informanter som er brukere av metodene og informanter som er mottakere av det ferdige produktet. I tillegg vil det kunne være en svakhet med studiet at jeg er ansatt i

selskapet og har vær involvert i utviklingen. Dette er en rolle jeg har forsøkt å være bevist gjennom å vurdere all informasjon så objektivt som mulig. Jeg har derfor forsøkt å holde på prosedyren; dersom jeg er i tvil om beskrivelsen kvalifiserte til å være god nok til den kategorien jeg tenkte, da var det ikke tvil og da skulle den ikke kvalifisere.

5 Empiri

I dette kapittelet redegjøres det for resultatet av dokumentanalysene. Jeg vil først starte med å vise til hvordan Statoil definerer security og hva de legger i begrepet security risiko. Dette gjøres i første delkapittel. Det teoretiske grunnlaget i oppgaven peker på at metoden for risikovurderingen påvirker innsikt i risikoforhold og årsaker, som igjen gir grunnlag for å finne de riktige barrierene. Jeg vil derfor i presentasjon av resultatene fra dokumentanalysene også inkludere metode og analyseprosess. Dette gjøres i det andre delkapitlet som omhandler utviklingen og forankring av barrierestyring i Statoil og baserer seg på analyse av styrende dokumentasjon, brukerveiledere, malene for security risikoanalyser og materiale benyttet i opplæring. Det siste delkapitlet presenterer analyseresultatene av de undersøkte security risikoanalysene utført i selskapet siden 2013 og frem til 2018.

5.1 Definisjon

I Statoil defineres security som beskyttelse mot ondsinnet intensjon (*protection against malicious intent*). Security deles opp i tre området:

- **Fysisk**: Beskyttelse av personell og materielle verdier
- **Informasjon**: Beskytter konfidensialiteten, integriteten og tilgjengeligheten av informasjon
- **Personell**: Beskyttelse mot dem som utnytter autorisert adgang til uautoriserte handlinger eller hensikter, også kjent som insiders.

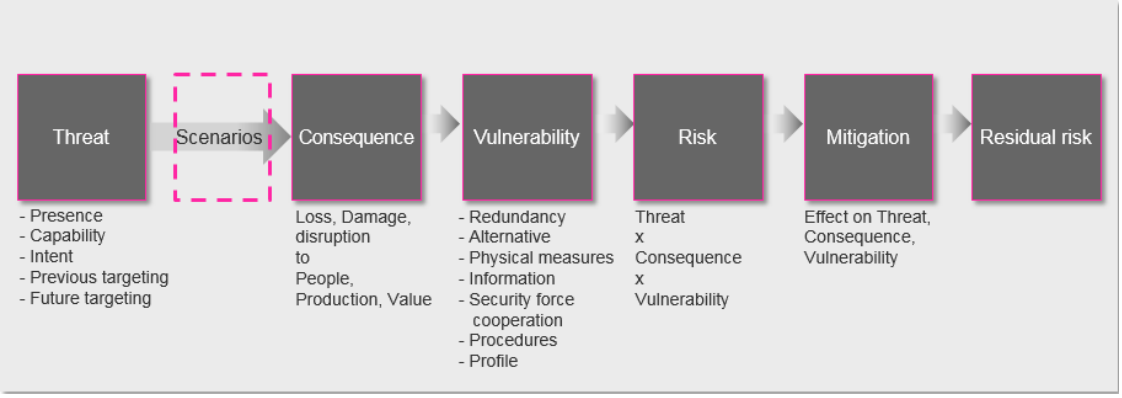
Security risiko defineres som relasjon eller funksjon mellom komponentene *trussel, konsekvens* og *sårbarhet*. Dette forklares videre med følgende: «*A threat to Statoil implies that somebody has the intent and the capability to do us harm. Vulnerability is a weakness, or*

gap, in our protective measures, procedures or behavior that can be exploited. The consequence is the outcome of a threat acting upon a vulnerability and normally has a value implication – it affects our business negatively by causing loss, damage or disruption"[18]

5.2 Metode

5.2.1 Tidsperioden 2013 - 2016

Statoil benyttet i perioden 2013 til 2016 en metode for å vurdere security risiko som, vist til over, baserer seg på faktorene trussel, konsekvens og sårbarhet. Metoden blir omtalt som trefaktormodellen, er tilnærmet lik metoden beskrevet i NS5832 (Egeli, 2014), men også inspirert av Department of Homland Security i USA og American Petroleum Institute (ibid). Den er i hovedsak kvalitativ, men med en kvantitativ komponent. Selve analysen ble gjennomført i en egenprodusert mal i Excel, mens dokumentasjonen ble gjort i en egenprodusert Word mal. I dokumentasjonen (Word malen) skulle også usikkerheten i analysen kommuniseres. Den baserer seg på en kvalitativ beskrivelse av komponentene trussel (scenario), konsekvens og sårbarhet, samt en subjektiv kvantitativ vurdering (fra 1 til 10) av disse komponentene. Multiplisering av faktorene gav det totale risikobildet for objektet.



Figur 6: Viser overordnet security risikoanalyseprosess (Insight: Statoil intranett)

[18] Security brochure, Insight, 2018 (Statoil intranett)

5.2.1.1 Analyseprosessen

Selve analyseprosessen bestod i tre deler. I den første delen ble det fysiske objektet beskrevet, sammen med dokumentasjon om hvem som hadde bidratt i prosessen og hva som er informasjonsgrunnlaget for analysen. I del to ble den identifiserte trusselen detaljert beskrevet, basert på fem kategorier. Kategoriene beskrev trusselens tilstedeværelse, evne, tidligere hendelser *(past targeting*), intensjon og antatt fremtidige hendelser (*anticipated future targeting*). Denne trusselbeskrivelsen var igjen grunnlaget for å vurdere om trusselen var en relevant trussel for Statoil eller ikke.

Dersom trusselen ble vurdert til å være relevant ble det i del tre skrevet detaljerte scenarioer som var basert på trusselbeskrivelsen og samtidig skulle være realistiske for konteksten. Detaljerte scenarioer skulle gjøre det enklere å vurdere hva som kunne blitt verste utfall, men samtidig skulle det gi en realistisk konsekvens dersom scenarioet ble gjennomført. Det er viktig å påpeke at det er scenarioet (som vist under) og vurderingen av trusselaktørens kapasitet og intensjon i scenarioet som ligger til grunne for risikonivået, ikke trusselvurderingen i forkant. Konsekvensen (verdien) baserte seg på satte kriterier for skade og tap av menneskelig, skade på miljø og finansielt tap/skade.

Scenario number	Threat (T_1) - Scenario descriptions (A detailed narrative describing the asset-specific scenario along the 'pathway' from the origin to the target)	Scenario category	Threat factors		**Threat (T_1)**	Consequence (C_1) (What is the anticipated worst-case effect of the scenario? Indicate if there is potential for significant reputation risk.)	Consequence			**Consequence (C)**	Vulnerability (V_1) (Identify specific vulnerabilities using the 'pathway' method in terms of: - Acceptance / consent - Alternative options - Physical protection - Procedures - Profile - Redundancy - Security force integration (information, protection, response - Situational awareness / reporting)	**Vulnerability (V_1)**
			Capability	Intent			Personnel	Financial impact (loss of production, damage) in mUSD	Environment			
1.a.												
1.b.												

Figur 7. Viser utdrag av del tre i analyseprosessen (Insight, 2018)

5.2.1.2 Sårbarhetsvurderingen – Barrierestyringen

Både i veilederen og gjennom opplæring ble det poengtert at de detaljerte scenarioene skulle få frem detaljene for hvordan trusselaktøren(e) ville gå frem (*threat pathway*) og på denne måten ville en få frem hvilke barrierer som ville påvirke scenarioet. Denne informasjonen ble igjen benyttet til å gi en subjektiv vurdering av sårbarheten i form av svakheter (*weaknesses*) og/eller enkeltheten/vanskeligheten trusselaktøren(e) ville ha med å gjennomføre scenarioet. Sårbarhetsvurderingen ble basert på følgende faktorer (oversettelsen og forklaring er utført i forbindelse med skrivingen av oppgaven):

- Acceptance/consent: Vurdering av hvorvidt tilstedeværelsen til Statoil var akseptert
- Alternative options: Vurdering om det var andre mål, overføring av risiko
- Physical protection: Fysiske barrierer
- Procedures: Vurdering av egne prosedyrer som reduserte sårbarheten
- Profile: Vurdering om Statoil sin profil tiltrakk seg trusler
- Redundancy: Vurdering av redundante løsninger for å redusere konsekvensen
- Security force integration: Vurdering av sikkerhetsstyrkenes støtte i form av informasjon, fysisk beskyttelse og respondering på hendelser
- Situational awareness/report: Vurdering av de ansattes bevissthet til trusselen og rapportering av hendelser.

Vurderingen og graderingen (fra 1 til 10) på hvor stor sårbarheten var ble helt og fullt basert på analytikerens kunnskap og subjektive vurdering av alle faktorene over. Det var ingen beskrivelser som skulle rettlede analytikeren på dette området. For vurdering og gradering av trusselbeskrivelsen (de fem faktorene), scenarioenes kapasitet og intensjon, samt konsekvensvurderingen var det laget egne beskrivelser som skulle bistå analytikeren med å gradere mellom 1 og 10.

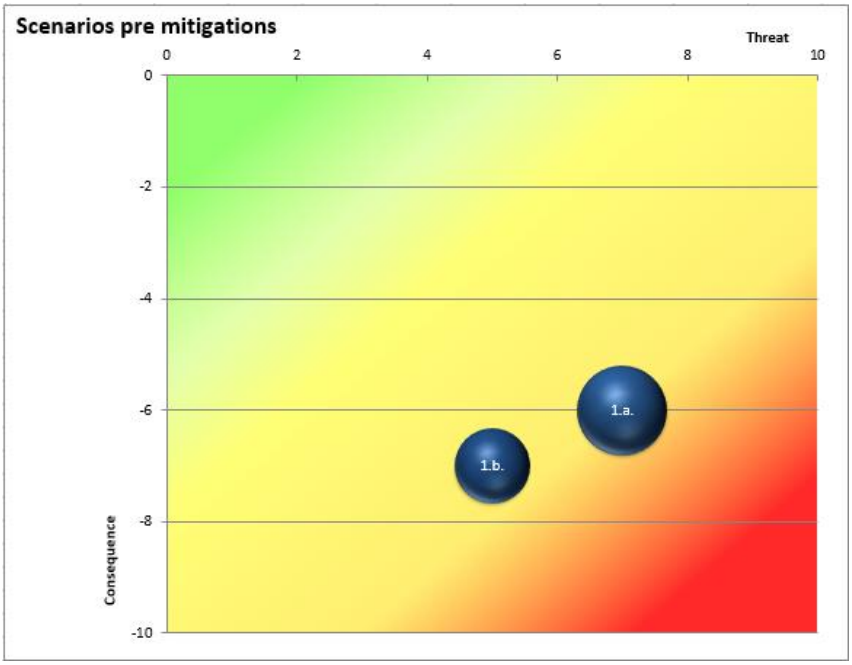
Resultatet ble konvertert til en kvalitativ bekrivelse av risikonivået (figur 8). Der hvor scenarioene avdekket sårbarheter skulle det anbefales nye barrierer og analysen ble repetert. Ut i fra analytikerens vurdering av totaliteten av nye og gamle barrierene ble fortrinnsvis sårbarheten redusert, noen gange konsekvensen og sjeldent trusselen eller intensjon i scenarioet. Prosessen ble gjentatt til det totale risikonivået var redusert til et tolerabelt nivå. I beskrivelsen av hva som er et tolerabelt risikonivå henviser veilederen både til ALARP[19] prinsippet og til at tolerabelt nivå var det nivået som risikoeieren (ansvarlige i landet eller på lokasjon) og analytikeren kom frem til.

