UNIVERSITETET I STAVANGER

MASTERGRADSSTUDIUM I

RISIKOSTYRING OG SIKKERHETSLEDELSE

MASTEROPPGAVE

SEMESTER:

Våren 2023

FORFATTER: Erlend Larsen

VEILEDER:

Ole Andreas Hegland Engen

TITTEL PÅ MASTEROPPGAVE:

Dilemma mellom safety og security. Lar disse seg løse gjennom en felles sikkerhetskultur?

EMNEORD/STIKKORD:

Sikkerhetskultur, safety culture, security culture, dilemmaer,

SIDETALL: 64

STAVANGER ....13.10.2023.....

DATO/ÅR

Innholdsfortegnelse

1 Sammendrag

Safety og security er to fagretninger som fra et felles kunnskapsgrunnlag har utviklet seg til to ulike profesjoner, og som i økene grad blir ivaretatt av dedikert personell med sterk knytning av identitet til eget fagområde. Fagområdene har over tid utviklet forskjeller i forståelse av risiko, vurderinger av risiko og håndtering av risiko, og baserer seg også på ulike verdier og faglige tilnærminger. Begge fagretningene er virksomhetsovergripende og søker i så stor grad som mulig å forme kulturen i virksomheter, inkludert hvordan ansatte oppfatter virkeligheten, tenker og agerer.

Safety og security er ikke uavhengige av hverandre. Interaksjonene må dels anses som komplekse, ved at begge deler legger betydelige føringer på det daglige liv i virksomheter, inkludert uformalisert samhandling og kommunikasjon. Dette medfører at det oppstår dilemmaer i grensesnittet mellom dem. At virksomheter står ovenfor dilemmaer er ikke unikt og enhver virksomhet er til enhver tid avhengig av å måtte vurdere ulike hensyn mot hverandre, der den klassiske konflikten står mellom sikkerhet på den ene siden og produksjon og økonomi på den andre. Selv om dilemma mellom safety og security er godt kjent fra litteraturen, er det få studier som har tatt for seg dette på virksomhetsnivå. Denne oppgaven har derfor gjennom intervjuer med 9 ledere og medarbeidere i en valgt virksomhet studert hvilke dilemma som oppstår i grensesnittet mellom safety og security, mulige årsaker, handlingsrommet for løsninger og om en omforent sikkerhetskultur vil kunne bidra til at disse dilemmaene finner sin løsning.

Dilemmaene som er identifisert i denne oppgaven er knyttet til åpenhet kontra hemmelighold, beskyttelse av informasjon kontra tilgjengelighet, insiderproblematikken, beredskap, risikostyring samt sikkerhetsstyring. Årsakene til dilemmaene er sammensatte, men kan i stor grad tilskrives ulikheter i faglige tilnærminger mellom safety og security. Samtidig vil det være ulikheter i handlingsrommet for å løse dilemmaene. Prinsippene for å løse dilemmaene vil imidlertid være de samme, og man er i praksis avhengig av å måtte finne kompromisser med utgangspunkt i at den totale sikkerheten ivaretas på en best mulig måte. En god sentralisert styring av grensesnittet mellom safety og security er en forutsetning for å få dette til i praksis.

Sikkerhetskultur-begrepet brukes gjerne til å skape en forbindelse mellom dypereliggende forhold i en organisasjon, som virkelighetsforståelse og verdier, og måten sikkerheten ivaretas av medarbeidere i utøvelsen av organisasjonens daglige virke. Sikkerhetskultur er ikke en frittstående aktivitet, men er tett integrert i bl.a. ledelse, organisatoriske forhold, arbeidspraksis og teknologiske løsninger. Å skulle beskytte mot intensjonelle handlinger med formål å forårsake skade krever andre faglige tilnærminger enn å skulle beskytte mot ulykker som følge av menneskelige feilhandlinger, og dette medfører også divergerende oppfatninger mellom safety og security om hva innholdet i en virksomhetsovergripende sikkerhetskultur bør være, og legger også føringer for hvilke verdier som bør ligge til grunn for kulturen.

Oppgaven argumenterer for at vesentlige deler av sikkerhetskulturen bør være virksomhetsovergripende og ledelsesstyrt, men samtidig tilpasset virksomhetens egenart og relaterte farer ved virksomheten. Samtidig vil det neppe være hverken formålstjenlig eller realistisk å få til en helt omforent kultur på tvers av virksomheten, da ulike deler av organisasjonen har svært ulike oppgaver og som forutsetter ulikt tilnærming og ulike perspektiv på sikkerhet. Det vil derfor være viktig at en felles toppstyrt sikkerhetskultur balanseres opp mot en sterk profesjonskultur og som er forankret i beste praksis for de ulike profesjonene.

Oppgaven argumenterer for at endring av kultur må skje gjennom endring av praksis, og at dette igjen vil medføre at underliggende verdier og antagelser endres slik at disse blir kongruente med gjeldende praksis. Kultur henger samtidig sammen med struktur, og god struktur vil medvirke til utvikling av en god sikkerhetskultur. En felles virksomhetsovergripende kultur handler samtidig om å at man på tvers av virksomheten deler en virkelighetsforståelse. Viktige virkemidler for å skape en felles virkelighetsforståelse mellom safety og security vil være gjennom dialog og samhandling, samt forståelse og respekt på tvers av fagområdene.

2 Forord

Denne masteroppgaven representerer endepunktet for mitt studium innen risikostyring og sikkerhetsledelse ved Universitetet i Stavanger.

Sikkerhetskultur er en problemstilling jeg har interessert meg for i to tiår, og er et begrep som brukes av mange personer og i mange sammenhenger. Sikkerhetskulturen får gjerne skylden om noe går galt og får gjerne æren om det ikke går galt. Samtidig er det ikke så enkelt å bli klok på sikkerhetskultur, da det finnes mange meninger og få gode svar på hva som gjør en sikkerhetskultur god.

Jeg har i min bakgrunn lang erfaring fra å ha jobbet med både safety og security i en sektor der det er høye forventninger til begge deler. Sikkerhetskultur er et begrep som går igjen innenfor begge fagfeltene, men jeg har samtidig opplevd at dette er et begrep som har et svært ulikt innhold. Å skulle skrive en oppgave som handler om sikkerhetskultur, og der jeg samtidig hadde muligheten til å ta et dypdykk i hvorfor kultur er så veldig forskjellig mellom safety og security, har derfor vært særdeles interessant og lærerikt. Det at det samtidig har vært forsket lite på hva som i praksis skjer på et virksomhetsnivå der safety og security møtes, har gjort arbeidet med oppgaven ekstra spennende.

Jeg vil takke Ole Andreas Hegland Engen som har vært veileder for denne oppgaven. Dette har fungert veldig godt og jeg har satt pris på våre diskusjoner og Ole Andreas sine evner til å se alle detaljene i en litt større sammenheng. Samtidig vil jeg takke samtlige av mine kolleger som har latt seg intervjue i forbindelse med oppgaven, og som hver og en har bidratt med nyttige perspektiver inn i oppgaven. Jeg vil samtidig takke min arbeidsgiver, IFE, for deres positive holdning til dette studiet og for å ha latt seg studere i denne oppgaven.

3 Innledning

Større ulykker de siste tiårene har vist at det finnes flere typer industriell virksomhet der ulykker kan forårsakes gjennom sammensatte, og til dels komplekse, hendelsessekvenser og medføre omfattende konsekvenser langt ut over virksomhetens grenser. Bophal-ulykken (kjemisk prosessindustri, India, 1984), Tsjernobyl-ulykken (kjernekraft, Belarus, 1986), Deepwater Horizon-ulykken (oljerigg, Mexico-gulfen, 2010) og Exxon Valdez-ulykken (oljetanker, USA, 1989) er noen eksempler på dette. Samtidig har blant annet terrorangrepene i USA 11.09.2011 tydelig demonstrert en vilje til å ramme sårbare sivile mål for å skape konsekvenser for samfunnet rundt. Dette har resultert i mye oppmerksomhet på terrorbeskyttelse av virksomheter med potensiale for omfattende konsekvenser for omgivelsene. Organisasjoner som over årtider har utviklet gode systemer understøttet av en god kultur for å ivareta safety, har derfor i løpet av kort tid vært nødt til å gjøre tilsvarende for security.

Begrepet sikkerhetskultur ble lansert av Det Internasjonale Atomenergibyrået i 1991 på bakgrunn av bl.a. Tsjernobyl-ulykken og Bophal-ulykken og har i tiden etterpå blitt brukt til å årsaksforklare disse og andre ulykker. Begrepet skaper en knytning mellom sikkerhetsmessig adferd som utøves av mennesker i en organisasjon og normer, regler, verdier, holdninger etc. som er institusjonalisert i organisasjonen. Begrepet sikkerhetskultur er imidlertid ikke knyttet til noen fysisk eller målbar størrelse, og det representerer heller ikke konsensus hverken om definisjoner, hva som ligger i en god sikkerhetskultur eller hvordan man skal oppnå det.

Akademia spiller en viktig rolle i å utvikle teori rundt hvorfor større ulykker skjer og hvordan disse kan unngås, og større ulykker har i flere tilfeller resultert i paradigmeskifter innen teoriutviklingen. Teoriene danner basis for hvordan virksomhetene jobber systematisk for å redusere risiko og for å innfri samfunnets stadig økende forventning til trygghet. De metodiske tilnærmingene virksomhetene bruker støttes av en sikkerhetskultur og som typisk vektlegger åpenhet og erfaringslæring (ofte ut over organisasjonens grenser), en systemtilnærming, erkjennelse av at feil er unngåelig og verdsetting av en spørrende holdning til etablert sikkerhetspraksis.

I motsetning til safety, der menneskelig feilhandling eller uvørenhet enten er en initierende årsak til en hendelse eller bidrar til å forverre en feil, er den grunnleggende antagelsen innen security at hendelser er forårsaket av forsettlig intensjon om å forårsake skade. En slik intensjon foreligger oftest eksternt, hos mennesker som ønsker å skade virksomheten eller bruke virksomheten som et middel for å skade samfunnet rundt, men kan også foreligge hos virksomhetens medarbeidere (insidertrussel). På tilsvarende måte som innen safety, er virksomhetenes arbeid med security forankret i akademisk teori og søkes også understøttet av en god sikkerhetskultur. En slik security-kultur skiller seg imidlertid fra det som normalt anerkjennes som en god safety-kultur, da den utfordrer sentrale verdier innen safety som tillit og åpenhet.

Sikkerhetsorganisasjoner kjennetegnes av at sikkerhet gjennomsyrer måten organisasjonen tenker på og hvordan organisasjonen handler. Dette gjelder både innen safety og security, og der begge fagområder har sine perspektiver og metodiske tilnærminger og begge ønsker å definere og forme virksomhetens sikkerhetskultur. Utfordringer med å forene safety og security er kjent både fra litteraturen og fra virksomheter. Det finnes imidlertid få akademiske studier som har gått i dybden på hvilke dilemma som oppstår når safety og security må forenes i en organisasjon, bakenforliggende årsaker til dilemmaene og hvordan de best løses innenfor rammene av organisasjonen. Tilsvarende er det lite studert i hvilken grad det vil være mulig å skape en omforent kultur og som kan bidra til å løse de utfordringer som oppstår i skjæringspunktet mellom safety og security. Det er disse problemstillingene denne oppgaven handler om.

3.1 Bakgrunn

En av det 20-ende århundrets største oppdagelser var spaltningen av atomet og utviklingen av nukleærteknologi. Denne teknologien har gitt atomvåpen og kjernekraft, og også gjort det mulig å framstille eksempelvis radioaktive nuklider for diagnostikk og behandling av kreftsykdommer. Sikkerhet innen nukleærteknologi har samtidig hatt stor betydning for teoriutvikling innenfor sikkerhetsfaget. Et eksempel er Jens Rasmussens forskning bl.a. på sikkerhetssystemer, den menneskelige faktor og risikoanalyser. Tilsvarende ble Charles Perrows teorier om normalulykker inspirert av Tree Mile Island ulykken i USA i 1979 og Clark & Perrows forsking rundt beredskap basert på en feilet beredskapsplanlegging ved Shoreham Nuclear Power Station på Long Island i USA.

Nukleær virksomhet omfatter alt fra store kommersielle kjernekraftverk til små forskningsreaktorer inne på en universitetscampus, men også støttende infrastruktur som forskingsfasiliteter, anlegg for produksjon av reaktorbrensel og anlegg for håndtering av radioaktivt avfall. Tilsvarende er det også store forskjeller i anleggenes kompleksitet og i farepotensial, der Tsjernobylulykken i 1986 medførte radioaktivt nedfall over store deler av Europa. Farepotensialet, og persepsjonen av dette, gjør samtidig nukleær virksomhet til attraktive terrormål og der et terrorangrep vil kunne framprovosere hendelse med alvorlig utslipp til omgivelsene. I tillegg håndterer nukleære anlegg radioaktivt materiale, som for terrorister vil være attraktive for tyveri med hensikt brukt i «skitne bomber» eller lignende.