Extreme	500 – 1,000
High	221 - 499
Medium	76 - 220
Low	1 - 75

[19] Aven. M.fl. 2008

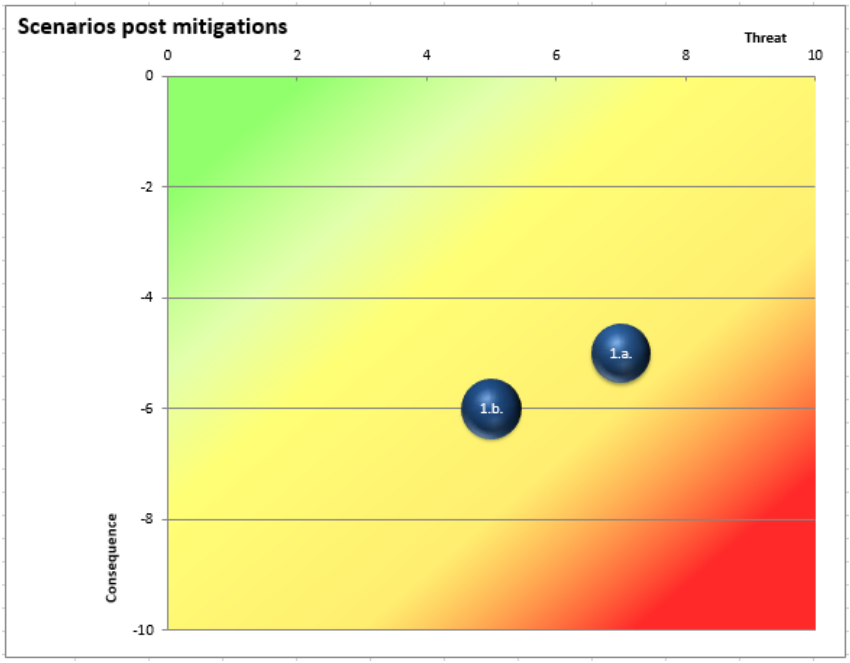
Figur 8. Viser konvertering fra kvantitativ risiko til kvalitativ beskrivelse[20]

Effekten av hver enkelt barriere ble ikke beskrevet, men den totale sårbarheten og reduksjonen i form av redusert risikonivå ble dokumentert og visualisert. Eksemplene under viser visualiseringen via et boblediagram som var integrert i malen. X-aksen visualiserer trusselen, mens Y-aksen visualiserer konsekvensen. Sårbarheten Statoil hadde ovenfor nettopp det scenarioet ble visualisert med størrelsen på boblene. I tillegg inneholder visualiseringen en fargekoding i bakgrunnen, som kjent fra risikomatriser, for å gi ytterligere informasjon om risikonivået.



Figur 9: Produsert i malen for risikoanalyse, illustrerer to scenarioer før nye barrierer er anbefalt.

[20] Veileder for Security Risiko Analyse (Statoil, 2013)



Figur 10: Produsert i malen for risikoanalyse, illustrerer de samme to scenarioer etter nye barrierer er anbefalt. Reduksjon i sårbarheten visualiseres med at størrelsen på boblene er redusert.

Den ferdige og godkjente security risikoanalysen er et av grunnlagene for sikringsplanen, som også inneholder en «State of Alert» matrise. I denne skal indikasjoner (triggere) på endringer i trusselbildet, og dermed også security risikoen, identifiseres og beskrives sammen med tilhørende nye tiltak. «Triggerne» skal hjelpe risikoeier å kjenne igjen endringer, både positive og negative, og gjøre de riktige tiltakene.

5.2.2 Tidsperioden etter 2016

Metoden som benyttes i Statoil i dag er basert på de samme prinsippene som tidligere beskrevet og selve metoden vil derfor ikke bli gjentatt her. Men det er gjort endringer vil bli belyst og vil bli redegjort for.

5.2.2.1 Forskjeller

Den første forskjellen ligger i beskrivelsen av scenarioet, som skal være forankret i trusselbeskrivelsen. Trusselbeskrivelsen er i hovedsak lik metoden før 2016, men *antatt*

fremtidige hendelser er byttet ut med *trussel trend*. En forsøker med andre ord å si noe om hvordan en tror trusselen vil utvikle seg i fremtiden. I tillegg til å være forankret i, så skal scenarioet i tillegg være dimensjonert ut av trusselen trusselbeskrivelsen. Det betyr at dersom det er identifisert en trusselaktør som i liten grad har tilstedeværelse, lav kapasitet og lav intensjon så kan ikke scenarioet være et komplekst scenario som krever høy grad av tilstedeværelse, kapasitet og intensjon til å gjennomføres. Det scenarioet som benyttes skal være det scenarioet som er sannsynlig at selskapet blir utsatt for dersom de blir utsatt for den trusselen som er identifisert. Det er ikke en vurdering av sannsynligheten for at de blir utsatt for trusselen, men hvordan og da basert på eksisterende trusselnivå og/eller det fremtidige ved å ta høyde for trusselens utvikling.

En annen forskjell mellom metodene ligger i grunnlaget for vurderingen og graderingen av scenarioet. Det blir fortsatt vurdert ut ifra kapasitet og intensjon, men intensjonsvurderingen er endret. Faktorer som tidligere ble vurdert som en sårbarhet, slik som manglende aksept for tilstedeværelse eller alternative mål som overfører risiko til andre, blir nå vurdert under intensjonen i scenarioet. I tillegg vurderes aktøren(es) motivasjon for å gjennomføre scenarioet, attraktiviteten objektet utgjør, opplevd gevinst/suksess, risiko for å mislykkes, objektets synlighet ovenfor trusselaktøren(e) og deres oppfattelse av objektets kritikalitet for Statoil. Dette utgjør intensjonen i scenarioet og vurderes helt og fullt ut ifra hvordan analytikeren mener trusselaktøren(e) vurderer dette.

I sårbarhetsvurderingen, basert på endringen over, vurderes kun de operasjonelle-, tekniske- og organisatoriske barrierene som Statoil implementerer og kontrollerer for å redusere sårbarheten mot de scenarioene som benyttes, som vist i eksemplet under.

Threat agent	Threat scenario barrier is related to	Barrier description	Functionality	How the barrier is implemented	Barrier effectiveness in scenario	Status	Comments
Terrorist	Scenario 1	CCTV	Deter, Detect	Beskrivelse av hvordan CCTV-løsningen er implementert og monitorering	Beskrivelse av effektiviteten denne barrierer har på scenarioet	Existing	Beskrivelse av sammenhengen mellom CCTV og sikkerhetsvakter
Terrorist	Scenario 1	Sikkerhetsvakter	Deter, Detect, Delay, Respond	Beskrivelse av plassering, antall og fokus/rutiner	Beskrivelse av effektiviteten denne barrierer har på scenarioet	Existing	Beskrivelse av sammenhengen mellom sikkerhetsvakter og adgangskontroll
Terrorist	Scenario 1	Adgangssperrer	Deter, Delay	Beskrivelse av adgangskontrollen	Beskrivelse av effektiviteten denne barrierer har på scenarioet	Existing	
Terrorist	Scenario 1	Innbruddsalarm	Detect	Beskrivelse av funksjonen og utrykningstid for sikkerhetsvakter eller vektere	Beskrivelse av effektiviteten denne barrierer har på scenarioet	Existing	Beskrivelse av sammenhengen mellom alarmering og reaksjon

Figur 11: Eksemplet er laget i komponenten for sårbarhetsvurdering i dagens metode (ARIS).

5.2.2.2 Barrierestyringen

Vurderingen av sårbarheten og styringen av barrierene er i dagens metode integrert i samme prosess da det er barrierene som avgjør sårbarheten. I vurderingen av sårbarheten, og som vist i eksemplet over, settes scenarioet opp mot hver enkelt barriere det «treffer». De enkelte barrierene beskrives med hvilken funksjonalitet den har, hvordan den er eller skal implementeres og hvilken effektivitet den har på nettopp det scenarioet. I tillegg beskrives (i kommentarfeltet) dersom det er avhengigheter, synergier eller mangler på sådan mellom barrierene mot det samme scenarioet. Den totale sårbarheten Statoil har for hvert enkelt scenario baserer seg på en vurdering av de enkelte barrierenes samlede effekt på scenarioet.

Basert på risikobildet for hvert enkelt scenario og det totale risikobildet for hver enkelt trusselaktør kan analytikeren anbefale nye barrierer og tiltak i den samme delen av analysen. De knyttes, som i eksemplet over, en til en mot scenarioet og gis samme beskrivelse og vurderinger. Status-kolonnen har en nedfallsmeny hvor «anbefalt» settes på alle nye barrierer og tiltak. Deretter gjøres det en ny vurdering av den samlede sårbarheten, basert på både eksisterende og nye barrierer.

Det er den enkelte risikoeier, slik som beskrevet over, som beslutter hvilke tiltak som skal godkjennes og således bestemmer hva som er tolerabelt nivå for security risiko. Dette fremgår både av styrende dokumentasjon[21] og igjennom analyseprosessen. Den ferdige godkjente analysen lagres både lokalt og sentralt i selskapet.

Det er den enkelte risikoeier som er ansvarlig for å sørge for at tiltakene blir implementert på en slik måte at de oppnår den effekten som er beskrevet i analysen. Ofte settes det ned egne prosjekter som skal sørge for å identifisere de riktige komponentene som gir den effektiviteten som er beskrevet i analysen. I denne fasen, hvor nye tiltak implementeres, benyttes fortsatt komponenten for barrierebeskrivelse. Nedfallsmenyen i status-kolonnen har flere valgalternativer som kan benyttes igjennom hele prosessen fra security risikovurdering, via beslutningsprosessen, til endelig implementering. Alternativene beskriver nåværende status på barrierene og er som følgende: *Eksisterende*, *anbefalt*, *godkjent*, *avvist*, *dekket* (tidligere beskrevet i annet scenario) og *implementert*. Barrierebeskrivelsen i vurderingen viser i utgangspunktet et oppdatert bilde på barrierestatus.