Etter andre verdenskrig var det i Norge stor optimisme rundt atomalderen. Etter stormaktene (USA, UK, Sovjetunionen Frankrike) og Canada, var Norge det første landet som klarte å konstruere og sette i drift en forskningsreaktor (JEEP I) i 1951. I perioden fram til 1967, ble det etablert ytterligere tre forskingsreaktorer: NORA, Haldenreaktoren og JEEP II. De to siste ble permanent nedstengt i 2018 og 2019. Planene om kommersiell kjernekraft i Norge ble forlatt etter et vedtak i Stortinget i 1979. Norge har imidlertid gjennom forskningsvirksomheten ved Haldenreaktoren, hatt en unik rolle i å etablere et eksperimentelt basert kunnskapsgrunnlag om reaktorbrensel og materialer for bruk i kjernekraftindustrien og som har gitt et vesentlig bidrag til sikrere kjernekraft hos de inntil 23 landene som har vært samarbeidspartnere i forskningen. Debatten om kommersiell kjernekraft i Norge har imidlertid de senere år kommet opp igjen, og kommersielle aktører har konkrete planer om å etablere små modulære kraftreaktorer i Norge.

3.2 Problemformulering

Oppgaven tar utgangspunkt i Institutt for Energiteknikk (IFE) som ble etablert i 1948 under navnet Institutt for Atomenergi, med formål om å etablere kjernekraft og annen nukleær teknologi i Norge. Etter at forskningsreaktorene ble nedlagt har virksomheten ved det nukleære IFE vært rettet mot en virksomhetsoverdragelse til et nyopprettet selskap, Norsk Nukleær Dekommisjonering (NND), og som skal sørge for nedbygging av anleggene og håndtering av radioaktivt materiale.

Nedbyggingen av nukleær forskningsinfrastruktur, inkludert den som trenges for å håndtere høyt radioaktivt reaktorbrensel vil ta flere tiår. Sikkerheten må ivaretas fram til alt er fjernet. Før virksomhetsoverdragelsen kan finne sted, må det gjennomføres flere store tunge tekniske analyse - og utredningsarbeider, og som krever innleid kompetanse fra utlandet. IFE er underlagt nye krav til security, og som legger føringer for virksomhetens interne prosesser og for samhandlingen mot eksterne aktører.

Bakgrunnen for at IFE kan anses som en god case er at den nukleære virksomheten har potensiale til å forårsake konsekvenser ut over anleggene. Virksomheten har eksistert i 75 år og har et veletablert arbeid med å ivareta safety. Samtidig har virksomheten i nyere tid gjennomført omfattende oppgraderinger innen security.

Problemstillingen med oppgaven er:
«Hvilken rolle spiller målkonflikter i sikkerhetskultur ved integrasjon mellom safety og security i virksomheten»

Oppgaven skal, med utgangspunkt i IFE som case, diskutere følgende forskningsspørsmål:

1. *Undersøke og drøfte hvilke dilemmaer det er mellom safety og security og mulig opphav til disse.*
2. *Undersøke mulighetsrommet for løsninger på disse dilemmaene og som ivaretar både safety og security på en akseptabel måte.*
3. *Diskutere hvordan sikkerhetskultur kan bidra til en tettere integrering mellom safety og security, hva som bør være essensen i en omforent kultur og hvordan man bør gå fram for å etablere den.*

3.3 Avgrensning

Institutt for Energiteknikk er et forskingsinstitutt med eksperimentell virksomhet innenfor flere fagområder, f.eks. radioaktive legemidler, fornybar energi og petroleum. Oppgaven avgrenser seg til den nukleære delen av virksomheten.

Oppgaven begrenser seg til å se på ledelsesmessige og organisatoriske forhold knyttet til å ivareta den samlede sikkerheten i grensesnittet mellom safety og security. Det er fra litteraturen kjent at innføring av nye regimer for security vil kunne påvirke arbeidsmiljøet og medføre også arbeidsmiljømessige og psykososiale utfordringer (Pettersen & Bjørnskau, 2014). Dette er omtalt i denne oppgaven, men er ikke gått i dybden på.

3.4 Oppbygningen av oppgaven

Tematikken i denne oppgaven er for en utvalgt virksomhet å studere dilemma som oppstår når en organisasjon med et vel etablert arbeid innen safety må gjøre en reorientering av arbeidet for å møte en ny hverdag med strenge forventninger til security og i hvilken grad en omforent kultur vil kunne bidra til å løse disse dilemmaene. Teoridelen av oppgaven vektlegger derfor på et mer generelt grunnlag å diskutere hva som skiller og hva som forener safety og security. Deretter gjennomgår oppgaven en del teoretiske perspektiver på sikkerhet og som i noe varierende grad blir vektlagt innenfor safety og security. Disse perspektivene er sentrale for hvordan man arbeider med sikkerhet, og kulturen som etableres for å understøtte dette arbeidet.

Konseptet sikkerhetskultur er diffust og blir brukt med ulike formål, og der det er relativt fritt til å fylle det med eget innhold. Teoridelen av oppgaven avsluttes derfor med en diskusjon rundt sikkerhetskultur, da med vekt på hva som ligger i begrepet, hva som kjennetegner en god sikkerhetskultur, hvordan kultur kan etableres og endres, samt i hvilken grad det er nødvendig for en virksomhet å ha en enhetlig kultur.

Det empiriske arbeidet i denne oppgaven har omfattet en undersøkelse ved bruk av strukturerte intervjuer blant ni ledere og medarbeidere i den studerte virksomheten. Detaljene rundt hvordan dette arbeidet har blitt gjennomført er beskrevet i metodekapitlet, og som også inneholder vurderinger av validiteten til undersøkelsen og til teoriene som blir brukt for å tolke denne. Resultatene fra undersøkelsen er rapportert i empirikapitlet, og som er organisert rundt hvert av de tre forskingsspørsmålene.

Oppgaven avsluttes med et diskusjonskapittel og et konklusjonskapittel. Diskusjonskapitlet er strukturert på bakgrunn av forskingsspørsmålene og vektlegger å diskutere funnene fra empirien opp mot teorien beskrevet i teorikapitlet. Konklusjonene i oppgaven blir deretter trukket på bakgrunn av diskusjonskapitlet.

3.5 Begrepsavklaring

Begreper kan i utgangspunktet forstås på ulike måter. For noen av begrepene vil det finnes formaldefinisjoner gitt eksempelvis i ISO-standarder. For andre begreper vil det finnes legaldefinisjoner. I denne begrepslisten er det valgt å gi en enkel forklaring på begrepene og som i størst mulig grad skal sammenfalle med hvordan de er ment forstått innenfor rammen av oppgaven:

- **Beredskap:** Forberedte tiltak som vil kunne iverksettes for å redusere konsekvenser knyttet til tap av kontroll ved hendelse.
- **Deterministisk analysemetode.** Analysemetode som vurderer hendelsessekvens og konsekvens, gitt forutsetningen at hendelsen inntrer.
- **Dilemma:** Beslutningssituasjon der man må velge mellom ikke forenelige verdier, strategier, mål eller lignende.
- **Epistemisk usikkerhet:** Usikkerhet som framkommer pga. manglende informasjon.
- **KPI (Key Performance Indicator):** Måleindikator som brukes til å måle utviklingen innen et område.
- **Målkonflikt**: Beslutningssituasjon der man må velge mellom to ikke forenelige mål.
- **Probabilistisk analysemetode**: Analysemetode som inkluderer sannsynlighet.
- **Risiko:** Et utrykk for konsekvenser knyttet til en gitt aktivitet i kombinasjon med tilhørende usikkerheter.
- **Safety:** En tilstand med akseptabel risiko for uønskede konsekvenser som følge av uhell og ulykker.
- **Security:** En tilstand med akseptabel risiko for uønskede konsekvenser som følge av forsettlige handlinger som terrorisme, ødeleggelse, tyveri etc.
- **Sikkerhet:** En tilstand der risiko for uønskede konsekvenser er akseptabel, inkludert både safety og security.
- **Sikkerhetskultur**: Den delen av organisasjonskulturen som har betydning for hvordan sikkerheten ivaretas.
- **Sårbarhet**: Svakheter i systemet og som kan utnyttes av trusselaktør til å forårsake security-hendelse. (Innen safety brukes utrykket til å beskrive konsekvenser av en tenkt hendelse om den inntreffer).
- **Trusselaktør**: Entitet (person eller gruppering) som forbindes med en trussel.

4 Teori

Det sentrale tema i denne oppgaven er de dilemmaene som oppstår der safety og security møtes på virksomhetsnivå og hvordan organisasjonen bør gå fram for å løse disse. Kapittel 4.1 belyser derfor hva litteraturen anser er forskjeller og likheter mellom disse to fagdisiplinene, og beskriver også hva som tidligere er kjent av dilemmaer på virksomhetsnivå der safety og security møtes.

En viktig del av argumentasjonen som vil bli gjort i denne oppgaven er at forskjeller mellom safety og security langt på vei kan forklares med ulik oppfatning av årsaken til at hendelser skjer samt hvorfor og hvordan de utvikler seg. Selv om sentrale sikkerhetsperspektiver deles mellom safety og security, har disse perspektivene noe ulik relevans og blir også i ulik grad brukt. Ulikheter i perspektiver på sikkerhet, vil da få stor betydning på hva man vektlegger i sikkerhetsarbeidet, men også hvilke verdier man legger til grunn for arbeidet. Kapittel 4.2 vil derfor gjennomgå noen sentrale perspektiver og som vil bli brukt i diskusjonsdelen av oppgaven.

Et annet sentralt tema i oppgaven er hvilken rolle kultur har i å finne veien ut av dilemmaene, og hvordan man bør gå fram for å etablere en omforent kultur mellom safety og security. Kapittel 4.3 handler derfor om sikkerhetskultur og prøver å belyse sentrale tema som hva som ligger i begrepet sikkerhetskultur, hva som kjennetegner god sikkerhetskultur, hvordan sikkerhetskultur utvikles og om det faktisk er slik at en virksomhet trenger å ha en omforent kultur.

4.1 Sikkerhet, safety og security

I henhold til (Möller, et al., 2006) handler sikkerhet om en tilstand der risiko har blitt redusert til et gitt (tolererbart) nivå, hensyntatt epistemiske usikkerheter. Han anser videre at det ikke er meningsbærende å snakke sikkerhet i betydningen av fravær av risiko (absolutt sikkerhet), da dette ikke er en tilstand man kan oppnå. På norsk brukes begrepet sikkerhet både i betydning safety og security. Til tross for at disse to over tid har utviklet seg til egne fagområder, finnes det ingen universelt aksepterte definisjoner på begrepene «safety» eller «security» (Blokland & Reiners, 2020). Det finnes imidlertid mange ulike definisjoner, eksempelvis i ordbøker, faglitteratur og industristandarder. Felles for flesteparten av disse er at de i stor grad baserer seg på to distinksjoner, eller som en kombinasjon mellom disse to (Pettersen Gould & Bieder, 2020):

1. Intensjon: Der safety setter søkelys på farer ved ikke-intensjonelle handlinger eller ulykkesrisiko i motsetning til security og som setter søkelys på ondsinnede trusler og intensjonell risiko.
2. Opphav (Årsak)-konsekvens: Der safety handler om systemets evne til ikke å skade omgivelsene, mens security handler om omgivelsenes evne til ikke å skade systemet. I noen definisjoner trekkes det også inn systemets evne til ikke å skade seg selv.

Da denne oppgaven skal diskutere dilemmaer mellom safety og security, er det i dette delkapitlet gjort nærmere vurderinger av det teoretiske grunnlaget for å skille disse fagområdene, hva skillet i praksis består i og hva dette skillet medfører av utfordringer der to ulike tilnærminger til sikkerhet møtes.

4.1.1 Det vitenskapelige grunnlaget for å skille mellom safety og security

For at et fagområde skal kunne anerkjennes som en vitenskapelig disiplin er det gitte kriterier som må være oppfylt, blant annet i form av et unikt, felles og delt kunnskapsgrunnlag og metodiske tilnærminger som etableres på bakgrunn av en vitenskapelig prosess og metode. Safety som fagdisiplin etterlever disse kriteriene, og har derfor status som en egen vitenskapelig disiplin (Aven, 2014).