[21] «Håndtering av security risiko» (Prosess SF-501): ARIS

Resultatene oppsummeres på første side. Der er det informasjon om hvem som er risikoeier og hvem har gjennomført analysen, hva er eksisterende risikonivå (HR1, høyeste risikoscenario), hva kan oppnås med nye barrierer (HR2) og hvilket nivå har risikoeier besluttet er tolerabelt nivå (HR3). I tillegg listes alle identifisert trusler og vurderingen, de tre høyeste scenarioene innen hver trusselaktør og en oversikt over alle barrierene som er godkjent eller avvist av risikoeier.

5.3 Styringssystemet i Statoil

Styringssystemet i Statoil presenteres og organiseres gjennom verktøyet kalt ARIS (Insight, 2018)[22]. Statoilboken[23] er en del av styrende dokumentasjon og beskriver videre både hensikt og oppbygging av styringssystemet. Systemet er et sett med prinsipper, policyer, prosesser og krav som skal støtte organisasjonen i å nå sine mål via sikre og effektive operasjoner, redusere risiko og spare tid og kostnader. Et viktig verktøy som er fremhevet i styrende dokumentasjon for å tilrettelegge for risikostyring i all aktivitet er Etterlevelse & Ledelse[24]. Styringssystemet er hierarkisk og består av tre nivåer, *grunnprinsipper*, *krav* og *anbefalinger*. *Grunnprinsippene* er gjeldende uavhengig av hvor en jobber og uten unntak. Men *krav* gjelder for spesielle områder av selskapet. Her er det de ulike virksomhetene som er ansvarlig for å etablere og implementere styringssystemet som er tilpasset den enkelte forretnings operasjon og kontekst. *Anbefalinger* er støttedokumentasjon som skal bidra til at kravene etterleves på mest mulig effektiv måte. Etterlevelse av styringssystemet er et krav for alle som arbeider for Statoil. Det gjelder med andre ord ikke bare for de ansatte, men også kontraktører og leverandører. Styringssystemet er en viktig organisatorisk barriere som legger rammer for styring av selskapets hele aktivitet og ressurser.

5.3.1 Metodens forankring i Styringssystemet

Håndtering av security risiko er en egen prosess i styrende dokumentasjon i Statoil[25]. Prosessen har en klart definert hensikt: *forhindre at Statoil har et security risikonivå mot*

[22] Statoil intranett
[23] www.statoil.com
[24] Statoilboken (www.Statoil.com)
[25] SF-501 Manage security risk, ARIS

personell, miljø og verdier som ikke er tolerabelt. Prosessen setter krav til når det skal gjennomføres security risikoanalyser. Det første kravet er allerede i designfasen, når et nytt konsept utvikles for en lokasjon, plattform eller et anlegg, samt en ny eller oppdatering når byggingen er ferdig og klar til bruk. Prosessen setter videre krav om oppdatering eller nye security risikoanalyser basert på tidsfrekvens oppimot risikonivå og på grunnlag av endringer. Dersom trusselen endrer seg eller objektet endres seg på grunn av endret eller økt aktivitet krever prosessen at en ny vurdering gjennomføres. Prosessen setter i tillegg krav til involvering av funksjoner, slik som IT, HR, anskaffelse og logistikk, for å sikre både kompetanse og kunnskap inn i analysen. Prosessen forankrer beslutningsmyndigheten til hva som er tolerabelt risikonivå til linjen i organisasjon og til den som er risikoeier for lokasjonen, land eller region. Videre ligger det et mandat til å beslutte hvordan tiltakene operasjonaliseres gjennom prosedyrer og instrukser, som igjen er knyttet oppimot beredskapshåndteringen[26] og organisering av beredskapsorganisasjonen i Statoil. Beredskapsorganisasjonen i selskapet er basert på tre nivåer eller linjer. Første beredskapslinje (*Emergency Response Team*) er de ressursene som fysisk håndterer hendelsen lokalt hvor hendelsen skjer. Når de mobiliseres får de full beslutningsmyndighet til hvordan hendelsen håndteres. Andre beredskapslinje (*Incident Management Team*) skal koordinere og støtte første linje. Tredje beredskapslinje (*Crisis Management Team*) finnes det bare ett av i selskapet og har det strategiske ansvaret for håndtering av hendelser.

Metodikken for hvordan security risiko analyseres, som barrierestyringen er en del av, er forankret inn i den samme prosessen og som beslutningsgrunnlag for hva som er tolerabelt risikonivå. Styrende dokumentasjon[27] setter i tillegg krav til å kommunisere risikonivå opp i organisasjonen dersom barrierer og tiltak ikke reduserer risikoen tilstrekkelig. Statoil har i tillegg et eget system (MIS[28]) hvor all risiko rapporteres og er synlig for hele organisasjonen. Her løftes risiko i linjen, men kan og synliggjøres på tvers av forretningsområdene.

Konsernsikring i Statoil har produsert et eget analyseverktøy som samler all informasjon fra alle sentralt lagrede security risikoanalyser og som er basert på den metoden som benyttes i dag. Verktøyet kan filtrere informasjonen ut i fra brukerens behov. For konsernledelsen kan det for eksempel visualisere det totale security risikonivået i Statoil, per dags dato, innenfor et

[26] SF-700 Preparedness and response (ARIS)
[27] RM-100 Risk Management (ARIS)
[28] Insight (Statoil intranett)

forretningsområde, region eller land. Den kan også filtrere på tvers av alle analysene etter trusselaktører, type scenario, barrierer eller status på barrierer.

5.4 Analyse av security risikoanalyser i Statoil

Dette delkapitlet inneholder det jeg har funnet relevant fra analyse av 12 security risikoanalyser utfør i Statoil i perioden 2013 til 2018. Security risikoanalysene er utført for objekter spredd over hele verden og fordeler seg likt på de to metodene beskrevet over. Analysene inneholder totalt 71 identifiserte security trusler, basert på definisjonen over, noe som betyr at det er samme type trussel identifisert flere steder, for eksempel terrorisme. Videre inneholder, samlet, security risikoanalysene 158 scenarioer som beskriver hvordan Statoil kan bli eksponert for de identifiserte truslene.

Security risikoanalysene er analysert gjennom kartlegging av samtlige 158 scenarioer og de tilhørende opplysningene i sårbarhetsvurderingen i de to tilnærmingene. Veiledning og opplæring, for begge metodene, viser til at detaljerte scenario som beskriver handling, metode og «threat pathway» gir bedre grunnlag for å vurdere en mest mulig korrekt konsekvens og sårbarheten ovenfor det beskrevne scenario. Resultatene blir derfor i hovedsak presentert i relasjon til scenarioene. Først vil analyse av scenarioene bli beskrevet, deretter presenteres resultatene av analyse av sårbarhetsvurderingene i perioden før 2016 og perioden etter 2016 og til slutt sees disse resultatene opp mot hverandre.

5.4.1 Scenarioene

Det er stor variasjon i detaljnivået i de analyserte scenarioene. Noen av scenarioene er skrevet med stor grad av detaljer som legger til grunne både antakelser og hendelser, samt planlegging som strekker seg flere måneder tilbake i tid som forberedelser for handlingen. De beskriver hvordan trusselaktøren(e) tenker og vurderer situasjonen mens det «skrir frem». Andre scenarioer er mer korte og konsise, men som likevel inneholder en klar beskrivelse av antall aktører, utstyr, fremgangsmåte og viser til hvilken intensjon aktøren(e) har med handlingene. Begge typene er scenarioer som gir grunnlag for å vurdere både konsekvens og sårbarhet. Det er 158 scenarioer og 82 av dem er fra perioden før 2016, mens 76 er fra

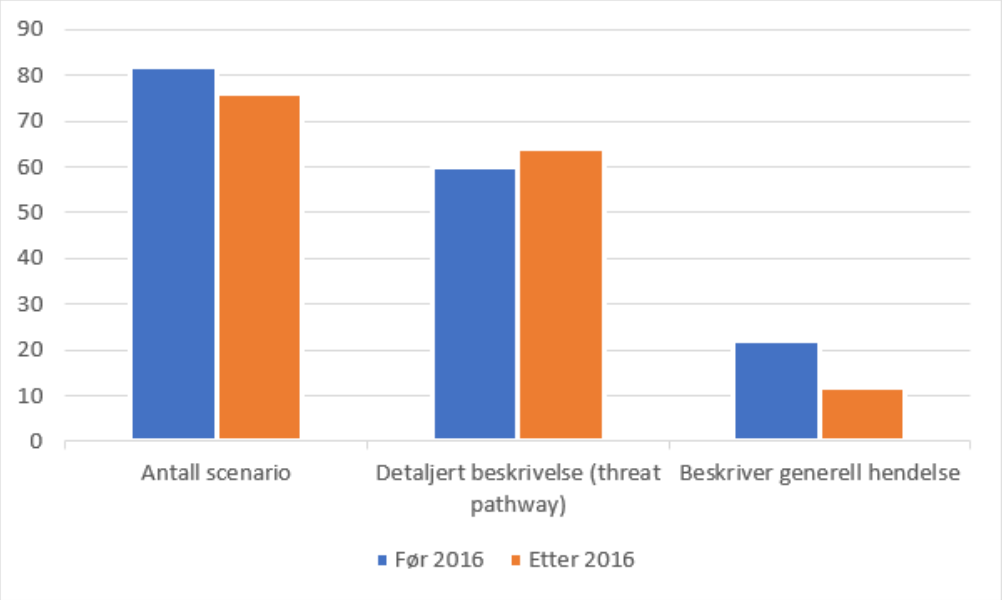
perioden etter og frem til 2018. Analyse av disse scenarioene viser at 126 av de totalt 158 scenarioene inneholder beskrivelser som vist til over. 60 av disse scenarioene er fra før 2016, mens 64 er fra perioden etter 2016, som visualisert i under (figur x). Scenarioene er kategorisert som: Detaljerte beskrivelser.

> *En liten gruppe, 3-5 personer, ankommer kontorbygningen i to kjøretøy. De tar seg inn på området ved bruk av eksplosiver og håndvåpen, for deretter å ta seg inn i bygningsmassen igjennom hovedinngangen med bruk av samme middel og med intensjon om å angripe ansatte.*[29]

De resterende 34 scenarioene fordeler seg på 22 fra perioden før 2016 og 12 fra perioden etter. Disse har enten en manglende beskrivelse av en tydelig «threat pathway» og/eller har en manglende beskrivelse av trusselaktøren(e), fremgangsmåten, utstyr og intensjon. De gir likevel en viss forståelse av hva selskapet kan bli utsatt for. Scenarioene har en varierende grad av informasjon i scenarioene. De korteste scenarioene kan for eksempel være av typen: «*Ansatt utsatt for kriminalitet, tyveri, ran eller vold på utested*». Scenarioene i seg selv forteller at det er en ansatt som blir ranet, utsatt for vold eller tyveri. Men ut over dette gir ikke scenarioene informasjon om hvordan dette skjer eller hvor mange gjerningspersoner som er involvert. De beskriver heller ikke hvorvidt det benyttes noen form for våpen eller om hendelsen er relatert til spesifikke steder eller lokasjoner, samt tid på døgnet. I denne samme kategorien er det også beskrevet mer «*kompliserte*» scenarioer. Disse scenarioene viser til at en trusselaktør kan ved bruk av multiple metoder oppnå intensjonen sin. Scenarioene beskriver ikke alle alternativene, men viser til at trusselaktøren *kan* bruke mange alternativer og beskriver da to tre av disse. Det tas med andre ord høyde for en aktør som benytter metoder som ikke er beskrevet. I tillegg beskrives det i ett og samme scenario at aktørene benytter de forskjellige metodene på forskjellige objekter, slik som personer, kontorer og teknologiske enheter.

[29] Egenprodusert eksempel på scenario, basert på kunnskap fra analyseresultatet

Trusselaktøren bruker et bredt spekter av modus operandi, som kan inkludere metoder som kultivering, forskjellige måter for avlytting og phishing-epost[30] for å stjele sensitiv informasjon.[31]



Figur 12. Viser fordelingen av scenarioer, egenprodusert.

Det antallet scenarioer som er undersøkt fordeler seg forholdsvis likt, henholdsvis 82 og 76 på perioden før og etter 2016. Hvis vi ser videre på det prosentvise antallet scenario innenfor hver periode som er kategorisert som detaljerte beskrivelser er det 11% flere detaljerte beskrivelser etter 2016.

5.4.2 Sårbarhetsvurderingene i perioden før 2016

Det fremgår i empirien over at eksisterende barrierer og tiltak skulle vurderes i sårbarhetsvurderingen slik at det kunne anbefales nye barrierer og tiltak. Men metoden legger også opp til at flere aspekter enn kun barrierer skulle vurderes og analyse av sårbarhetsvurderingen for 82 scenarioer bekrefter dette. Det vil derfor først beskrives noen generelle funn som er fremkommet gjennom denne analysen. Deretter vil resultatene av analyse av barrierer og tiltak i sårbarhetsvurderingene beskrives.

[30] Falsk e-post sendt til deg for å «fiske» etter sensitiv informasjon, www.nettvett.no
[31] Egenprodusert eksempel på scenario, basert på kunnskap fra analyseresultatet

Det er stor grad av variasjon i sårbarhetsvurderingene, både med tanke på hvordan de er skrevet og hvilken type informasjon som er tatt med. Det er sårbarhetsvurderinger som tar utgangspunkt i det beskrevne scenarioet, for deretter å beskrive alle barrierene som er på plass og som vil kunne påvirke resultatet av scenarioet. Det gis underveis en vurdering av de barrierene som er beskrevet, en beskrivelse av hvordan barrierene fungerer og hvorvidt de er tilknyttet andre barrierer. Dette kan for eksempel være alarm og respons, fjernåpning av noen dører via video kontroll og muligheten for nødstenging av andre dører og evakuering. Evakueringsmuligheter og alternativer blir beskrevet, samt hvilke tiltak som reduserer sårbarheten igjennom evakueringen. Det gis en vurdering av svakheter og styrker i de forskjellige tiltakene og hvorvidt de gir forsinkelse nok til trygg evakuering. Videre anbefales det nye tiltak som skal redusere de svakhetene som er beskrevet i tiltakene og det gis en vurdering av i hvor stor grad den totale sårbarheten er redusert. I tillegg pekes det på eksisterende sårbarheter som ikke har latt seg redusere og at dette i noen grad kan kompenseres for gjennom trening og øvelse, men at det vil ha sine begrensninger. Det gis et tydelig bilde på hva som er på plass, hvordan det fungerer, hva en kan forvente og hvilke sårbarheter som ikke har latt seg redusere.

I en av de undersøkte enhetene er det flere strukturerte scenarioer. De beskriver en tydelig «threat pathway» og barrierene beskrives oppimot denne. Det gis en anbefaling på nye barrierer og tiltak som skal redusere sårbarheten som er beskrevet i forbindelse med de eksisterende barrierene. I et senere scenario og sårbarhetsvurdering, i samme undersøkte enhet, anbefales det også nye barrierer, men for dette siste scenarioet. Likevel poengterer analytikeren som har gjennomført vurderingen at de anbefalte barrierene for det siste scenarioet også vil kunne redusere sårbarheten i det tidligere nevnte scenarioet dersom de blir implementert. Analytikeren har med andre ord sett en total sammenheng mellom noen scenario og barrierene som er anbefalt.

Graden av annen informasjon beskrevet i sårbarhetsvurderingene, for eksempel om det er vurdert alternative mål som overfører risiko eller aksept for selskapets tilstedeværelse i området, er i liten grad tilstede der hvor graden av barrierebeskrivelser er høy.

I de sårbarhetsvurderingene hvor graden av beskrivelser av barrierer er lav eller svært lav, er graden av annen informasjon større. Informasjonen er fortsatt relevant og i henhold til hvordan metoden var for den perioden. I disse enhetene er det i liten grad informasjon som

beskriver hvorvidt det lokalt er aksept (*acceptance*[32]) for selskapets tilstedeværelse eller aktivitet. I de undersøkte enhetene er det derimot flere eksempler på vurderinger av selskapets profil som for eksempel beskriver selskapets kontor som relativt lite og anonymt i en større by hvor det er stor tetthet av andre energiselskap som både er større (internasjonal tilstedeværelse) og mer synlig i det lokale bybildet. Vurderingen er videre at dette reduserer sårbarheten Statoil har for den type scenario som er beskrevet. Profil handler ikke kun om merking av kontorbygg eller synlighet, det handler også om hvilken type aktivitet selskapet er kjent for og hvordan selskapet utøver denne aktiviteten. Det er i tillegg eksempler hvor det er vurdert at andres profil overfører risiko til Statoil.

Den x ambassade leier hele 5. etasje i samme bygg som Statoil og benytter den samme hovedinngangen og heisene som Statoil. På grunn av deres geopolitikk vil de i større grad enn Statoil tiltrekke seg oppmerksomhet og fokus fra denne trusselaktøren. Dette gjør Statoil sårbar.[33]

Vurdering eller beskrivelse av at sårbarheten er redusert på grunn av redundante løsninger er ikke funnet i det undersøkte materialet.

Men i to av de undersøkte enhetene er det funnet sårbarhetsvurderinger som inkluderer informasjon om sikkerhetsstyrker eller nasjonale politistyrker, hvor det vises til deres tilstedeværelse, kvalitet og hva som er forventet responstid. I en enhet ble lokalbefolkningens årvåkenhet ovenfor trusselaktøren og kultur for å rapportere til myndighetene beskrevet i sårbarhetsvurderingen. I begge tilfellene ble det vurdert til å redusere selskapets sårbarhet, i tillegg til barrierer.

I noen få[34] tilfeller er informasjon i sårbarhetsvurderingen ikke relevant. Det gis ingen beskrivelser hvorvidt selskapet er sårbar for det beskrevne scenarioet. Det gis heller ingen beskrivelser av eksisterende barrierer eller foreslås nye. Det er ingen informasjon for å vurdere sårbarheten og det er heller ingen vurdering av sårbarheten. Det benyttes kun en gradering, fra 1 til 10, for hva analytikeren mener sårbarheten er. De undersøkte enhetene dekker objekt(er) hvor det er eksisterende barrierer.

---

[32] Dette (*acceptance*) er et kjent begrep i den humanitære sektoren og brukes som strategi for å redusere risiko mot ansatte og mottakere av hjelp. De søker å opparbeide en aksept fra lokalbefolkning eller trusselaktører for at deres tilstedeværelse og dermed unngår å bli et mål. www.eisf.eu.
[33] Deler av en sårbarhetsvurdering fra en av de undersøkte enhetene.
[34] Fire tilfeller funnet i det undersøkte datagrunnlaget

Informasjonen i disse tilfellene er av generell karakter. Den beskriver trusselbildet og trusselkarakteren, slik som i andre del av prosessen, og det gis informasjon om hva som kan endre dette bildet. Det gis informasjon om geopolitiske forhold og hvilke faktorer som kan endre dette bildet, uten at det beskrives hvordan dette påvirker selskapet.

I perioden etter 2016 utgjør eksisterende og anbefalte nye barrierer sårbarhetsvurderingen. Den vil derfor ikke bli gjennomgått på lik linje med sårbarhetsvurderingen før 2016.

5.4.3 Effekten av utviklingen

I dette kapitlet beskrives hvilken informasjon som fremkom i sårbarhetsvurderingene gjennom analyse av forskjellige typer scenario. Det er viktig og igjen påminne leseren at oppgaven og analysene ikke ser på risikonivået i Statoil og derfor heller ikke svarer på om risikoen er høyere eller lavere nå enn før. For å strukturere informasjon vil funnene bli presentert i relasjon til scenarioene.

5.4.3.1 Strukturerte scenarioer før 2016

Analyse av 82 scenario fra perioden før 2016 viser at 60 av dem var skrevet detaljert og gav en forståelse av hvordan trusselaktør(ene) ville gå frem, såkalt *threat pathway*. I 46 av disse (60) er det beskrevet barrierer eller en prosedyre som er knyttet til *threat pathway*. De er identifisert ut i fra hvordan trusselaktøren(e) går frem.

Ved å se nærmere på selve barrierebeskrivelsene i de 46 scenarioene som har en tydelig beskrevet *threat pathway* er det kun i 37 av dem hvor en finner tydelige beskrivelser av selve barrierene. Her ble det lagt til grunne at barrierene var beskrevet og forklart på en slik måte at det er tydelig hva det var. I en enhet ble det for eksempel beskrevet at det var implementert prosedyrer og tiltak for å redusere sårbarheten ved transport, men det var ingen beskrivelse av verken tiltakene eller prosedyrene. Dette funnet ble ikke regnet blant de 37. I en annen enhet, hvor det også ble belyst risiko ved transport, ble det funnet beskrivelser av tiltakene og prosedyrene. Det ble beskrevet hvordan kommunikasjon mellom objektene skulle være, samt hva og når det skulle kommuniseres, det ble lagt vekt på viktigheten av bevissthet på andres bevegelser i bybildet, rutiner ved inn og utpassering av porter var beskrevet og at dører og vinduer skulle være lukket og låst under transport. Dette er et funn blant de 37. I det samme

utvalget, på 37, er det beskrevet barrierefunksjoner i 35 av dem og som da dekker funksjonene avskrekke, oppdage, forsinke og respondere eller gjenopprette.

Videre er barrierer beskrevet som flere lag med beskyttelse, som kan gi en form for *forsvar i dybden*, i 29 av de 46 scenarioene og da rettet mot å begrense sårbarheten for nettopp det scenarioet. I de 29 scenarioene var det beskrevet en klar sammenheng eller en form for aktivering mellom lagene av barrierer i 27 scenarioer. Denne sammenhengen kan være mellom kun to eller tre av alle barrierer i samme scenario. Innbruddsalarm på vinduer, overvåkning av alarmen i en vaktsentral og sikkerhetsvakter som skal respondere når de blir varslet av vaktsentralen er eksempler som er funnet. Videre er det beskrevet sammenheng mellom barrierer som automatisk skal detektere bevegelse (CCTV[35]), dette skal gi en alarm som sikkerhetsvakter skal identifisere og verifisere via monitorer for deretter eventuelt å nødstenge via fjernstyring og varsle ansatte.