Sammenlignet med safety, er security en mer framvoksende profesjon, og som ennå ikke er godt definert eller støttet av en robust akademisk disiplin. Kunnskapsgrunnlaget innen security er fragmentert, og det er også stor variasjon i hva som undervises ved akademiske institusjoner (Brooks & Coole, 2020). Litteraturen som omhandler security låner også en del perspektiver fra safety, men uten at de i tilstrekkelig grad er validert gjennom studier. Det er heller ikke gjort gode avgrensinger av security som fagområde, og security kan derfor anses som multidimensjonal ved at den omfatter en rekke område og spenner fra individnivå til et mellomstatlig nivå (Jore, 2019). Ved at security pr. i dag ikke har et tilstrekkelig kunnskapsgrunnlag for å skille seg fra safety, konkluderer Jore med at security heller ikke kan anses som en egen vitenskapelig disiplin (Jore, 2019). Før dette kan skje er det nødvendig å bestemme hvilke konsepter og teorier som er relatert til området, hvilke nivåer og mål av samfunnet som skal inkluderes, i tillegg til samvirke og avhengigheter til andre disipliner. Samtidig påpeker Jore at det er stort rom for samarbeid og læring mellom safety og security.

4.1.2 Likheter og ulikheter mellom safety og security

På et overordnet nivå er det store likheter mellom safety og security, i at begge utrykker «fravær av skade», dvs. at begge søker å forebygge og minimere uønskede konsekvenser for mennesker, miljø eller eiendom (Bieder & Pettersen Gould, 2020). Tilsvarende er det klare likheter i kunnskap når det kommer til risikohåndtering, kontroll, ledelse og yrkesmessig utførelse (Brooks & Coole, 2020). Både safety og security anvender seg om konseptet risiko for å håndtere farer/trusler. Selv om metodikken er ulik, vil en risikohåndteringsprosess ofte bestå av de samme trinnene. Tilsvarende vil også større organisatoriske ulykker inkludere de samme tekniske, organisatoriske og menneskelige elementene, der mennesker spiller en viktig rolle i å oppdage, håndtere og begrense omfanget av en hendelse/ulykke (Jore, 2019).

Det er mellom safety og security store ulikheter når det kommer til farer og trusler, teknologi og underliggende teorier. Mens risikostyring innen safety setter søkelys på å styre farer, styres risiko innen security etter ondsinnede trusler, dvs. deres intensjoner og kapasiteter. For kontroll av farer, er søkelyset innen security rettet mot intensjon, og kontrolltiltak er i stor grad rettet mot fysisk herding, avskrekking og forsinkelse i kombinasjon med teknologi for å detektere og sikre menneskelig respons på hendelser. Innen safety er det vesentlig mindre vektlegging av intensjon, mens kontrolltiltakene typisk er rettet mot å unngå menneskelig feil og å sikre samsvar (Brooks & Coole, 2020).

Skillet i synet på menneskelig intensjon, medfører videre at det er forskjeller når det kommer til hvordan hendelser vurderes, håndteres og forebygges. Innen safety anerkjennes tillit som en viktig verdi og deling av informasjon blir generelt betraktet som et kriterium for forbedring. Security representerer en verden av hemmelighold både for mulige gjerningspersoner og for organisasjoner som er mulige terrormål. (Formulert av forfatterne: *«In safety we trust, in security we distrust»)* (Bieder & Pettersen Gould, 2020)

(Jore, 2019) argumenterer med at det er vanskelig å skille security fra safety kun ut fra menneskelig intensjon, fordi menneskelig intensjon også spiller en vesentlig rolle innen safety. Eksempelvis kan personer med forsett velge å bryte sikkerhetsregler, noe det kan tenkes flere ulike motiver for å gjøre. Man må derfor i tillegg inkludere et forsett om å forårsake skade, men heller ikke dette gir en klar grenselinje mellom fagområdene. Eksempelvis kan man (innen safety) tenke seg brudd på sikkerhetsregler som følge av bruk av narkotika. Samtidig kan man tenke seg flere typer handlinger, eksempelvis opportunistiske tyverier og der det ikke foreligger et direkte forsett om å forårsake skade. Det vil derfor være en uklar grenseflate mellom fagområdene, og som refereres til som et «grått område». God samhandling og som vil måtte forutsette kompromisser både fra safety og security er derfor viktig, ikke minst ut fra at begge aspektene i økende grad ses i et større samfunnsperspektiv (Pettersen Gould & Bieder, 2020).

Praksis innen både safety og security kan variere fra det høyt spesialiserte støttet av en skarp kunnskap til en rutinemessig praksis basert på sedvane, regler og lovverk. Praksis kan i mange tilfeller være fundert på økonomiske hensyn og i etterlevelse av policyer og regelverk, heller enn å ha et godt vitenskapelig fundament. Disse kan være fastsatt både av nasjonale myndigheter og på konsernnivå. Dette gjelder i større grad innen security enn i safety, da security i utgangspunktet bygger på et svakere kunnskapsgrunnlag enn safety (Pettersen Gould & Bieder, 2020).

Som det framgår av kapittel 4.1.1, er det ikke en omforent forståelse for teorier og konsepter innen security og faglitteraturen kan også avvike noe i sin framstilling av dette. Smith og Brooks er blant de mer anerkjente lærebokforfatterne, og beskriver i sin lærebok et konsept bestående av prinsipper, security-ledelse, miljøet rundt og styring av security-risker (Smith & Brooks, 2013).

- Security-ledelse: Omfatter bl.a. systemisk tilnærming, security-ledelse, strategisk rammeverk, organisatorisk resilliens, ledelsesfunksjoner, policyer og prosedyrer og etikk.
- Prinsipper: Omfatter de 10 kjerneprinsippene: (1) Informert, (2) Styrt, (3) Uavhengig, (4) Samarbeidende, (5) Overvåket, (6) Konsistent, (7) Uforutsigbar, (8) Konsentrert, (9) Hensiktsmessig og (10) Aksepterbar.
- Risikoledelse: Omfatter etablering av kontekst, risikoidentifikasjon, risikoanalyse, risikoevaluering og risikohåndtering. I tillegg kommer overvåking og gjennomgang samt kommunikasjon og konsultasjon.

Innholdet som her tillegges security-ledelse samsvarer i stor grad med hva som regnes som en god praksis innen safety. Etikk blir i mindre grad trukket fram som et selvstendig tema innen safety, selv om det kan argumenteres for at etikk vil være en underliggende forutsetning for etablering av sikkerhetskultur. Prinsipper for security vil i stor grad også være gyldige også innen safety. Et unntak er prinsippet om uforutsigbarhet, og som er diskutert i kapittel 7.2.2 av denne oppgaven. Samtidig er det også viktig å merke seg at flere av prinsippene legger føringer for grensesnittet mellom safety og security, eksempelvis prinsippet om at security skal være samarbeidene og at tiltak skal være hensiktsmessige og aksepterbare.

Metodikken for risikoanalyse (3-faktor modellen) avviker fra det som brukes i safety, men risikoledelsen følger i utgangspunktet samme systematikk som innen safety. Dette fordi den baserer seg på en allmenn modell for risikostyring (International Organisation for Standardization, 2018). (Bieder & Pettersen Gould, 2020) anser at både safety og security bør kunne håndteres innenfor et overordnet rammeverk for risikostyring. I dette viser de til (Leveson, 2020) sin tilnærming om at begge handler om systemets tap av kontroll, og at det derfor ikke er nødvendig å skille mellom måten de vurderes og håndteres. Det er derfor fullt mulig å inkludere security-trusler til feil-scenario i eksisterende sikkerhetsanalyser innenfor safety. (Bieder & Pettersen Gould, 2020) ser imidlertid

noen utfordringer i å blande safety og security. Den ene av disse er insidertrusselen, der man i utgangspunktet kan ha personer som er gitt tillit for å håndtere safety, men samtidig representerer en security trussel. Germanwings-piloten som med overlegg styrtet eget fly i 2015 er et eksempel på dette. Den andre utfordringen er at security-relaterte trusler ofte kan utnytte sårbarheter utenfor organisasjonens grenser.

4.1.3 Utfordringer mellom safety og security på virksomhetsnivå

Mye av forskningen rundt samspillet mellom safety og security er gjort enten på konseptnivå eller omhandler tekniske konstruksjoner. Selv om fagområdene har eksistert side om side i mange år, er det lite forskning på den praktiske implementeringen (Pettersen Gould & Bieder, 2020). Et unntak er en studie som tok for seg utfordringer rundt innføringen av ny og strengere security-regulering ved norske flyplasser (Pettersen & Bjørnskau, 2014). Dette er en sektor preget av en strømlinjeformet drift og der det er lite organisatorisk slakk til å tilpasse seg nye situasjoner. Organisasjonene er videre å anse som høypålitelighetsorganisasjoner (kapittel 4.2) og er avhengige av å kunne agere på svake signaler på at noe er galt. Sektoren er derfor avhengig av god og direkte kommunikasjon, samtidig som vurderinger og beslutninger løpende blir foretatt av fagpersonell på et lavere nivå i organisasjonen. Kulturen i sektoren er preget av tillit, og av at de ansatte aksepterer de reglene som gjelder, samtidig som de oppfatter at de behandles rettferdig om de begår feil eller om reglene blir brutt.

Det nye regimet for security i luftfarten ble innført på bakgrunn av et oppdatert direktiv fra EU og motivert i terrorhandlingene i USA 11.09.2011. Direktivet var preskriptivt av natur og det var ikke rom for lokale tilpasninger ved den enkelte flyplass. Implementeringen ble i stor grad foretatt av en organisasjon som var uavhengig av den som ivaretok safety. En sammenligning mellom organisering for safety og security er gitt i tabell 1.

Tabell 1: *Sammenligning av safety og security organisering knyttet til implementering av nytt regime for luftfartssikkerhet (Oversatt fra* (Pettersen & Bjørnskau, 2014)*).*

	Safety organisering	**Security organisering**
Trusler (mål):	Interne og regelmessige.	Eksterne og tilfeldige.
Utfall som motiverer tiltakene/opptreden:	Kjent/basert på evidens eller erfaring.	Ukjent.
Organisatoriske strukturer:	Funksjonelt med lokale nettverk.	Autokratisk.
Klima:	Søker tillit.	Mistenksom.
Makt:	Legitimitet/ekspert.	Korrektiv.

Studien ble gjennomført som en kvantitativ undersøkelse blant 675 ansatte og resultatene ble analysert statistisk. Viktige funn i studien var bl.a. følgende:

- Flertallet anså at security-tiltakene hadde gitt en forringelse i kommunikasjonen mellom de ulike yrkesgruppene.
- Mange ansatte anså tiltakene som urimelige og hadde problemer med å forstå motivasjonen bak tiltakene og sammenhengen mellom utformingen av tiltakene og forventet gevinst. Blant disse var det også enkelte som betvilte effektiviteten av tiltakene.
- Det var enkelte som var frustrert over tiltakene. Det var mange av flymannskapet som anså at de tapte autoritet om de ble undersøkt foran passasjerene. Det var også ansatte som

følte seg mistenkeliggjort, både blant flymannskap og bakkemannskap hvis daglige oppgaver bestod i å ivareta sikkerheten.

- Det var mange som opplevde måten sikkerhetskontrollen ble gjennomført på som stressende.

4.2 Sentrale teoriretninger innen sikkerhet

For å være i stand til å forebygge og håndtere hendelser og ulykker, trenger man en forståelse for hvorfor disse skjer og hvordan de utvikler seg. Innenfor akademisk teori, og som ligger til grunn for virksomhetenes arbeid med sikkerhet finnes det flere dels overlappende og dels kompletterende teorier rundt dette. Hvilket teoretisk perspektiv man legger til grunn vil ha betydning for hvordan man i praksis arbeider med sikkerhet, blant annet i form av overvåkingen av risiko og strategi for risikoreduksjon. I denne oppgaven er det tatt utgangspunkt i fem teoretiske perspektiver (tabell 2) og som er allment anerkjent som en del av det teoretiske grunnlaget innen sikkerhet. Bakgrunnen for valget av disse, er at de har en distinkt forklaring på årsaken til at hendelser skjer og gir en retning for hvordan man bør jobbe for å forebygge hendelser. Andre teorier, som Safety II og Resilience Engineering, tilbyr i mindre grad en egen årsaksforklaring på hvorfor hendelser skjer. Dette utelukker ikke at de kan være svært nyttige innen safety, og sannsynligvis innen security. Å skulle legge et maktperspektiv til grunn for analyse i egen organisasjon vil sannsynligvis vært svært krevende.

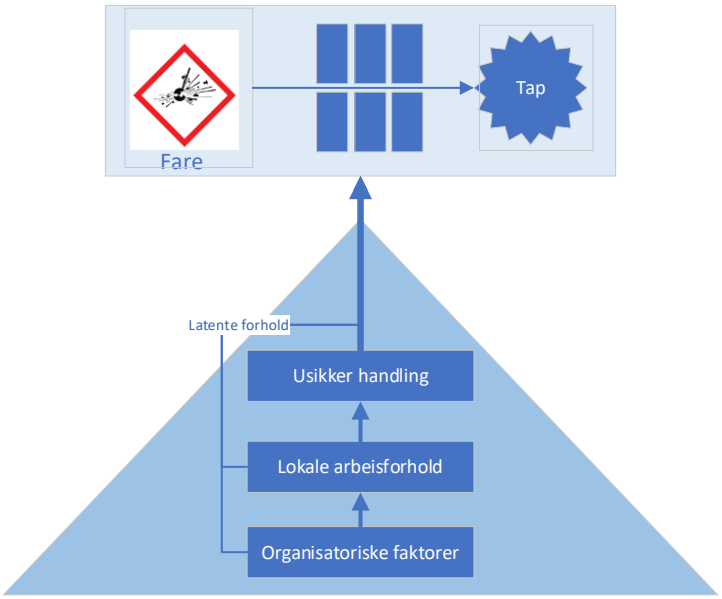
Tabell 2: Oppsummering av fem perspektiver for sikkerhet (basert på (Rosness, et al., 2004)).

Tema	**Energi og barriere-perspektivet**	**Normalulykke - perspektivet**	**HRO - perspektivet**	**Informations-prosesserings-perspektivet**	**Beslutnings-perspektivet**
Hvorfor skjer større ulykker?	Hendelse i kombinasjon med latent forhold gir brudd i samtlige barrierer i dybdeforsvaret	Komponentfeil forplanter seg i tett koblede systemer. Vanskelig å forutsi hvordan feilen utvikler seg i systemer med komplekse interaksjoner.	Som i NAT	Rigid tro og antagelser i organisasjonen medfører feiltolkning av informasjon om framvoksende farer.	Konflikter mellom motstridende mål.
Hvordan kan risiko for større ulykker overvåkes?	Overvåkning av kvalitet/effektivitet til barrierer.	Overvåkning av interaktivitet og kompleksitet i koblinger. Overvåke samsvar mellom kontroll-strukturer og teknologi.	Overvåke strukturelle og kulturelle forutsetninger for organisatorisk redundans.	Kombinere risikovurderinger med helhetlig tilnærming til menneskelige og organisatoriske faktorer. Kontrollere organisasjonens evne til å følge opp tegn på farer, eksempelvis nestenulykker.	Er tilbakemeldinger fra ulike organisasjonsnivå åpen? Strategiske verktøy som balansert målstyring kan være til hjelp.
Strategier for risiko-reduksjon	Dybdeforsvar gjennom barriere-funksjoner i konstruksjon av systemer. Kompenserende tiltak ved utfall av barrierer.	Redusere kompleksitet og løsne koblinger. Sentralisert kontroll av systemer med komplekse interaksjoner. Desentralisert	Bygge organisatorisk redundans. Bygge kultur som kombinerer krav om feilfri ytelse med åpenhet for	Systematisk arbeid med å samle og analysere informasjon om farer. Bygge kultur som fremmer aktivt søk etter signaler på farer, samt deling av	Gjøre grensen for uakseptabel ytelse tydelig og håndgripelig. Etabler motkrefter som favoriserer sikker adferd. Hold fokus på situasjoner hvor den enkelte medvirker

	Overvåking og vedlikehold av barrierer under systemets levetid.	kontroll over systemer med tette koblinger. Unngå systemer med komplekse interaksjoner og tette koblinger.	faktum at feil vil oppstå.	kunnskap ut over organisasjonens grenser.	har begrenset oversikt over den totale situasjonen.

Perspektivene for sikkerhet er del av et felles kunnskapsgrunnlag delt mellom safety og security og alle disse er i utstrakt bruk innen safety. Innen security er det primært energi-barriere-perspektivet som har fått sin utbredelse (Jore, 2019). I diskusjonsdelen av denne oppgaven vil det bli argumentert for at ulikheter i teoretiske perspektiver er en underliggende årsak til at man tenker ulikt mellom safety og security, og at dette har en vesentlig betydning for hvordan man tenker rundt årsak og utvikling av hendelser, men også rundt viktigheten av informasjonsflyt og rundt viktige verdier som åpenhet og tillit. Det er derfor i dette kapitlet valgt å gi en kort oppsummering av de teoretiske perspektivene.

Et allment perspektiv på sikkerhet, og med sin opprinnelse tilbake på 1960-tallet, er den såkalte Energi-barriere-modellen, eller «sveitserostmodellen». Utgangspunktet for denne modellen er et system bestående av en energikilde og barrierer som skal forhindre at farlig energi frigis og forårsaker skade på et sårbart objekt. En ulykke vil i henhold til denne modellen forårsakes ved tap av kontroll over energien og som medfører brudd i barrierene og skade på det sårbare objektet. Barrierene i et slik system kan være fysiske (f.eks. en brannvegg) eller administrative (f.eks. en kontrollprosedyre), og begrepet «forsvar i dybden» brukes til å beskrive et system sammensatt av preventive og konsekvensreduserende barrierer.

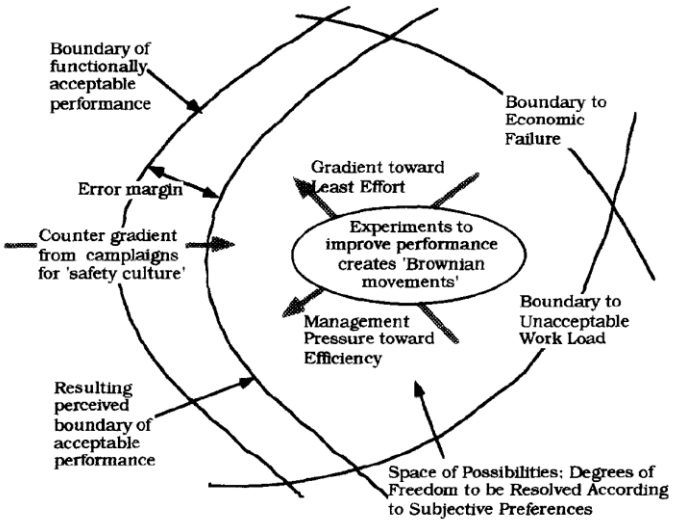


Figur 1*: Reasons framstilling av vekselvirkingen mellom usikker handling, lokale arbeidsforhold og organisatoriske faktorer (* **(Reason, 1997)** *side 17).*

Mens energi-barriere modellen beskriver et system med et enkelt årsaks-virkningsforhold, ble dette perspektivet utvidet gjennom teoriene til Reason for å beskrive organisatoriske ulykker. Typisk for organisatoriske ulykker er at de involvere mange ulike personer på ulikt sted i organisasjonen og har et svært sammensatt årsaksforhold. Konsekvenser av organisatoriske ulykker kan være katastrofale, men slike ulykker er heldigvis sjeldnere enn enklere ulykker som f.eks. HMS hendelser. I Reasons

modell for organisatoriske ulykker (figur 1) settes den usikre handlingen, som er den direkte årsaken til ulykken, inn i en systemkontekst sammen med lokale arbeidsforhold og organisatoriske faktorer. Utgangspunktet for Reasons teori er at det i alle systemer vil finnes såkalte latente forhold, og som i kombinasjon med en usikker handling vil kunne utløse en hendelse som trenger gjennom alle lag i forsvaret i dybden. Disse forholdene, og som av (Westerum & Adimski, 2009) betegnes som «latente patogener», vil kunne ha ligget uoppdaget i organisasjonen i årevis og vil være forårsaket av lokale arbeidsforhold (f.eks. stress, dårlig design eller dårlig utstyr) og som igjen vil ha sitt opphav i organisatoriske forhold (f.eks. dårlig lederskap, mangelfull trening, uklarhet i ansvar etc.). En situasjon der man ikke aktivt jobber med å identifisere og håndtere de latente forholdene («Don't rock the boat») medfører en degradering av dybdeforsvaret (dvs. «flere og større hull i sveitserosten»).

Beslutningsperspektivet handler om at enhver organisasjon, og organisasjonens medlemmer, til enhver tid må balansere mellom motstridende mål. Den klassiske konflikten vil være mellom produksjon og sikkerhet. En uforsvarlig vektlegging av produksjon kan medføre katastrofe og et overdrevent vektlegging av sikkerhet kan medføre konkurs (Reason, 1997) (s 4-5). Samtidig vil også menneskene i organisasjonen ha motstridende mål, inkludert mellom å ivareta sikkerheten opp mot å skape en behagelig og meningsfylt hverdag. Organisasjonen er derfor i konstant bevegelse mellom disse målene, og ulykker skjer da i form av utglidninger i adferd og som bryter grensen for hva som sikkerhetsmessig er akseptabelt (Figur 2).



Figur 2: Visuell framstilling av målkonflikter i beslutningsperspektivet (Rasmussen, 1997).

Innenfor informasjonsprosesserings-perspektivet anses ulykker å være et resultat av sammenbrudd i informasjonsflyt eller i tolkning av informasjon relatert til fysiske hendelser. Informasjonsflyt-perspektivet er knyttet opp til virksomhetens kultur ved at organisasjonen over tid, i den såkalte inkubasjonsperioden, bygger seg opp rigid tro og antagelse om farer og måten virksomheten håndterer disse på og en undervurdering av framvoksende farer. Denne perioden kjennetegnes videre av manglende samsvar med diskreditert eller utdatert regelverk, ignorering av klager utenfra, informasjonsutfordringer og støy, samt løsninger som ikke adresserer rotårsaken til problemene. Ofte vil involvering av fremmede, og som ikke har fått tilstrekkelig opplæring, medvirke til en utløsende hendelse for en ulykke.

Perrows teori om normalulykker «Normal Accident Teory» (NAT)) tar for seg komplekse systemer, og der mindre feil (på komponentnivå) vil kunne eskalere til komplekse ulykker (og som omfatter store deler eller hele systemet) gjennom uventede interaksjoner mellom flere latente og aktive feil. Begrepene interaksjon og kobling er sentrale i NAT:

- Interaksjon betegner komponentenes evne til å vekselvirke utenfor sin naturlige produksjonssekvens. Kompleks interaksjon kjennetegnes av at komponenter interagerer med komponenter i andre systemer, noe som kan gi opphav til uforutsigbare hendelsessekvenser. Lineære interaksjoner gjør ikke det.
- Koblinger beskriver i hvilken grad det er «slakk» i systemet. I tett koblede systemer er man avhengig av at aksjoner og prosesser skjer til en bestemt tid og i en bestemt rekkefølge. I løst koblede systemer er man ikke det.

Perrow anser videre at systemer med tette koblinger må ha en sentralisert styring, mens systemer som har komplekse interaksjoner må styres desentralisert. Han mener videre at det ikke er mulig å styre virksomheter, som kjernekraftverk, som kombinerer tette koblinger og komplekse interaksjoner, og at normalulykker derfor er uunngåelige.

Høypålitelighetsorganisasjons-teorien («High Reliability Organisation» (HRO)-teorien) er basert på studier av organisasjoner som har vist evne til å håndtere komplekse systemer uten at dette medfører ulykker, og ble etablert for å utfordre NAT. Sentrale konsepter i HRO er å bygge organisatorisk redundans og kapasitet, samt å kunne tilpasse seg krevende situasjoner og kriser. Sentrale aspekter i HRO-perspektivet er:

- Feiltoleranse gjennom organisatorisk redundans. I dette ligger at personer med overlappende ansvar og kompetanse i kritiske situasjoner har øye-til-øye kontakt og god kommunikasjon. Feil og avvik vil da kunne korrigeres umiddelbart før de får utviklet seg.
- Evnen til spontant å rekonfigurere organisasjonen. I dette ligger at man under normale forhold har klart definerte kommandolinjer, men ved kriser har en mer fleksibel organisering og der medarbeidere gis autoritet basert på kunnskap heller enn formell rang.
- Evnen til å kombinere sentralisert og desentralisert kontroll.
- Følelsen av «mindfullness». I dette ligger en forventning og oppmerksomhet rundt det uventede, samt vektlegging av å håndtere det ukjente gjennom forpliktelse og ekspertise.