Knyttet til 33 scenarioer, av de totalt 60 som var detaljert beskrevet, ble det funnet beskrivelser for hvordan eksisterende barrierer var implementert eller nye barrierer skulle implementeres. Disse 33 funnene er alle i de same 37 funnene over. I disse 33 tilfellene er det for eksempel funnet detaljerte beskrivelser av type kamera som skal benyttes for overvåkning av et objekt, hvor mange kamera som trengs for å gi den dekningen analytikeren mener er behovet og hvordan overføringen av bildene skal overvåkes og hvor. Det er i tillegg gjort 3 funn hvor det er beskrevet hvilken ytelse (ytelseskrav) barrieren har eller skal ha. Et eksempel er at det ble beskrevet i forbindelse med anbefaling av et nytt tiltak at dette tiltaket ville forsinke utviklingen av scenarioet nok til at en evakuering kunne gjennomføres.

5.4.3.2 Generelle handlingsscenario

Det ble funnet 22 scenarioer som ikke er omtalt som detaljerte scenarioer. Disse, som forklart tidligere, har en generell beskrivelse av en hendelse og har ikke en tydelig beskrevet *threat pathway*. Det er funnet beskrivelser av barrierer i 7 av sårbarhetsvurderingene og i 4 av disse 22 scenarioene er det funnet at barrierene er beskrevet på en slik måte at de er vurdert til at de dekker scenarioet slik det er beskrevet. I de resterende 15 scenarioene er det funnet at det beskrives at fysiske barrierer er på plass, uten at selve barrierene beskrives. Det er også

[35] Eng. closed-circuit television

funnet beskrevet at selskapet er sårbar og at barrierene må forsterkes eller forbedres, uten at det gis beskrivelse av hvilke barrierer eller hvordan.

I de 4 scenarioene er det funnet ett tilfelle hvor barrierene er beskrevet på en slik måte at de utgjør en form for forsvar i dybden, mens det i 3 av de 4 er beskrevet sammenhenger eller en form for aktivering mellom to barrierer.

Det er funnet ett tilfelle hvor barrierefunksjonene til barrierene er beskrevet, mens det i 6 av sårbarhetsvurderingene er beskrevet hvordan barrierene er eller nye skal implementeres. Det er ikke beskrevet ytelseskrav i noen av sårbarhetsvurderingene knyttet til scenarioene.

5.4.3.3 Strukturerte scenarioer etter 2016

Det er analyser 76 scenarioer og tilhørende sårbarhetsvurderinger fra perioden etter 2016, hvor det er benyttet den nye metoden for sårbarhetsvurdering.

Analyse av disse (76) scenarioene viser at 64 av dem er detaljert beskrevet og gir en god forståelse av *threat pathway*, altså hvordan trusselaktøren(e) vil gå frem for å gjennomføre handlingen.

I samtlige av de 64 scenarioene er det beskrevet barrierer og det er oppgitt hvilken funksjon de forskjellige barrierene har. Ved å se nærmere på strukturen av barrierene i hver enkelt sårbarhetsvurdering er barrierene i 48 av dem tydelig identifisert og beskrevet i henhold til fremgangsmåte beskrevet i scenarioet. Det er videre funnet beskrivelser av sammenheng mellom to eller tre barrierer eller en form for aktivering av neste barriere i 44 av sårbarhetsvurderingene. Sammenhengene her er tilsvarende som vist til for perioden før 2016 og eksemplifiseres derfor ikke. I 42 av sårbarhetsvurderingene er det beskrevet lag med barrierer som utgjør en form for *forsvar i dybden* og dekker funksjonene *avskrekke, oppdage, forsinke* eller *respondere*. Funksjonsbeskrivelsen av barrierene er forhåndsdefinert og analytikeren har ikke mulighet til å endre dette. Funksjonsbeskrivelsen *gjenoppretting* er ikke et av valgene i denne menyen.

Videre er det funnet beskrivelser av hvordan barrierene enten er implementert eller hvordan nye barrierer skal implementeres i 50 sårbarhetsvurderinger knyttet til de 64 scenarioene. I et funn er det beskrevet sikkerhetsvakters tilstedeværelse, både med tanke på antall og tid på døgnet. Det er videre beskrevet hvordan gjerde er satt opp og fungerer som perimeter, samt

antall videokamera som dekker perimeteret og hvor og hvordan dette overvåkes. I et annet funn er kompetanse og trening oppgitt som barriere og det beskrives hvilke interne kompetanseinitiativ som må gjennomføres for å oppnå denne kompetansen og det beskrives type øvelser som må gjennomføres.

Ytelseskrav er ikke en beskrivelse som «kreves» i metoden som er benyttet etter 2016. Det er gjort funn i 12 sårbarhetsvurderinger av beskrivelser i implementeringen som setter krav til ytelsen i barrieren. Det er funnet beskrevet krav til sikkerhetsvakter og hva de skal kunne gjøre, det er beskrevet hva enkelte fysiske barrierer skal tåle og det er beskrevet hva som skal kunne detekteres ved kameraovervåkning uavhengig av vær vind og lysforhold.

5.4.3.4 Generelle handlingsscenario etter 2016

For denne tidsperioden er det funnet 12 scenarioer som ikke er beskrevet som detaljerte scenarioer og heller ikke har en tydelig *threat pathway*. I samtlige tilhørende sårbarhetsvurderinger er det beskrevet barrierer.

Ved undersøkelse av den enkelte barrierebeskrivelse er det i 6 av sårbarhetsvurderingene beskrevet barrierer slik at de er vurdert til å dekke scenarioet. Det er videre funnet beskrivelser av sammenheng mellom barrierer eller aktivering av neste barriere i 5 av sårbarhetsvurderingene, slik som tidligere beskrevet. Det er i 1 av 12 sårbarhetsvurderinger funnet beskrivelse av flere lag med barrierer og på en slik måte at det utgjør en form for *forsvar i dybden*.

Barrierefunksjonen til barrierene er beskrevet i 7 av sårbarhetsvurderingene for de 12 scenarioene, mens det er tydelige barrierer i 6 av de 12 sårbarhetsvurderingene. Barrierene er beskrevet som «*revidering av prosedyrer*» og «*generell bevissthet*» og er derfor ikke kategorisert som tydelige barrierer. I 7 av sårbarhetsvurderingene er det beskrevet hvordan barrierene er eller nye barrierer skal implementeres. Det er ikke beskrevet ytelseskrav i noen av sårbarhetsvurderingene knyttet til scenarioene.

5.4.3.5 Barrierenes effektivitet

I dagens metode for sårbarhetsvurdering skal også den enkelte barrierens effektivitet og barrierenes totale effektivitet i å redusere sårbarheten vurderes. Det er funnet beskrivelser av både den enkelte barrierens effektivitet og den totale effektiviteten av alle barrierene i alle sårbarhetsvurderingen med unntak av sårbarhetsvurderinger knyttet til 5 scenario. Her er ingen informasjon gitt.

Beskrivelsene av de enkelte barrierenes effektivitet i sårbarhetsvurderingene varier i noen grad. De enkleste beskrivelsene angir kun effektiviteten i form av grad, slik som lav, medium, høy eller god effekt. Effektiviteten er også vurdert ved at det beskrives hvordan barrieren fungerer, det kan være en prosedyre eller rutiner som forklares, og på den måten vises det til hvorfor den har effekt på nettopp det scenarioet.

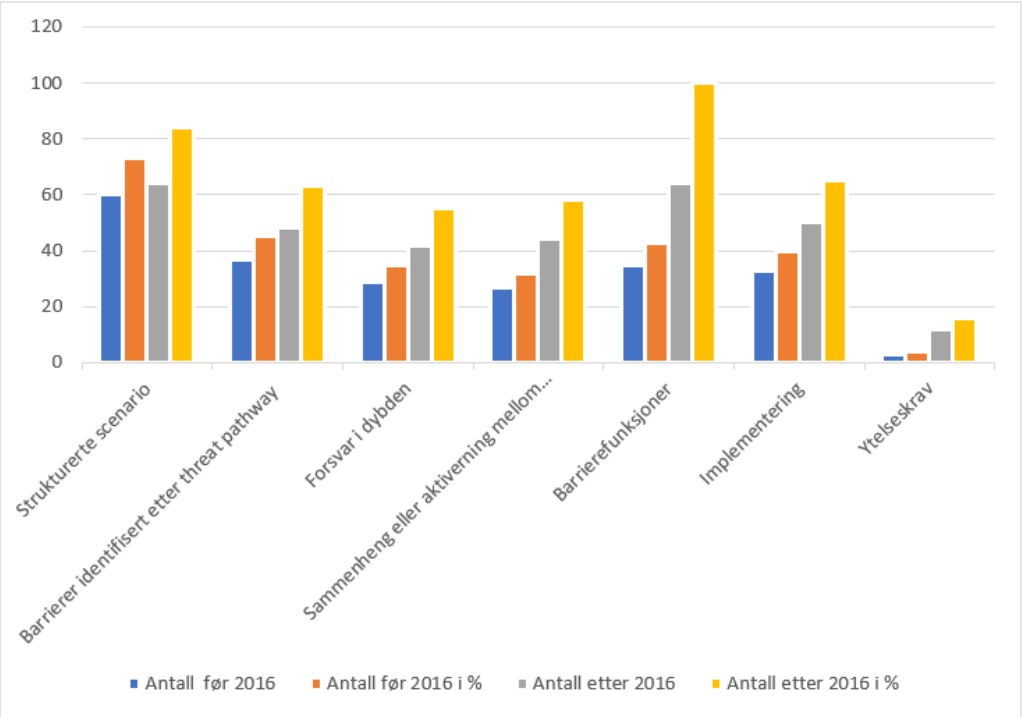
Det er også funnet mer komplekse vurderinger av effektiviteten. I noen tilfeller blir det vurdert både hvor effektiv barrieren er i å oppnå den funksjonen den er gitt, for eksempel det å oppdage en trussel, samt hvilken effekt dette har på det enkelte scenarioet i form av å kunne gi tidlig varsling om hendelsen. I disse mer komplekse vurderingene er det også belyst hva som skal til for at for at «*scenarioet*» omgår en eller flere barrierer.

5.4.4 Oversikt av resultatene

I dette kapitlet er resultatene fra analysene av bruken av metodene samlet. Dette er for å gi leseren en enklere oversikt. Det totale antall scenarioer og sårbarhetsvurderinger som er analysert er 158 og fordeler seg forholdsvis likt på de to periodene. 82 er fra perioden før 2016 og 76 er fra perioden etter.