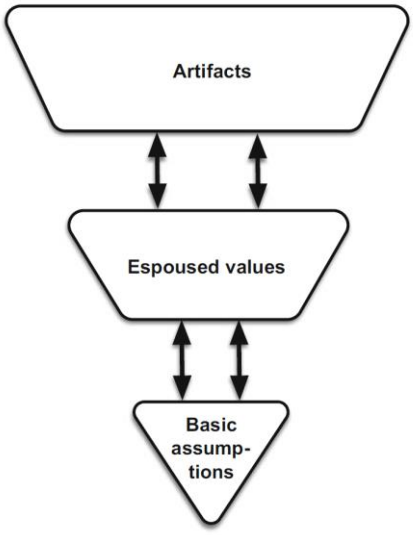
4.3 Sikkerhetskultur

Ett av forskningsspørsmålene i denne oppgaven omhandler i hvilken grad kultur vil kunne medvirke til tettere integrering mellom safety og security. For å være i stand til å diskutere dette spørsmålet, må vi først se på hva vi mener med sikkerhetskultur og hvorvidt sikkerhetskultur er å anse som et nyttig og viktig konsept. Samtidig er det viktig å være kjent med hvilke egenskaper som kjennetegner god og dårlig sikkerhetskultur og å ha en forståelse for i hvilken grad en kultur vil være formbar og hvordan den kan formes. Samtidig med dette er det innen teorien liten grad av konsensus knyttet til hva man legger i begrepet sikkerhetskultur eller om hvordan den formes. Med dette som utgangspunkt, er det i denne delen av teorikapitlet tatt utgangspunkt i litteratur med litt ulik tilnærming til temaet sikkerhetskultur og som vektlegger litt ulike aspekter rundt temaet. Det er i utvalget av referanser valgt også å referere nyere arbeider, i tillegg til «klassikere» som Schein og Reason.

4.3.1 Hva mener vi med sikkerhetskultur?

Det er i utgangspunktet vanskelig å definere hva som er essensen i «kultur», ut over at kultur representerer en legemliggjøring av verdier, normer, meninger, overbevisning, antagelser etc. Kultur er videre noe som oppstår der mennesker bor eller arbeider sammen og som gir en felles forståelse av virkeligheten, og som gjør det mulig for mennesker å forstå og fungere i verden. Kultur eksisterer mellom mennesker og blir aktivert når disse møtes, ser symboler fra, eller gjennomfører ritualer i henhold til kulturen de har tilegnet seg. Personer kan derfor bære i seg flere ulike kulturer og som framkalles i ulike kontekster, f.eks. på jobb, hjemme og under fritidsaktiviteter. En mye brukt framstilling av kultur er Scheins modell (figur 3), og som representerer kulturen slik den kan betraktes fra utsiden. Modellen kan ses som en påminnelse om «ikke å skue hunden på hårene», dvs. at det som er mest synlig oppe i dagen, ikke nødvendigvis representere den kulturen som ligger under. I henhold til denne modellen, kan kultur deles inn i tre lag (Guldenmund, 2018):

- Grunnleggende antagelser. Dette er kjernen i kulturen og utgjør de grunnleggende antagelsene holdt av organisasjonen. Disse består typisk av fastholdt overbevisning («strong held beliefs»), verdier, normer, etc.
- Eksponerte verdier. Dette er det midtre laget i modellen og som er håndgripelige, men som ikke direkte lar seg oversette til de grunnleggende antagelsene. Dette kan typisk være det personer svarer når de blir spurt om noe, men som ikke nødvendigvis avslører det som ligger på et dypere nivå. Eksempler kan være gode intensjoner, framtidige ambisjoner, en sosialt akseptert forestilling eller et politisk korrekt svar.
- Artefakter. Dette er det ytre laget, eller fasaden, og som er mest synlig, men som ikke nødvendigvis sier så veldig mye om kulturen under.



Figur 3: Scheins modell for sikkerhetskultur

Begrepet «sikkerhetskultur» brukes gjerne for å betegne sikkerhetsmessig opptreden innenfor en definert gruppe og hvordan denne er forankret i dypereliggende forhold (f.eks. verdier og holdninger) innenfor denne gruppen. Sikkerhetskultur er i utgangspunktet ikke et konkret håndgripelig fenomen eller en målbar størrelse, men er mer å anse som en sosialt konstruert forklaringsmodell på sikkerhetsmessig adferd. Det kan også stilles spørsmål til om det finnes en egen sikkerhetskultur, men heller egenskaper med en større organisasjonskultur og som påvirker

organisasjonens sikkerhetsnivå (Antonsen, 2009). I likhet med begrepet «sikkerhet», har heller ikke begrepet «sikkerhetskultur» en omforent definisjon og det finnes mer enn 50 ulike definisjoner av sikkerhet og sikkerhetskultur, noe som skaper betydelig forvirring både innenfor industrien og akademia (Cooper, 2018).

En måte å bruke konseptet sikkerhetskultur på, og som anses å ha en nytteverdi, er som redskap til selvrefleksjon. I dette ligger at organisasjonen ved hjelp av flere supplerende metodikker beskriver ulike aspekter ved egen kultur og «lag for lag prøver å arbeide seg inn mot kjernen» slik at organisasjonen får en bedre selvinnsikt i sine delte oppfatninger, antagelser, handlingsmønstre og hva som holder dem tilbake (Guldenmund, 2018).

Sikkerhetskultur handler primært om de valgene individer eller grupper tar i situasjoner som medfører risiko. Begrepet risikoadferd («At-Risk-Behavior») beskriver i denne sammenhengen handlinger der individer eller grupper tar risikable valg ubevisst eller feilaktig vurderer sine handlinger som sikre. Selv om det i alle organisasjoner vil kunne finnes individer med avvikende eller kriminell adferd, har slik risikoadferd som regel ikke til hensikt å forårsake skade. Kulturbegrepet er uavhengig av om handlingene faktisk medfører skade eller ikke. I denne sammenheng er det viktig at feil kan skje uten at dette nødvendigvis kan tilskrives mangler i sikkerhetskultur og at mangler i sikkerhetskultur ikke nødvendigvis manifesterer seg i form av skade. Det kan videre være flere årsaker til risikoadferd, og det er derfor viktig å forstå disse årsakene for å arbeide med å påvirke kulturen. Eksempelvis vil det ikke bestandig være lett å se farene som skal unngås ved sikkerhetsreglene. Alternativt kan det være incentiver i systemet som belønner avvik fra sikkerhetsreglene (Marx, 2018).

I følge (Guldenmund, 2018), blir sikkerhetskulturbegrepet ofte misbrukt både som en årsaksforklaring på noe som har skjedd og til negativt å stemple organisasjoner eller grupperinger i organisasjoner. Selv om det kan være både enkelt og overbevisende å snakke om sikkerhetskultur i en slik sammenheng, er dette, ifølge Guldenmund, hverken sannferdig eller nyttig. En negativ effekt av å årsakforklare ulykker med mangelfull sikkerhetskultur, kan være at dette hindrer organisatorisk læring. Dette fordi et stempel av at det er noe galt med den aktuelle organisasjonen, kan medføre en formening om at tilsvarende ulykker ikke kan skje andre steder. Tilsvarende er det, i ifølge (Antonsen, 2009), i fagmiljøene diskusjoner rundt om vektlegging av sikkerhetskultur går på bekostning av nye og sikrere løsninger basert på teknologi. I dette ligger en avveiing mellom å kompensere for farer gjennom (myke) prosedyremessig tiltak eller å kunne eliminere en fare ved hjelp av (hard) teknologi.

Det er innen akademia noe divergerende oppfatning av hvor viktig sikkerhetskultur i realiteten er. På spørsmål om hvorfor ikke Perrow nevnte kultur i sin berømte bok om normalulykker fra 1984, svarte han at han ikke anså det som nyttig. Selv om han selvfølgelig anerkjenner at det er kultur i selskaper, anser han at det er makt som er det viktige temaet når det gjelder risiko og sikkerhet og da mye viktigere enn verdier og tro. Makt og utøvelse av makt er videre dokumentert som en viktig årsak til ulykker (eksempelvis Challanger-ulykken i 1986) og er dessuten viktig for bl.a. hva organisasjonen anser som risiko. Forholdet mellom makt og sikkerhetskultur er lite studert i litteraturen (Antonsen, 2009).

4.3.2 Kjennetegn ved god og dårlig sikkerhetskultur

Begrepet «sikkerhetskultur» er normativt i den forstand at det er gitte egenskaper ved en organisasjonskultur som anses som ønskelige og som fremmer sikkerhet, mens andre ikke er det.

Westerun har identifisert tre generiske organisasjonstyper, med utgangspunkt i Reasons modell for organisatoriske ulykker (kapittel 4.2): Patologiske organisasjoner, byråkratiske organisasjoner og generative organisasjoner (tabell 3.) (Westerum & Adimski, 2009). I dette ligger at patologiske organisasjoner tenderer til å undertrykke og kapsle inn unormaliteter, heller enn å forholde seg til dem og løse dem. Byråkratiske organisasjoner kan ha gode rutiner for å løse forutsigbare problemer, men er dårlige til å identifisere og håndtere latente patogener (kapittel 4.2). Generative organisasjoner kjennetegnes av god kommunikasjon, god evne til selvorganisering og er flinke til å identifisere rotårsaken til problemer som ikke ligger lett synlig oppe i dagen.

Tabell 3: Sammenfatning av Westerums typologi for sikkerhetskultur (Westerum & Adimski, 2009)

Patologisk	**Byråkratisk**	**Generativ**
Informasjon er skjult.	Informasjon ignoreres.	Informasjon søkes aktivt.
Varslere blir skutt.	Varslere blir tolerert.	Varslere blir trent.
Ansvar blir krympet.	Ansvar er oppdelt.	Ansvar er delt.
Brobygging blir frarådet.	Brobygging er tillatt, men ikke oppfordret.	Brobygging er belønnet.
Feil dekkes til.	Organisasjonen er rettferdig og barmhjertig.	Feil medfører granskninger.
Nye ideer blir knust.	Nye ideer forårsaker problemer.	Nye ideer ønskes velkommen.

En egenskap ved enkelte virksomheter med negativ kultur, er såkalt «lært hjelpeløshet». Dette kjennetegnes av at medarbeidere lærer seg til at forsøk på å endre egen situasjon er nytteløs, gir opp og mister energi. Et noe tilsvarende fenomen er angst-unngåelse («anxiety-avoidance»), der organisasjoner oppdager en teknikk for å redusere sin kollektive angst og bruker denne om og om igjen uavhengig av om den faktisk virker. I dette ligger at organisasjonen tillegger seg ritualer, tankemønster og handlingsmønstre og som opprinnelig var motivert i å unngå smerte. Disse mønstrene blir ikke utfordret selv om årsaken til den opprinnelige smerten forsvinner, fordi unngåelse av angsten gir en positiv forsterkning (Reason, 1997)(s 193).

4.3.3 Utvikling av sikkerhetskultur

Kultur skapes spontant der mennesker møtes og man ser i prinsippet for seg en prosess der en felles virkelighetsoppfatning etableres, utveksles, formaliseres, overføres og forsterkes som indikert i figur 4. Det finnes imidlertid få, om noen studier, av hvordan sikkerhetskultur faktisk blir dannet i en organisasjon og utviklingen blir ofte forklart med «komplekse sosiale prosesser» (Antonsen, 2009).

Figur 4: *Modell for utvikling av kultur*

Reason anser at sikkerhetskultur kan konstrueres, på en ingeniørmessig måte, gjennom å identifisere å produsere elementene og sette dem sammen til en fungerende helhet. For Reason handler kulturbyggingen om praktisk arbeid om systemer og prosesser, heller enn om å skulle påvirke verdiene til organisasjonen. Sagt med hans egne ord (Reason, 1997)(s 192): *«Many people talk as if a safety culture can only be achieved through sine awesome transformation, akin to a religious experience".* Reasons perspektiv på sikkerhetskultur er naturlig nok basert på hans teorier rundt sikkerhet for organisatoriske ulykker (kapittel 4.2). Elementene som ifølge Reason må bygges er (Reason, 1997)(s 191-222):

- En rapporterende kultur, dvs. en kultur (og et system) for å rapportere og analysere hendelser for å sikre erfaringstilbakeføring og organisatorisk læring.
- En rettferdig kultur, dvs. en kultur der det er forhåndsdefinerte og kjente kriterier for hva som er akseptabel og uakseptabel opptreden og der dette vurderes uavhengig av om opptredenen har medført et vellykket utfall eller ikke.
- En fleksibel kultur, dvs. en kultur der beslutningsmyndighet for å løse akutt oppdukkende problemer kan delegeres ned i organisasjonen.
- En lærende kultur, dvs. en kultur som er i stand til å observere, reflektere, skape og handle.

Reason har lite tro på å skulle endre kollektive verdier, og viser til organisasjonsantropologien Hofstede (Reason, s 194): *"Changing collective values of adult people in an intended direction is extremely difficult, if not impossible. Values do change, but not according to someone's master plan. Collective practiced, however, deponent om organizational characteristics like structures and systems, and can be influenced in more or less predictable ways by changing these".*

I følge (Hopkins, 2018) er det ikke noe motsetningsforhold i å skulle endre kulturen gjennom å endre praksis. Fra psykologien vet man at mennesker vil kjenne ubehag om ikke handlinger stemmer overens med verdier, og at verdier derfor vil endres slik at de stemmer overens med handlingene. Over tid vil endringer i praksis medføre endringer i kulturen gjennom endringer i kollektive verdier og antagelse. Hopkins trekker fram bruken av bilbelte som et eksempel på dette, og der påbud og sanksjoner har medført en holdningsendring og aksept for at bruk av bilbelte er en god ide (Hopkins, 2018).

Struktur og lederskap blir av (Hopkins, 2018) framhold som de viktigste forutsetningene for å etablere en god sikkerhetskultur. Eksempler på struktur kan i denne sammenhengen være formelle organisasjonsstrukturer (eksempelvis hvilke funksjoner som deltar i ulike ledergrupper), men også hvilke faktorer organisasjonen rapporterer på og blir målt på. Rammen rundt virksomheten i form av myndigheter, regelverk etc. vil også være en del av disse strukturene. Kultur formes av hva ledelsen legger til rette for, og man kan eksempelvis få en byråkratisk kultur eller en kultur for hemmelighold om ledelsen legger til rette for dette. Kulturen vil videre formes av hva ledelsen gir sin oppmerksomhet. Dette omfatter alt fra hva ledelsen i det daglige legger merke til og kommenterer, til virksomhetens mer strukturerte systemer for måling og styring samt tilhørende incentiver. Det er derfor viktig at det strukturelle blir tilpasset det utkommet man ønsker.

For (Westerum & Adimski, 2009) er sikkerhetskultur kun ett av flere elementer i det de beskriver som den menneskelige konvolutt og som omkranser de sosiotekniske systemene. Westerum & Adimski bruker i denne sammenheng begrepet høyintegritets kultur om en kultur som på en god måte integrerer konstruksjon, drift og vedlikehold inn i et høyintegritets sosioteknisk system. Westerum & Adimski anser at organisasjonskultur både kan fremme og degradere den menneskelige konvolutten. En slik høyintegritets kultur er derfor ett av seks elementer i Westerums menneskelige konvolutt sammen med (1) riktig utstyr, (2) bruken av utstyret, (3) vedlikehold av de menneskelige

aktiva, (4) styring av grensesnitt og (5) evaluering og læring. Westerum & Adimski trekker spesielt fram kommunikasjon og godt klima for samarbeid som viktige for etablering av en høyintegritets kultur. Viktige egenskaper ved en høyintegritets kultur vil være evnen til trening, koordinering, tilpassingsevne, involvering, informasjonsprosessering, beslutningstagning, læring, ressursstyring og forestillingsevne. Westerum & Adimski er også tydelig på at den menneskelige konvolutten ikke er begrenset til egen organisasjonen, men også omfatter viktige interessenter som bl.a. leverandører og regulerende myndigheter.

En utfordring knyttet til etableringen av sikkerhetskultur er at sikkerhetskultur er vanskelig å måle, og mye av metodikken for måling og benchmarking av sikkerhetskultur mangler en god vitenskapelig forankring. I realiteten er mange av metodene som brukes i større grad rettet mot å kartlegge sikkerhetsklima, heller enn sikkerhetskultur. Sikkerhetsklima er i denne sammenheng en psykologisk variabel, og som beskriver holdninger og oppfatninger hos enkeltindivider i en gruppe. Dette utelukker imidlertid ikke at denne typen kartlegginger vil kunne ha en verdi brukt i en dialog om sikkerhet mellom ansatte (Guldenmund, 2018).

4.3.4 Felles overgripende sikkerhetskultur kontra flere subkulturer

Ideen om en felles enhetlig ledelsesstyrt virksomhetsovergripende sikkerhetskultur kan nok på mange virke besnærende, men må antas som svært krevende å få til. I organisasjoner over en gitt størrelse vil det bestandig være en horisontal fordeling av arbeidsoppgaver og en vertikal fordeling av makt, noe som også bidrar til kulturell differensiering. Ansatte med ulik faglige bakgrunn vil kunne representere noe ulik kultur, noe som i enkelte organisasjoner gir ulikheter mellom ledelseskultur, ingeniørkultur og driftskultur. Enkelte organisasjoner vil også kunne ha motsetninger mellom yrkesgrupper. Antonsen argumenterer for at det er fem forhold som kan sikre kulturell integrering på tvers av en organisasjon (Antonsen, 2018).

1. Kulturell homogenitet, dvs. om personer har felles nasjonal og etnisk kultur.
2. Felles ledelse for alle medlemmene i organisasjonen.
3. Felles organisasjonsstrukturer, webside, intranett, prosedyrer og styrende dokumenter.
4. Felles verdigrunnlag som beskriver hvordan organisasjonen ønsker å bli oppfattet av interne og eksterne.
5. Felles opplevelser, eksempelvis kriser eller katastrofer i nær fortid.

Westerum & Adimski peker på at subkulturer innenfor flyindustrien har vært en medvirkende årsak til ulykker med fatalt utfall, ved at subkulturer i gitte sammenhenger har vært til hinder for god koordinering i krisesituasjoner. (Westerum & Adimski, 2009).

Spørsmålet om hvorvidt sikkerhetskultur best formes «top-down» som en ledelsesstyrt prosess eller «bottom-up» som en profesjonsstyrt prosess blir diskutert av (Journé, 2018). Artikkelen tok for seg Safety-Culture-as-Tool (SCT), og som er et ledelsesverktøy utviklet av Det Internasjonale Atomenergibyrået (IAEA) og som skal hjelpe virksomheter i å skape en enhetlig sikkerhetskultur gjennom en prosess der kulturen skal læres, deles og implementeres av alle individer i organisasjonen. Denne ledelsesstyrte tilnærmingen ble i artikkelen vurdert opp mot en profesjonsstyrt tilnærming (Professional Safety Culture (PSC)s) der sikkerhetskultur defineres gjennomarbeidsgrupper, profesjons- og yrkesmessige grupper. Artikkelen konkluderte med at det er et relativt komplekst forhold mellom den ledelsesstyrte (SCT) og den profesjonsstyrte (PSC) tilnærmingen. Styrker med den ledelsesstyrte er at den gir en god strategisk forankring og også gir godt samsvar med strategiske og ledelsesmessige føringer på tvers av organisasjonen. Svakheten er

at den kan oppfattes å mangle relevans ved at den blir for overordnet og generell, og at det derfor blir vanskelig for ansatte å sette den inn i konteksten av egen arbeidshverdag. Motsatt finner man at de profesjonsdrevne sikkerhetskulturene vil være enklere for ansatte å forholde seg til. Ulempen med disse er bl.a. at de ikke nødvendigvis er godt forankret i strategiske mål, samtidig som det lett vil oppstå uoverensstemmelser mellom profesjonsgrupper og mellom profesjonsgrupper og ledelsen, slik at systemet totalt sett blir usammenhengende.

Tabell 4: *Sammenhengen mellom styrker og svakheter i ledelsesstyrt og profesjonsstyrt sikkerhetskultur.*

		Profesjonsstyrt (PCSs)	
Ledelsesstyrt (SCT)		**Svak**	**Sterk**
	Svak	**(1) Mangel på sikkerhetskultur** - Svak integrert. - Svak differensiering. Sårbarhet: ***Uakseptabel i høyrisiko industri***.	**(2) Profesjonell sikkerhetskultur** - Svak integrering. - Sterk differensiering. Sårbarhet: *Usammenhengende, konflikter, manglende strategisk forankring.*
	Sterk	**(3) Byråkratisk sikkerhetskultur** - Sterk integrering. - Svak differensiering. Sårbarhet: *Mangel på relevans, Ikke i stand til å håndtere komplekse problemer.*	**(4) HRO sikkerhetskultur** - Sterk integrering. - Sterk differensiering. Sårbarhet: *Forutsetter organisatorisk slakk som kan trues ved nedskjæringer.*

(Journé, 2018) argumenterer for at en god sikkerhetskultur må inneholde både et sterkt ledelsesstyrt element og et sterkt profesjonsstyrt element (tabell 4). En slik kultur forutsetter nødvendigvis en god del slakk, men vil bestå av ulike profesjonsgrupper som utfører sine oppgaver i tråd med en god faglig praksis. Dette i samspill med et sterkt ledelsesstyrt element som sikrer godt samsvar og god integrering på tvers av organisasjonen.

(Antonsen, 2009) er skeptisk til en sterkt toppstyrt maktorientert prosess der ledelsen prøver å tre sine verdier ned over organisasjonen og der sikkerhetskultur reduseres til et spørsmål om samsvar med regler og prosedyrer. En slik tilnærming vil utøke sikkerhetsstyringen fra å skulle kontrollere de ansattes handlinger til også å ville kontrollere deres hjerter og sinn. Bakgrunnen for denne skepsisen er at ledelsen rimeligvis har et perspektiv på hvordan sikkerheten skal ivaretas, men dette synet er ikke det eneste og heller ikke bestandig det mest riktige. I sum kan dette medføre at organisasjonen mister evnen til å ivareta og forbedre sikkerheten.

5 Metode

5.1 Forskingsdesign

Det empiriske arbeidet ble gjennomført gjennom strukturerte intervjuer med utvalgte medarbeidere i den studerte virksomheten. Intervjuene ble gjennomført fysisk, med unntak av ett som ble gjennomført på Teams.

Intervjuene ble gjennomført i henhold til intervjuguiden gitt i vedlegg 1, og som er strukturert basert på forskingsspørsmålene gitt i kapittel 3.2. Guiden er i stor grad basert på åpne spørsmål, for å unngå å legge føringer for svarene fra informantene. Ved behov ble det stilt avklaringsspørsmål for å verifisere at informantene ble forstått riktig. Hvert intervju ble dokumentert gjennom at informantens svar fortløpende ble notert ned i et svarskjema mens intervjuet pågikk. Informantene fikk tilsendt svarskjema i etterkant av intervjuene for kvalitetssjekk.

5.1.1 Utvalg av informanter

Det var totalt 9 informanter som deltok i undersøkelsen. I utvalget av informanter ble det vektlagt at det skulle være en tilnærmet lik sammensetning mellom personer med primære arbeidsoppgaver innen safety og security. Det ble også valgt noen informanter som hadde oppgaver knyttet til begge fagfelt. Det ble videre vektlagt at informantgruppen skulle representere begge lokaliteter, ulike stabsavdelinger og linjeorganisasjonen, samt en sammensetning både av ledere og medarbeidere. Medarbeidere er typisk tunge fagpersoner på sine områder og som ivaretar en rådgiverrolle.

Tabell 5: Oversikt over informanter som har blitt intervjuet i forbindelse med oppgaven.

Rolle	**Enhet**	**Fagområde**
Rådgiver	Sikkerhetsstab	Safety
Avdelingsleder	Sikkerhetsstab	Safety
Rådgiver (Beredskap)	Divisjonsstab	Safety og security
Sikkerhetssjef	Sikkerhetsstab	Safety og security
Info sikkerhetsleder	Sikkerhetsstab	Security
Avdelingsleder (Driftssjef)	Drift	Safety
Rådgiver	Sektorstab	Security
Avdelingsleder (Driftssjef)	Drift	Safety
Rådgiver (Beredskap)	Operativ sikkerhet	Security

5.2 Datareduksjon og analyse

Ved at empirien omfattet intervju av ni informanter, representerer svarskjemaene et stort datamateriale og det ble derfor vurdert som lite hensiktsmessig å gjengi intervjuene i sin helhet i denne oppgaven. Systematisering og strukturering av svarene ble gjort ved at svarene på hvert delspørsmål ble samlet og vurdert under ett. Svarene som framkommer i kapittel 6 av denne oppgaven er derfor et sammendrag av synspunktene som framkom på hvert av spørsmålene. I flere tilfeller framkom informantens synspunkt under et annen spørsmål enn det som opprinnelig var tenkt. Innholdet i synspunktet blir da reflektert under det spørsmålet hvor det naturlig hører hjemme.

Det er i oppsummeringen vektlagt å beskrive i hvilken grad et synspunkt har framkommet i mange, noen få eller i et enkelt intervju. Videre er det også vektlagt å få fram eventuelle divergerende synspunkter, da primært der disse synes å følge skillelinjer mellom safety og security. I noen tilfeller er det valgt å sitere informantene for å illustrere viktige poenger. Det er imidlertid ikke beskrevet hvem som har fremmet disse synspunktene, ut over at det i relevante tilfeller er angitt f.eks. at det er en lederfunksjon eller en informant fra safety eller security.