5.4.4.1 Strukturerte scenario

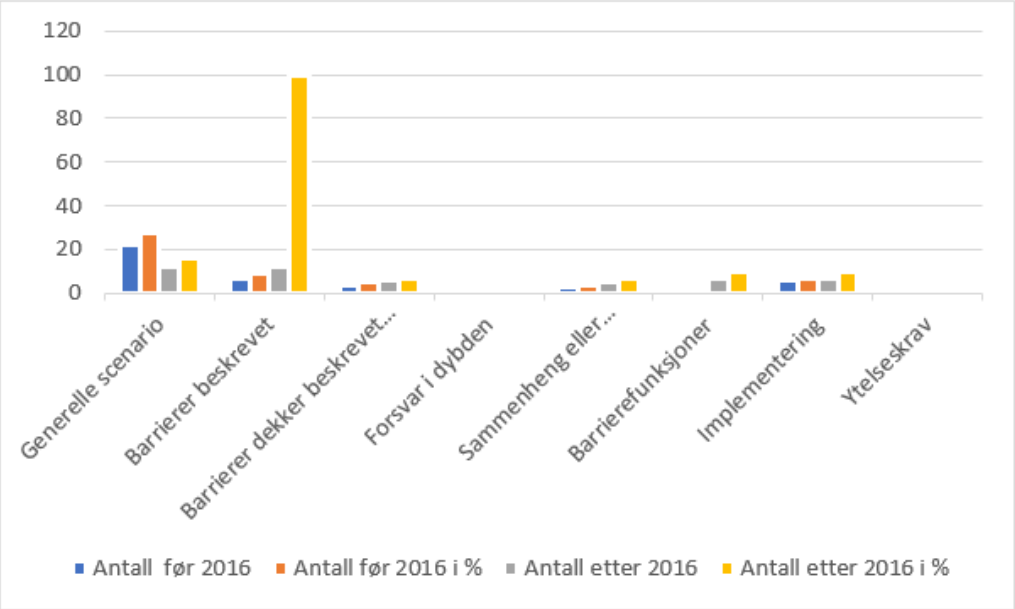
I tabellen under er det tatt utgangspunkt i antall scenarioer fra hver periode og visualisert den samme analyseringen av informasjon som er beskrevet tidligere. Tabellen tar utgangspunkt i antall strukturerte scenarioer (*threat pathway*) av totalen innen sin periode. Den prosentvise fremstillingen er basert på totalen av scenarioer innenfor sin periode.



Figur 13: Egenprodusert, visualiserer analyse av strukturerte scenario. Antall i prosent er basert på antall innen egen tidsperiode.

5.4.4.2 Generelle handlingsscenario

I tabellen under er det tatt utgangspunkt i antall scenarioer fra hver periode og visualisert den samme analyseringen av informasjon som er beskrevet tidligere. Tabellen tar utgangspunkt i antall generelle handlingsscenarioer (uten en tydelig *threat pathway*) av totalen innen sin periode. Den prosentvise fremstillingen er basert på totalen av scenarioer innenfor sin periode.



Figur 14: Egenprodusert, visualiserer analyse av generelle scenario. Antall i prosent er basert på antall innen egen tidsperiode.

6 Drøfting

I denne delen av oppgaven vil de teoretiske bidragene som er presentert i kapittel 3 bli drøftet oppimot de empiriske funnene. Kapittelet er strukturert etter forskningsspørsmålene og er således tre-delt. Første delkapittel vil omhandle metodens utvikling, mens det andre delkapittelet fokuserer på forankringen i styrende dokumentasjon. I tredje delkapittel vil de empiriske funnen av effekten av utviklingen bli diskutert. Med dette som bakgrunn vil problemstillingen bli besvart i siste kapittel.

6.1 Hvordan har metoden for styring av barrierer mot tilsiktede uønskede hendelser utviklet seg siden 2013?

Mine funn viser at da Statoil endret metodikken for security risikoanalyser i 2013 gikk de i retning av standardisering. De valgte å benytte en metode hvor security risiko er definert som et uttrykk av relasjonen mellom trussel, konsekvens og sårbarhet, ofte kalt trefaktormodellen. Metodisk er den lik NS 5832, men inspirert av andre ble den tilpasset. I 2016 ble det på nytt gjort endringer i metodikken. Fortsatt er metodikken lik NS 5832 og definisjon for å uttrykke security risiko ble det samme, men endringene var basert på egne erfaringer. De metodiske valgene Statoil har gjort siden 2013 virker å være i tråd med hva flere av forskerne i FFI-rapport 2015/00923 uttrykker. Den konkluderer også med at det ikke finnes en fremgangsmåte eller metodikk for security risikoanalyser, internasjonalt eller nasjonalt, som det er felles enighet om. De overordnede tilpasningene og operasjonaliseringen av metodikken følger, i all hovedsak, konklusjonen i rapporten om hva som kjennetegner en god tilnærming. Men ett unntak her er at metoden som ble tatt i bruk fra 2016 ikke tydelig kommuniserer usikkerhet[36].

Funn viser videre at det i tillegg til forskjeller i sårbarhetsvurderingen mellom metodene, som omhandles senere, så er det to forskjeller til. Den første er en tydeliggjøring av at scenarioet skal dimensjoners av trusselbeskrivelsen i security risikoanalysen og den andre er hva som ligger til grunne for vurderingen av scenarioet og henger sammen med endringen av sårbarhetsvurderingen.

[36] Tema omhandles ikke videre da bruk av sannsynlighet (usikkerhet) i metodikken er en av oppgavens avgrensninger.

Det er tydeliggjort at scenarioet skal være basert og dimensjonert etter eksisterende trusselbeskrivelsen, men samtidig er rammen for trusselbeskrivelsen «åpnet opp» ved å inkludere *trusselens trend*. Basert på egen kunnskap og tilgjengelig informasjon kan analytikere og bidragsytere mene noe om hvordan de tror trusselen vil utvikle seg i fremtiden. Dette gir igjen åpning for å benytte scenarioer ut over dagen trusselbilde og i retning av «*hva er det verste som kanskje*» scenarioer. Denne tenkningen finner vi igjen i Pidgeon & O`Leary (2000). I tillegg vil et tydelig skille på disse scenarioene, dagens situasjon og mulige fremtids-scenarioer, kunne gi risikoeier et enda bedre beslutningsgrunnlag for å håndtere security risiko. Manglende skille på hvilken type scenarioer som benyttes vil kunne gi et urealistisk høyt risikonivå, som igjen vil være svært kostnadsdrivende og dermed reduserer risikoeiers mulighetsrom til å utforske muligheter på den ene siden og det å unngå tap og skade på den andre siden. Dette er ifølge Aven (2007) essensen av risikostyring.

En security trussel er en ekstern faktor (Albrechtsen, 2003 og Jore, 2016). I trusselbeskrivelsen i begge metodene legges det til rette for å beskrive denne trusselen og da basert på de faktorene som en mener er viktige for å skrive scenarioer om hva en tror kan gå galt. Gitt at Schiefloe (2011) har rett med overføring av kunnskap og erfaring, vil Perrow (1999) tilsi at uansett hvor god beskrivelse vi har av trusselen (systemet) så vil uforutsette ting skje. De vil skje fordi en ikke har oversikt og kan kontrollere alle interaksjonene og konsekvensene av dem, noe Jore (2016) også peker på. Endringen i trusselbeskrivelsen i metoden etter 2016, *trusselens trend*, virker i større grad å legge til rette for denne tenkningen. Men samtidig er ikke det en garanti for at alle mulige fremtidige hendelser blir beskrevet eller tatt høyde for.

Vurdering og gradering av scenarioene er forskjellig mellom de to metodene på grunn av endringene i sårbarhetsvurderingen i dagens metode. I metoden som ble benyttet frem til 2016 var sårbarhetsvurderingen mer tilrettelagt for å vurdere totaliteten av hva som gjør objektet sårbart for den identifiserte trusselen. Den begrenset seg ikke kun til interne faktorer, men så også på eksterne faktorer som kunne påvirke objektets sårbarhet eller forenkle trusselaktøren(es) scenario. Når en legger til grunne at det skulle skrives detaljerte scenarioer for hvordan trusselaktøren(e) ville gå frem vil denne tilnærmingen kunne gi en total oversikt over alle faktorer som gjør objektet sårbart, både eksterne forhold som en ikke kontrollerer og interne forhold som en kontrollerer. Denne tilnærmingen finner en igjen i Reason (1997) og i Aven (2007), men krever at en benytter de riktige faktorene.

Metoden benyttet før 2016 viser til faktorer som kan vurderes i den totale vurderingen av sårbarheten, men den har få eller ingen krav til hva som skal beskrives eller hvordan. Samtidig legger metoden til rette for at eksterne sikkerhetsstyrker skal vurderes som en av faktorene i vurderingen av objektets sårbarhet. En baserer dermed vurderingen av sin egen sårbarhet på faktorer som en ikke kan kontrollere. Dette krever dialog, avklarte forventninger/lovnader og innsikt i andre myndigheters kapabilitet, reaksjonstid, prioriteringer og operasjonsmodus, noe et selskap ikke kan forvente å ha alle steder i verden. Å bruke denne faktoren i en sårbarhetsvurdering vil derfor være høyst usikkert og kan i verste fall skape en svakhet som kan utnyttes. Sårbarhetsvurderingen i metoden legger til rette for en helhetlig tilnærming, men samtidig legger den ikke tydelig til rette for en styring av barrierer, slik en finner i Ptil (2017) og Aven m.fl., (2004).

Endringene i metoden som benyttes i dag er i stor grad gjenkjennbart med Ptil (2017) og Aven m.fl., (2004). Den legger til rette for en strukturert beskrivelse og vurdering av de barrierene som Statoil kontrollerer. Når en også her legger til grunne at scenarioene skal skrives detaljerte ved å beskrive hvordan trusselaktøren(e) vil gå frem i gjennomføringen av scenarioet vil en kunne få en detaljert beskrivelse av disse barrierene. Metoden legger også til rette for beskrivelser av barrierene som gjør at beslutningstaker vil få et bedre grunnlag for beslutning. Struktur og beskrivelser gjør at en beslutningstaker vil kunne vurdere hver enkelt barriere, både med tanke på effektiviteten den har på det enkelte scenarioet, hvor mange forskjellige scenarioer påvirkes av den samme barrieren og den totale effekten av barrierene. Dette vil kunne gi et bedre beslutningsgrunnlag ved at beslutningstaker «ser» effekten av tiltakene og kan vurdere dette oppimot kostnadene. Metoden tilrettelegger for den risikostyringen vi finner igjen i Aven (2007).