5.3 Teoriens validitet

Teoriretningene rundt sikkerhet, som beskrevet i kapittel 4.2 , er generelt anerkjent som en del av kunnskapsgrunnlaget innen safety, og må i så henseende anses å ha høy validitet. Som det framgår av kapittel 4.1.1, inngår disse teoriene også i kunnskapsgrunnlaget for security, men er i begrenset grad validert gjennom studier. Teoriretningene blir i denne oppgaven primært brukt i en diskusjon om ulikheter i faglige tilnærminger mellom safety og security. For dette formålet må de anses å ha høy validitet. Brukt i konteksten av det nukleære IFE, må det også antas at enkelte av teoriretningene i dag er mindre relevant enn tidligere. Dette fordi risikobildet er vesentlig endret etter at reaktorene ble stengt ned, eksempelvis ved at man ikke på samme måte som tidligere har sterke koblinger forårsaket av systemer under trykk og temperatur.

Konseptet sikkerhetskultur, beskrevet i kapittel 4.3, må anses å ha en begrenset validitet da det i liten grad eksisterer konsensus rundt sikkerhetskultur. Teorienes validitet brukt på security må tilsvarende antas som lavere enn innen safety, da teoriene i utgangspunktet er utviklet med tanke på safety. Mye av innholdet i teoriene rundt sikkerhetskultur må imidlertid anses som valide, f.eks. antagelsen og at institusjonaliserte verdier, virkelighetsforståelse, normer etc. vil ha en vesentlig betydning for hvordan virksomheter ivaretar sikkerheten. Tilsvarende gjelder også teoriene rundt betydningen av lederskap, struktur, viktigheten av en sterk profesjonskultur etc. for sikkerhet. Prosessene rundt hvordan sikkerhetskultur etableres og formes, er i liten grad forstått og må derfor anses å ha lavere validitet.

5.4 Intern validitet

Utvalget av informanter vil, for enhver undersøkelse, ha vesentlig betydning for utfallet. I denne undersøkelsen er det bevisst valgt personer som på forhånd var antatt å kunne ha interessante synspunkter og der sammensetningen av informantgruppen var antatt å gi en bredde i synspunkter. Det er imidlertid en betydelig skjevfordeling i at alle informantene enten har en lederrolle eller en rådgiverrolle. Ved at utvalget av informanter er begrenset, og fordi det er en skjevhet i utvalget av informanter, er det bevisst valgt ikke å gjøre noen statistisk bearbeiding av svarene.

Synspunkt som framkommer i undersøkelser vil bestandig basere seg på informantenes persepsjoner, og som igjen vil kunne påvirkes av dialog og interaksjoner. Det er derfor forventet at personer som samarbeider tett i det daglige vil ha mer sammenfallende synspunkt enn personer som i det daglige har lite kontakt. Det ble derfor i undersøkelsen valgt i størst mulig grad å velge informanter fra ulikt sted i organisasjonen. Noen synspunkt kan også være formet av at personer er direkte involvert i prosesser. Eksempelvis kan det virke som om enkelte ledere som har vært delaktige i å skulle etablere en løsning, synes som mer positive til denne enn enkelte av medarbeiderne er. I oppgaven er det valgt i liten grad å gå inn i denne typen problematikk, ut over å påpeke divergerende oppfatninger.

Det synes som om bruken av åpne spørsmål på enkelte punkt har medført en betydelig forskjell i hva informantene har vektlagt i svarene. Eksempelvis er det noen dilemma og årsaker som har blitt trukket fram av en eller noen få personer, og for disse er det uklart om de resterende informantene er enige i disse eller ikke. Ledende spørsmål kunne gitt avklaringer, men risiko for å påvirke informantenes svar gjorde at ledende spørsmål ble unngått – spesielt da arbeidet foregikk i egen organisasjon.

Bearbeiding av informasjonen forutsetter noe skjønnsmessig vurdering. Eksempelvis vil det ligge en grad av tolkning til grunn for å vurdere om to synspunkt formulert på ulik måte i praksis utrykker det samme. Tilsvarende ligger det også en skjønnsmessig vurdering i bearbeidingen av dataene, eksempelvis i måten dilemmaene er valgt formulert på. Dette gjelder også for hva som tolkes som et dilemma.

Gjennomføring av undersøkelser i egen organisasjon vil rimeligvis bestandig være krevende, og man vil bestandig i egen organisasjon ha gjort seg opp noen meninger på forhånd. I intervjusituasjonen ble det spesielt vektlagt å innta en nøytral, litt passiv og lyttende rolle. Det ble i utvalget av informanter vektlagt å inkludere personer fra andre deler av organisasjonen og som representerer andre synspunkter enn forfatterens.

5.5 Ekstern validitet

Ut fra det som er redegjort for i denne oppgaven, må man forvente at det vil oppstå dilemmaer mellom safety og security i organisasjoner der begge fagområder ønsker å sitte i førersetet for å definere innholdet i sikkerhetsarbeidet og understøttende sikkerhetskultur. Det er også godt kjent at grensesnittet mellom safety og security er krevende for mange virksomheter i nukleær sektor (International Atomic Energy Agency, 2021). Innholdet i dilemmaer, og hvor framtredende det enkelte dilemma er, vil nok i større grad variere mellom sektorer og virksomhetenes egenart.

Dilemma som har framkommet i denne oppgaven har i stor grad latt seg forklare gjennom ulikheter i faglige tilnærminger mellom safety og security, med unntak av dilemmaet rund sikkerhetsstyring og som i større grad forklares gjennom ulikheter i tradisjon og sedvane. Det er derfor rimelig å anta at dilemmaene vil være relevante også for andre virksomheter og i andre sektorer. Enkelte av dilemmaene har også likheter med hva som er beskrevet hos (Pettersen & Bjørnskau, 2014).

5.6 Etiske hensyn

Alle informantene som har deltatt i oppgaven, har gjort dette frivillig og er informert om hva undersøkelsen skal brukes til. Informantene har også fått tilsendt oppsummeringen av eget intervju for å rette opp eventuelle misforståelser og unøyaktigheter. Innholdet i enkeltintervjuene er heller ikke delt med andre. Det har ikke i noen intervjuer framkommet sensitive personopplysninger, kompromitterende informasjon om enkeltpersoner eller virksomheter, informasjon om kommersielle hensyn, skjermingsverdig informasjon eller noen annen type informasjon som er av en karakter som bryter med vilkårene i virksomhetens taushetserklæringer.

Funnene fra undersøkelsen er sammenfattet i et nøytralt språk, og med hensikt å framstille et produkt som vil kunne ha verdi for organisatorisk læring, også ut over virksomheten. Et begrenset antall enkeltutsagn fra undersøkelsen er gjengitt, da med hensikt å illustrere eller å tydeliggjøre ulikheter i faglig perspektiver. Alle utsagnene er anonymisert.

6 Empiri

Empiridelen oppsummerer synspunktene som har framkommet i intervjuene med informantene på de enkelte spørsmålene i intervjuguiden. Empirikapitlet representerer informantenes synspunkter rundt dilemmaene, deres årsaker, mulige løsninger og rundt kultur. Funnene i empirien blir diskutert opp mot gjeldene teori i diskusjonskapitlet.

Oppbyggingen av empirikapitlet følger i utgangspunktet samme struktur som forskningsspørsmålene og der kapittel 6.1 handler om de dilemmaene som informantene anser finnes i organisasjonen og deres opphav. Kapittel 6.2 handler om det mulighetsrommet som informantene anser at finnes for å løse dilemmaene. Kapittel 6.3 handler om i hvilken grad informantene anser at kultur vil være et egnet virkemiddel for å løse dilemmaene mellom safety og security.

6.1 Dilemma mellom safety og security

Som det framgår av teoridelen av oppgaven (kapittel 4.1.3) er det få studier av hvilke dilemma som oppstår i grensesnittet mellom safety og security i virksomheter, men tidligere studier har imidlertid dokumentert vesentlige utfordringer knyttet til flyten av informasjon som følge av implementering av omfattende tiltak innen security.

I denne delen av empirien var det ønskelig å undersøke hvilke dilemmaer informantene selv hadde observert i organisasjonen (kapittel 6.1.1), hva de anså at dilemmaene resulterte i (kapittel 6.1.2), hva de anså som mulig årsaker til dilemmaene (kapittel 6.1.3), samt hvordan de ble håndtert i det daglige (kapittel 6.1.4). For ytterligere å kunne forstå bakgrunnen for dilemmaene, var det lagt inn et spørsmål om i hvilken grad informantene anså at det var vesentlige forskjeller i hvordan man jobbet med farer innen safety og hvordan man jobber med trusler innen security (kapittel 6.1.5).

6.1.1 Hva dilemmaene består i?

På spørsmål om hvilke dilemma informantene hadde observert i organisasjonen, var det flere informanter som trakk fram at safety og security gjensidig påvirker hverandre. Eksempelvis vil gjennomføringen av tiltak innen safety kunne kompromittere security – og motsatt.
Tilbakemeldingen fra informantene om observerte dilemma er strukturert til å omfatte følgende kategorier:

- Åpenhet kontra hemmelighold.
- Tilgjengelighet kontra beskyttelse av informasjon.
- Insiderproblematikken.
- Beredskap.
- Risikostyring.
- Sikkerhetsstyring.

Det var generelt stor ulikhet i hva de ulike informantene anså som dilemma. Så godt som alle informantene hadde identifisert dilemmaene knyttet til informasjon. De andre dilemmaene var det kun enkeltinformanter, eller noen få informanter, som hadde identifisert.

I tillegg til de som er beskrevet over, var det flere av informantene som pekte på en del utfordringer av praktisk karakter i grensesnittet mellom safety og security. Eksempler på dette var rømning ved brann, dører som må holdes åpne som del av byggearbeider, HMS knyttet til kontroll av innkomne

varer i adgangskontrollen og bruk av synlighetstøy. Disse vil ikke bli behandlet videre i denne oppgaven, da oppgaven i større grad konsentrerer seg om mer prinsipielle forhold. Mange av disse utfordringene synes samtidig å ha funnet sin løsning.

6.1.1.1 Åpenhet kontra hemmelighold

I et flertall av intervjuene med informantene framkom det et dilemma rundt hemmelighold av informasjon, spesielt om bakgrunnen for tiltakene innen security. Innen security er man svært tilbakeholden med å gi innsikt i vurderingene som ligger til grunn for sikkerhetstiltak og disse er ukjente for de fleste som jobber på anleggene. Et eksempel fra et av intervjuene *«Jeg anser at en medvirkende årsak er at de som jobber med safety ikke får tilgang til sentral informasjon om security. De forstår for eksempel ikke hvorfor informasjon er sikkerhetsgradert. En bakenforliggende årsak til dette igjen er dårlig samhandling».*

Det er dog verd å merke seg at det også blant informanter innen security framkom et divergerende syn rundt delingen av denne typen informasjon. En av informantene anså at det er et større problem med for lite enn med for mye informasjon, og at det var flere eksempler på at gradert informasjon ikke hadde blitt delt videre til medarbeidere som hadde et behov for denne.

Man har ved IFE lang tradisjon for åpenhet rundt farene ved anleggene. Innen safety ønsker man at ansatte skal forstå farene og bakgrunnen for sikkerhetstiltakene, og der tiltak eksempelvis kan være regler eller arbeidsmåter som er etablert for å unngå hendelser eller strålingseksponering. Dette inkluderer også kunnskap om den sikkerhetsmessige betydningen til ulike anleggsdeler, samt hvordan de ulike delene av anleggene virker sammen. Det er videre lang tradisjon i fritt å kunne dele informasjon innen en gruppe og å diskutere problemer og mulige løsninger.

6.1.1.2 Konfidensialitet kontra tilgjengelighet for informasjon

Tiltak for å beskytte konfidensialiteten til informasjon kontra informasjonens tilgjengelighet, var et sentralt tema i flere intervjuer. Det var imidlertid noe ulikhet i hvilke aspekter av dette informantene vektla. Det framkom ikke noe i intervjuene som tilsa uenighet om at det var et behov for å beskytte informasjon. Divergerende oppfatninger gikk mer på utforming og omfang av tiltakene.

Det framkom blant informantene noe ulik oppfatning knyttet til skadepotensialet om informasjon kommer på avveie og behovet for beskyttelse av informasjonens konfidensialitet. Det var også flere informanter som gav utrykk for at verdivurdering og gradering av informasjon var svært krevende, da de ikke var kjent med grunnlaget for beskyttelsen av informasjonen. I dette lå blant annet hvilken trussel informasjonen skulle beskyttes mot og hva slags informasjon som potensielt kunne misbrukes. Dette dilemmaet er derfor tett knyttet opp til dilemma 1 «Åpenhet kontra hemmelighold».