Men dagens metode legger ikke til rette for den samme oversikten av den helhetlige tilnærmingen som vi finner i den tidligere metoden. En del av faktorene som tidligere ble vurdert som en sårbarhet er nå faktorer som inngår som noen av faktorene i intensjonsvurderingen i scenarioet. Dette er faktorer som selskapet i liten eller ingen grad kontrollere ved etablerte objekter, men som likevel er viktige og kan påvirke behovet for nye barrierer. Når disse faktorene blir vurdert til å påvirke intensjonen i scenarioet vil også totalsummen av scenarioet øke og den totale security risikoen øker, som igjen vil gi behov for nye barrierer. Men når årsaken til økningen beskrives en plass, risiko og barrierer en annen plass, så kan dette gi mindre oversikt. Det igjen kan føre til misforståelser eller at feile barrierer introduseres eller forsterkes. Men disse faktorene vil få en helt annen betydning i

forbindelse med nye etableringer. Noen objekter, installasjoner, kan en i liten grad velge å etablere andre steder enn der hvor naturressursene er funnet. Men hvor en velger å etablere et kontor, og ikke minst hvordan, kan i større grad kunne påvirkes. Valget av kontorsted, type kontor og layout vil i stor grad kunne påvirke attraktiviteten, synligheten og muligheten til å overføre risiko til andre. Informasjonen som vi tidligere fant i den helhetlige sårbarhetsvurderingen finner vi igjen i dagens metode, men på to forskjellige plasser. Dette krever at beslutningstaker vet om dette og at analytikeren gjør beslutningstaker oppmerksom på det i forkant av beslutningsprosessen, både for nyetableringer og eksisterende. Det kan likevel være en viss fare for at fokuset blir på valget av barrierer og informasjonen som er tilgjengelig verken blir benyttet eller vurdert. Vi finner deler av dette i Turner (1978) og Turner & Pidgeon (1997).

Sett oppimot Ptil (2017) og Aven m.fl., (2004) er det noen forskjeller i dagens metode og barrierestyringen i den. Noe av årsaken til dette kan nok knyttes til hvordan selskapet har utviklet security som fag og tilhørende prosesser. Prosessen[37] beskriver hvordan security risiko skal analyseres, men operasjonaliseringen av tiltakene (barrierene) er det opp til hver enkelt risikoeier eller lokasjonsansvarlig å bestemme. Prosessen i Statoil følger her Aven (2007), men samtidig ser vi at utviklingen i dagens metode går i retning av Ptil (2007) og Aven m.fl., (2004). Denne utviklingen fører til at beslutningstaker både får bedre innsikt og støtte til både beslutningsprosess og implementering. Men samtidig legges det ikke til rette for å beskrive tydelige krav til hva de forskjellige barrierene skal oppnå for å gi den effektiviteten som er beskrevet. Dersom en ser dette i sammenheng med tekniske løsningers behov for kontroll og vedlikehold, som heller ikke er en faktor som er beskrevet i dagens metodikk, er det et gap oppimot Ptil (2017) og Aven m.fl., (2004). Dette gapet kan føre til at eksisterende barrierer, over tid, får redusert effektivitet og security risikoen øker uten at dette oppdages.

6.2 Hvordan er metodikken forankret og security risiko definert i styrende dokumentasjon?

Funn viser at selskapet har en egen prosess for hvordan security risiko skal håndteres. Denne prosessen er forankret i *grunnprinsippene* i selskapet og er således gjeldende for all aktivitet.

[37] SF-501 Manage security risk (ARIS)

Denne forankringen av prosessen virker å være i tråd med Reason (1997) og grunnlaget for å bygge en organisasjonskultur som formes etter en felles praksis[38]. Metodikken som benyttes i dag, både for security risikoanalyse og styring av barrierer mot tilsiktede uønskede hendelser er forankret i prosessen for håndtering av security risiko. I dette forankres også veiledere og maler, som gjør at strategien for hvordan security risiko håndteres, barrierene beskrives og implementeres er forankret i styrende dokumentasjon. Funn i grunnprinsippene peker på at fokuset på håndtering av risiko (også security risiko) i Statoil er i tråd med LaPorte & Consolini (1991) og Aven m.fl., (2004) om fokus på sikkerhet i operasjoner.

Prosessen inneholder i tillegg krav om når det skal gjennomføres security risikoanalyser, slik som at en security risikoanalyse skal gjennomføres i forbindelse med konseptutviklingsfasen, noe som gjør at bruken av metodikken også er forankret i styrende dokumentasjon. Dette finner vi igjen i Aven m.fl., (2004) og Ptil (2017).

Funn viser videre at det er en sammenheng mellom security og beredskap i styrende dokumentasjon i selskapet ved at de proaktive tiltakene som identifiseres og implementeres gjennom security risikoanalyse også vil ha en rolle i en beredskapshendelse og håndteres av beredskapspersonell. Dette henger sammen med organiseringen av beredskapsorganisasjonen i selskapet. De strategiske beslutningene for hvordan security risiko skal håndteres besluttes av risikoeier, som kan være en ansvarlig for en lokasjon eller alle lokasjonene i et land. Men dersom en hendelse inntreffer mobiliseres beredskapsorganisasjonen og myndigheten til å håndtere denne hendelser, på stedet og med de proaktive security tiltakene, overføres til første beredskapslinje. Denne overføringen av beslutningsansvar mellom strategisk og operasjonell ved håndtering av ulykker beskrives av Perrow (1999) og Weick & Sutcliffe (2007).

Det er funn som peker på at forankringen av metodikken på flere områder følger det teoretiske grunnlaget i studiet. Men funn viser også at den tydelige barrierestrategien vi finner i Reason (1997) ikke er like tydelig forankret i metodikken og styrende dokumentasjon for håndtering av security risiko.

Mine funn viser at Statoil har forankret gjennom styrende dokumentasjon en definisjon av security og security risiko. Definisjonen legger vekt på at security handler om beskyttelse mot handlinger med ondsinnede intensjonen, noe en finner igjen i Albrechtsen (2003). Men selv

[38] Temaet kultur vil ikke bli videre drøftet da det er en av oppgavens avgrensninger

om den metodiske tilnærmingen til hvordan security risiko analyseres i hovedsak er tilnærmet lik NS 5830 er det en viktig forskjell i definisjonen av risiko. Statoil definerer security risiko som relasjonen eller funksjonen av trusselen, konsekvensen og sårbarheten.

6.3 Hva er konsekvensen av denne utviklingen?

Funn viser at det i perioden etter 2016 i større grad enn i perioden før ble benyttet detaljerte scenarioer som beskrev hvordan trusselaktøren(e) kunne gå frem, en såkalt *threat pathway*, som kan tolkes i retning av Aven (2007) og Aven m.fl., (2004) beskrivelser om innsikt i alle risikoforhold. Det kan være nærliggende å tillegg de metodiske endringene grunnlaget for denne økningen, men trolig er det kun en medvirkende årsak. Endringene i metodikken kan ha hatt en positiv påvirkning gjennom analytikerens kunnskap om at en nå må identifisere de enkelte barrierer mot hvert scenario og derfor skriver scenarioet detaljert. I tillegg har de metodiske endringene ført til at en ikke lengre kan gi en generell vurdering av sårbarheten. Dette kan være med å «presse» frem detaljerte scenarioer. Men i perioden 2013 og frem til de siste security risikoanalysene som er analysert i denne oppgaven ble gjennomført har det i tillegg vært (og fortsatt er) et kontinuerlig fokus på og utvikling av security i selskapet, som vist til i innledningen av denne oppgaven. En naturlig konsekvens av dette vil være en økning i security kompetansen i hele selskapet og kanskje spesielt for dem som gjør security risikoanalyser og kan være en av årsakene til den økende andelen detaljerte scenarioer[39]. Det er med andre ord ingen direkte funn som gir grunnlag til å peke på kun en årsak til denne økende graden i bruk av detaljerte scenarioer, trolig er den sammensatt av flere årsaker.

Resultatet av denne økningen, uavhengig av årsaken, er at risikoforholdene (hva kan gå galt) knyttet til en aktivitet, personell eller et objekt i større grad blir detaljert beskrevet. Når risikoforholdene blir mer detaljerte vil det være mindre rom for misforståelser og en tydeliggjør kommunikasjon som igjen vil kunne øke forståelsen av risikoen. Forståelsen av den potensielle risikoen over et lengre tidsperspektiv uten hendelsers, som Reason (1997) påpeker, er spesielt viktig for å opprettholde marginene til å håndtere en tilsiktet uønsket hendelse. Security risikoanalyser er et beslutningsgrunnlag for risikoeier og detaljerte

[39] Temaet kompetanse vil ikke bli videre drøftet da det er en av oppgavens avgrensninger.

beskrivelser øker informasjonsgrunnlaget som beslutningene tas på. Utviklingen virker dermed å støtte opp under Perrow (1999).

Men på den andre siden viser både Jore (2016) og Albrechtsen (2005) at vår oppfattelse av trusselen, gjennom detaljerte beskrivelser av hvordan trusselaktøren(e) vil gå frem, fort kan vise seg å være feil eller at aktørene endrer fremgangsmåte underveis. En tilnærming hvor security risiko er håndtert gjennom detaljerte scenarioer vil kunne medføre gap i den totale rekken av barrierer ved at trusselaktøren(e) velger en annen tilnærming enn den som er valgt i risikohåndteringen. Bruk av flere scenarioer og alternative scenarioer vil kunne redusere dette gapet, men gitt security trusselens natur vil det fortsatt kunne være en grad av usikkerhet til hvorvidt alle muligheter er dekket.

Funnene viser at det i perioden etter 2016 er en større grad av struktur i barrierene og barrierebeskrivelsene enn før 2016. De metodiske endringene fremstår mer tydelig som årsaken til denne effekten, men også her vil det kunne være medvirkende årsaker, men som trolig har hatt mindre betydning. Grunnlaget for at en med større sikkerhet kan trekke denne slutningen ligger i at metodikkens nå tilrettelegger for denne type beskrivelse og struktur. I tillegg viser funnene at graden av struktur og barrierebeskrivelser er økende for begge typene scenario, men dog i større grad for de detaljert beskrevne scenarioene.

Resultatet av denne endringen betyr i første omgang at «alle» aspektene rundt risikoforholdene knyttet til en aktivitet, personell eller et objekt i større grad enn tidligere blir detaljert beskrevet og dokumentert, inkludert hvordan security risiko til slutt håndteres. Denne dokumenteringen sammen med både sentralisert lagring av alle security risikoanalyser og kommunikasjon av security risiko gjennom interne systemer gir i en mulighet til både synlighet, kontroll og etterprøvbarhet som ikke tidligere har vist seg mulig. Resultatene av endringen virker i større grad enn tidligere å støtte opp under hva som kjennetegner en god tilnærming til security risikoanalyser (FFI-rapport 2015, 00923).

Funnene viser videre at barrierebeskrivelsene i dagens metodikk i større grad en tidligere inneholder designbeskrivelser av barrierer (*forsvar i dybden*), beskrivende karakteristikker om barrierene og sammenhengen mellom dem, noe vi finner igjen i både Reason (1997), Ptil (2017) og Aven m. fl., (2004).

Resultatet av denne endringen betyr at sårbarhetsvurderingen i dagens metodikk i større grad enn tidligere blir et verktøy som tilrettelegger for en styring av barrierer mot tilsiktede uønskede hendelser enn tidligere. Strukturen og beskrivelsene gjør at hvert enkelt lag med

barrierer i større grad kan vurderes ut ifra hvilken effekt det har og hvor effekten kan eller må endres.

Det kan også her være nærliggende å tillegge metodikken det hele og fulle ansvaret for denne strukturen og beskrivelsene. Noe av årsaken ligger nok i strukturen som metodikken tilrettelegger for og beskrivelser den til tider «krever» at analytikeren tar stilling til. Men funn viser også at sårbarhetsvurderingene i noe større grad nå enn før 2016 også inneholder informasjon som Ptil (2017) og Aven m. fl., (2004) peker på, men som metodikken ikke etterspør. Det kan derfor være, som tidligere drøftet, flere årsaker til denne utviklingen hvorav kompetansen hos brukeren utpeker som en av dem.

7 Konklusjon

Utviklingen i samfunnet har ført til at det ikke lengre bare er politiet og forsvaret som har et ansvar i å håndtere security risiko, det er blitt et samfunnsansvar. Både faktiske terrorhendelser og mediedekningen fører til at vi alle sammen får et nærmere forhold til security risiko. Dette har også ført til at flere har en mening om både security, security risiko og security risikoanalyser. Det er laget metodikker og veiledninger for hvordan security risiko skal og bør analyseres, men det akademiske miljøet peker fortsatt på behovet for videre forskning innen fagfeltet da det fortsatt ikke er en metodikk som all kan enes om, både nasjonalt og internasjonalt. Det synes lettere å enes om en tilnærming enn en faktisk metodikk.

7.1 Oppsummering av oppgavens funn

Jeg har i denne oppgaven sett nærmere på den metodiske utviklingen i security risikoanalyser med fokus på sårbarhetsvurdering og barrierestyring. Den overordnede problemstillingen ble:

Hvordan har metoden for styring av barrierer mot tilsiktede uønskede hendelser utviklet seg i selskapet og hvordan er den forankret i styrende dokumentasjon?

For å svare ut denne problemstillingen og for å strukturere oppgaven ble det laget tre forskningsspørsmål. Metoden som ble valgt for å besvare problemstillingen er

dokumentstudier og det har i all hovedsak vært benyttet primærdata. Det er blitt undersøkt 12 security risikoanalyser fra to forskjellige tidsperioder og 158 scenarioer og sårbarhetsvurderinger er analysert. Gjennom analysene ble informasjonen ikke omskrevet, men kategorisert i sin originale form for å øke reliabiliteten. I tillegg utgjør både styrende dokumentasjon, maler og veiledere til metodikkene viktige empiriske bidrag da de sier noe om hvordan metodikken er ment å brukes.

Det teoretiske grunnlaget for oppgaven er strukturert på en måte som falt naturlig for forfatteren. Det starter med en redegjørelse av definisjonene på security og safety. Deretter var det naturlig å omhandle teoretiske perspektiver på hvorfor hendelser skjer, før en så på hvordan og om hendelser kan forhindres. Til sist ble fokuset rettet mot barrierer. Deretter ble de metodiske valgene og undersøkelsesdesignet både forklart og begrunnet, herunder en drøfting av validitet og reliabilitet.

Basert på drøfting av de viktigste funnene i det foregående kapitlet mener forfatteren å ha grunnlag for å trekke følgende konklusjon:

Metodikken har i hovedsak utviklet seg i retning av å bli en reell metodikk for styring av barrierer mot tilsiktede uønskede hendelser enn det tidligere metodikk har vært. Dette blir den på grunn av den økende informasjonen om barrierene, sammenhengen mellom barrierene og hvordan de knyttes til selve scenarioet. Metoden har en forankring i styrende dokumentasjon som gir håndteringen av security risiko synlighet i organisasjon. Metodikken tilrettelegger for beslutningsprosesser hvor «alle» risikoforhold i større grad enn tidligere er beskrevet. Beslutningene blir ikke nødvendigvis enklere, men informasjonsgrunnlaget for beslutning er høyere. Konsekvensene av endringene går ut over den helhetlige sårbarhetsforståelsen og det kreves en større bevissthet til viktig informasjonen som tidligere var tilgjengelig i sårbarhetsvurderingen, men som nå er beskrevet under scenarioet.

7.2 Anbefaling

Analysene av sårbarhetsvurderingene igjennom begge periodene viser at det i større grad i siste periode blir inkludert beskrivelser om barrierene som ingen av metodene etterspør eller legger godt til rette for. Det er i større grad i siste periode funnet beskrivelser av ytelseskrav knyttet til barrierene. Det er også i større grad i siste periode funnet beskrivelser for hvordan

barrierene understøtter hverandre eller aktiverer hverandre. Det er i tråd med det teoretiske grunnlaget i oppgaven (Aven m. fl. 2004 og Ptil, 2017) og kan være en indikasjon på at det er en kompetanse i selskapet som metoden ikke tilrettelegger for. Det anbefales derfor at det i oppdatering eller i videreutviklingen sees på.

7.3 Videre forskning

I løpet av denne oppgaven har det vært flere interessante spørsmål som kan være tema for videre forskning. For det første hadde det vært interessant å se nærmere på kompetanse og bakgrunn til de som gjennomfører security risikoanalyser og hvilken effekt dette har. Forskjellene og likhetene mellom security og safety er en pågående diskusjon. Det hadde derfor vært interessant å undersøke videre hvorvidt det er forskjeller på safety og security barrierer. Kan en si noe om hva som utgjør denne forskjellen?

8 Litteraturliste

Albrechtsen, E., (2003). *Security vs Safety*. NTNU-Department of Industrial Economics and Technology Management. Lastet ned fra: http://www.iot.ntnu.no/users/albrecht/rapporter/notat%20safety%20v%20security.pdf

Aven, T., (2007). *Risikostyring*. 2. opplag. Universitetsforlaget

Aven, T., Boyesen, M., Njå, O., Olsen, H. O. og Sandve, K., (2004). *Samfunnssikkerhet*. Oslo: Universitetsforlaget AS.

Aven, T., Røed, W., Wiencke, H.S., (2008) 2.opplag. *Risikoanalyse*. Oslo. Universitetsforlaget AS.

Bourrier, M. (2011) *The legacy of the theory of High Reliability Organizations: An ethnographic endeavor*
Sociograph – Working Paper No 6/2011
Genève: Université de Genève

Busmundrud, O. Maal, M. Kiran, J. H & Endregard, M (2015) *Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger*. Lastet ned fra: https://www.ffi.no/no/Rapporter/15-00923.pdf

Egeli, A. (2014). *Analysemetodikk i forbindelse med terrorisme – Bruke eller ikke bruk av sannsynlighet*. http://brage.bibsys.no

Enehaug, B. (2015). *Den menneskelige faktors betydning i barrierestyring*. http://brage.bibsys.no

Guldmundur, F., Hale, A., Goossens, L. Betten, J., Duijm, N. J. (2005). *The development of an audit technique to assess the quality of safety barrier management. Journal of Hazardous Materials.*
https://doi.org/10.1016/j.jhazmat.2005.07.011

Grønmo, S., (2004) *Samfunnsvitenskapelige metoder*. 2 utgave. Bergen. Fagbokforlaget.

Jacobsen, D. I., (2015). *Hvordan gjennomføre undersøkelser?* Oslo. Cappelen Damm AS

Jore, S. H., (2016) *Safety and Security – is there a need for an integrated approach?* Universitetet i Stavanger

Jore, S.H., Egeli, A., (2015). *Risk management methodology for protecting against malicious acts? Are probabilities adequate means for describing terrorism and other security risks?* I: Jore, S. H., (2016) *Safety and Security – is there a need for an integrated approach?* Universitetet i Stavanger

Kriaa, S., Pièrre-Cambacèdès, L, Bouissou, M & Halgand, Y (2015) *A survey of approaches combining safety and security for industrial control systems.* Lastet ned 10.02.2018, fra: https://doi.org/10.1016/j.ress.2015.02.008

Nagell, M. (2013) *Mindfullness og teknisk barrieresystem – risikohåndtering i bore- og brønnoperasjoner.* http://brage.bibsys.no

Olsen, O. E., Matheisen, E. R., Boyesen, M., (2008). *Media og krisehåndtering*. Høyskoleforlaget AS – Norwegian Academic Press
Kristiansand

Perrow, Charles (1999) *Normal Accidents. Living with High-Risk Technologies*. Princeton: Princeton University Press

Pidgeon, N., O`Leary, M., *Man-made disasters: why technology and organizations (sometimes) fail.*
Lastet ned 02.04.17: http://www.sciencedirect.com/science/article/pii/S0925753500000047

Pièrre-Cambacèdès, L. & Chaudet, C. (2010). *Avoiding ambiguities in the terms "security" and "safety".* The Sema referential framework. International Journal of Critical Infrastructure Protection, 55-66. Lastet ned 10.02.2018, fra: https://doi.org/10.1016/j.ijcip.2010.06.003

Pièrre-Cambacèdès, L, Bouissou, M (2013) *Cross-fertilization between safety and security engineering.* Lastet ned 10.02.2018, fra: https://doi.org/10.1016/j.ress.2012.09.011

Politiets sikkerhetstjeneste (2018) *Trusselvurdering 2018.*
https://www.pst.no/trusselvurdering-2018/

Ptil, (2011), *Nær på for Gullfaks C*. http://www.ptil.no/bronnsikkerhet/nare-pa-for-gullfaks-c-article7606-825.html

Ptil, (2015) http://www.ptil.no/regelverk/category696.html

Ptil (2017). *Prinsipper for barrierestyring i petroleumsvirksomheten*. www.ptil.no/

Reason, J. (1997). *Managing the Risks of Organizational Accidents*. Aldershot, Burlington USA, Singapore, Sydney, Ashgate.

Schiefloe, P. M., Notat 10/12, *En modell for samfunnssikkerhet*, 2011
Institutt for sosiologi og statsvitenskap
NTNU Samfunnsforskning AS

Statoil. (2013). *The In Amenas Attack.* ***Report of the investigation into the terrorist attack on In Amenas. Prepared for Statoil ASA's board of directors***. Lastet ned fra: http://e24.no/energi/her-er-statoils-rapport-om-terrorkatastrofen/21606092

Stålesen, J. S. (2011). *Security styring i petroleumssektoren*. http://brage.bibsys.no

Turner, B.A. (1978) *Man-made Disasters*. London: Wykeham Science Press

Turner, Barry A. And Pidgeon, Nick F (1997). *Man-Made Disasters*, Oxford: Butterwoth Heineman.

Stortingsmelding Nr. 12. (2005-2006). *Helse, miljø og sikkerhet i petroleumsvirksomheten*. Lastet ned fra: https://www.regjeringen.no/no/dokumenter/stmeld-nr-12-2005-2006-/id408103/

Weick, K. E., Sutcliffe, K. M., (2007), *Managing the Unexpected, Resilient Performance in an Age of Uncertainty*. Jossey-Bass