Enkelte informanter pekte her på at informasjonssikkerhet handler om å sikre informasjonens integritet og tilgjengelighet – og ikke kun konfidensialitet. Dette ble spesielt utrykt av en av informantene: *«Security legger kanskje fortsatt for stor vekt på konfidensialitet. Det blir en ubalanse i vurderingen av informasjon mellom konfidensialitet, integritet og tilgjengelighet, slik ny sikkerhetslov også i større grad stiller krav om å forhindre. Mange innen security har kun jobbet med gammel sikkerhetslov og med ensidig fokus rundt fysisk sikring og beredskap. Nødvendig forståelse av og kunnskap om digital sikkerhet er derfor en mangel og resulterer i en organisatorisk sårbarhet».* En av informantene mente også at usikkerhet rundt hvordan informasjonen skulle graderes

medførte at informasjon ble overgradert, for å unngå konsekvenser av ikke å oppfylle lovkrav, men at overklassifiseringen primært fikk konsekvenser for safety.

Flere informanter, spesielt innen security, anså at informasjonssikkerhetstiltakene var vel motivert ut fra trusselbildet, både i form av industrispionasje og en reell insidertrussel. Et eksempel på et synspunkt som framkom i ett av intervjuene er: *«I dagens digitale samfunn, der folk er vant med å jobbe hjemmefra og med mobiltelefon, vil fotavtrykkene fra sikkerhetsloven medføre at håndteringen av informasjon blir mer tungvidt. Mange forbinder også sikkerhetsloven med noe som er tungt å vanskelig. Her er det viktig at tiltakene har en årsak og at man ikke tilbakeholder informasjon bare fordi det er kult. Det er kun de som sitter tettest på, som er kjent med trusselbildet. Det er mye industrispionasje rundt omkring og insiderstrusselen er reell».*

Et divergerende syn fra en av informantene gikk på at det egentlig ikke var et dilemma knyttet til behandling av informasjon, men at dette heller var relatert til mangelfulle systemer og rutiner for håndteringen av den graderte informasjonen. Dette som utrykt i intervjuet *«Denne utfordringen er egentlig en ikke-problemstilling om virksomheten har systemer på plass. Da kan man godt dele informasjon, både nasjonalt og utenlandsk»*.

6.1.1.3 Insiderproblematikken

En problemstilling som framkom i et par av intervjuene, og da med personer innen security, går på at ansatte og innleide kan misbruke fysiske eller informasjonsmessige tilganger for å forårsake skade. Frykten for insidere må anses som en underliggende årsak til dilemmaet «åpenhet kontra hemmelighold», men er imidlertid videre og mer generisk og er derfor omtalt separat.

Det bli samtidig påpekt i intervju at arbeid med å forebygge å kunne detektere insidervirksomhet er svært krevende og at dette krever en fin balansegang mellom tillit og kontroll. Man vil heller ikke skape et arbeidsmiljø som gjør at folk mistenkeliggjøres eller går rundt «å skuler på hverandre». Samtidig er det erfart fra andre virksomheter at hverken bakgrunnssjekk eller andre tiltak, er tilstrekkelig for å hindre at det ansettes personer som blir insidere.

Mens det i intervju med flere av informantene ble trukket fram at tillit er en grunnleggende verdi innen safety, var en av informantene i security svært tydelig på at den eksisterende åpenhetskulturen ved IFE er til hinder for arbeid med insiderproblematikk. Insidervirksomhet er en del av trusselbildet innen security og dette medfører at det er behov for flere typer tiltak, heriblant å være i stand til å kunne avdekke insidervirksomhet. Det framkom i intervju at viktigste virkemidlet for å kunne være i stand til dette, er gjennom å etablere en kultur for årvåkenhet i virksomheten, dvs. at personer er i stand til å avdekke mistenkelige eller unormale forhold og varsle om dette.

6.1.1.4 Beredskap

Beredskapsplanlegging og håndtering av hendelser ble omtalt i et par av intervjuene, og spesielt en av informantene var også opptatt av vektingen mellom safety og security i beredskapsplanlegging og i håndtering av hendelser. Samhandlingen mellom safety og security ble også trukket fram, da spesielt knyttet til beredskapsplanlegging, dimensjonering av beredskap, øvelser og håndtering av hendelser. Blant annet framkom det synspunkter på at beredskapsplanleggingen synes å være farget av hvem som medvirket og hvilke deler av det totale risikobildet de hadde ansvar for og kunnskap om. For øvelser var det forskjeller i øvingsbehov mellom de ulike fagmiljøene og divergerende synspunkt på hvilke øvingselementer som skulle inngå.

Ulike typer hendelser krever ulike varslingsveier og håndtering og det ble også stilt spørsmål til om alle har samme varslingsforståelse, da det i en tidlig fase av en hendelse kunne være krevende å identifisere om en hendelse er relatert til safety eller security. Det er også en kjent taktikk at en safety-hendelse (f.eks. brann) vil kunne framprovoseres for å stjele oppmerksomheten, og gjøre det enklere å gjennomføre f.eks. et terrorangrep. For vaktfunksjonen skapes derfor et dilemma rundt i hvor stor grad man bør avvike fra normale kontrollprosedyrer opp mot hvor akutt hendelsen er for liv og helse. Som formulert av en av informantene: *«I beredskapssituasjon kan tidsfaktoren være viktig for hvordan en hendelse får utvikle seg. Fra safety er man opptatt av å få folk inn så raskt som mulig. Security vil gjerne sjekke både ambulanser og brannbiler».*

6.1.1.5 Risikostyring

Dilemmaet handler om den overordnede risikostyringen på tvers av safety og security. En av informantene trakk i intervjuet fram at det var utfordringer knyttet til hvordan man på tvers av safety og security kunne få til en omforent risikostyring, slik at man til enhver tid var i stand til å prioritere arbeid med de viktigste risikoene. Som det framgår av kapittel 6.1.5, er det store forskjeller i tilnærminger og metodikk for risikovurdering og risikostyring innen safety og security. Mens risiko innen safety langt på vei er intern, kvantifiserbar og kontrollerbar, er det innen security store usikkerheter knyttet til hva man skal beskytte seg mot. Usikkerhet knyttet til en mulig trussel og dens intensjoner, kapasitet og «modus operandi» gjør det svært vanskelig å skulle vurdere risiko, definere sikkerhetstiltak og å bestemme i hvilken grad eksisterende sikkerhetstiltak reduserer risikoen til et akseptabelt nivå.

På grunn av de store epistemiske usikkerhetene i security, avviker metodebruken i security fra det som er vanlig i safety og risikostyring handler i større grad om å lukke sårbarheter heller enn å styre på identifisert og vurdert risiko. Ut over å medføre utfordringer med å skulle prioritere risiko på et overordnet nivå, er dette dilemmaet også relevant på tiltaksnivå der man ofte vil måtte veie en security-risiko opp mot en safety-risiko. Et eksempel på dette kan være at deling av informasjon i et prosjekt vil gi en gevinst for safety, men utgjøre en risiko innen security.

6.1.1.6 Sikkerhetsstyring

Et par informanter anså at det var ulikheter mellom safety og security når det kommer til regelstyring og sanksjonering av regelbrudd. Informantene oppfattet videre at man innenfor security var mer «firkantet» enn innenfor safety, i den forstand at security i det daglige la opp til en mer regelstyrt praksis i kombinasjon med kontroll av etterlevelse. Innen safety har man en tilnærming mer preget av vurderinger, avveininger og optimaliseringer «case by case».

Et par av informantene anså at man innen safety hadde en større grad av systemtilnærming og var mer opptatt av å legge til rette for erfaringslæring, både for å forstå hvorfor man i enkelte situasjoner hadde lykkes og hvorfor man i andre situasjoner hadde mislykkes. Man var også innen safety opptatt av at medarbeideres skulle ha en spørrende holdning til etablert praksis og at rapportering av feil ikke skulle få negative konsekvenser. Security ble i sin kommunikasjon oppfattet i større grad å vektlegge at overtredelse av regler ville få konsekvenser, inkludert strafferettslig ansvar. Et eksempel på en formulering fra et av intervjuene er: *«Tror også man bør myke opp retorikken innen security. Gjør man noe galt, kan dette være grunn for oppsigelse. Innenfor safety får man «cred» om man rapporterer feil, inkludert egne feil. Er ikke samme åpenhetskulturen innen security som safety, ved å varsle om forhold der man selv er involvert».*

6.1.2 Hva resulterer dilemmaene i?

Informantene ble på dette punktet spurt om hva de identifiserte dilemmaene resulterte i. Måten undersøkelsen var utformet på, gav ikke en klar sammenheng mellom det enkelte dilemma og den enkelte konsekvens. De konsekvensene flest informanter trakk fram, kan imidlertid i stor grad anses å være relatert til dilemmaene rundt håndtering av informasjon.

6.1.2.1 Negativ påvirkning på sikkerheten

Informasjon som blir vurdert som gradert etter sikkerhetsloven, omfatter eksempelvis informasjon om anleggets konstruksjon, virkemåte, driftsmessige forhold, materialer på anlegget etc. Gradering medfør at tilgang til informasjonen krever sikkerhetsklarering og informasjonen kan kun behandles i dedikerte datasystemer. Disse har begrenset funksjonalitet, og dekker heller ikke alle behov. Det er videre krav til bl.a. at møter må foregå i dedikerte møterom der det også er begrensninger på hvilket utstyr som kan bringes inn. Samhandling med eksterne, og som krever tilgang til gradert informasjon, krever sikkerhetsavtale og som må godkjennes av myndighetene. For samarbeid over landegrensene må sikkerhetsavtalen godkjennes av myndigheter i flere land.

Flere informanter innen safety oppleves informasjonssikkerhetstiltakene som svært tungvinte og hemmende for samhandlingen, spesielt mot utenlandske konsulenter og leverandører. Dette medførte igjen at det ble vanskeligere og mer tidkrevende å arbeide med sikkerhetsvurderinger, oppdatering av sikkerhetsdokumentasjon etc. og at kvaliteten i dokumentasjonen ble dårligere. Videre var det bekymring for at personell ikke fikk tilstrekkelig informasjon til å ha en god nok forståelse for farepotensialet til de ulike delen av anlegget og hvordan de virket sammen eller til å forstå bakgrunnen for prosedyrer. Det ble videre utrykt sterk bekymring for at tiltakene utfordret framdriften i viktige safety-prosjekt.

Det var flere informanter som pekte på feilgradering av informasjon som en mulig konsekvens, der det også ble framholdt som sannsynlig at usikkerhet rundt gradering av informasjon medførte overgradering. Dette ville medføre at informasjonen ble vanskeligere tilgjengelig eller ikke tilfaller dem som har behov for å jobbe med den. Undergradering av informasjon vil medføre at informasjonen ikke ble beskyttet på en god nok måte. Tilsvarende vil det være en negativ konsekvens i form av risiko for kompromittering av informasjon om rutinene for informasjonssikkerhet ikke blir fulgt.

6.1.2.2 Frustrasjon og dårlig samhandling

Det var flere informanter som trakk fram at dilemmaene medførte frustrasjon, friksjon og dårlig samhandling. Det ble også bemerket at frustrasjon kunne medføre mistillit mellom nøkkelpersonell innen safety og security, ineffektive prosesser og dårlig samhandling mellom safety og security.

6.1.2.3 Utfordringer knyttet til risikostyring

Forskjeller i metodikk og tilnærming til risikovurderinger ble av en av informantene ansett gjøre det utfordrende å få en total oversikt over det samlede risikobildet. Dette ville igjen gjøre det krevende å drive en hensiktsmessig risikostyring.

6.1.3 Mulige årsaker til dilemmaene?

Informantene ble på dette punktet spurt om hva de anså som årsaker bak dilemmaene. Generelt var det store ulikheter i hvilke forhold informantene vektla, samtidig som mye av tematikken som framkom i intervjuene hadde store likheter. Synspunktene er i denne oppgaven kategorisert som følgende:

- Organisatoriske og styringsmessige forhold.
- Ulikt kunnskapsgrunnlag og ulike vurderinger mellom safety og security.
- Umodne administrative systemer og tekniske løsninger.
- Ulike verdier og ulik kultur mellom safety og security

Det var generelt også store forskjeller i hvor dypt informantene gikk inn i å utdype de ulike årsakene. Når det kommer til ulikheter i verdier og kultur mellom safety og security, framkom dette kun i enkeltintervjuer.

6.1.3.1 Organisatoriske og styringsmessige forhold

Organisatoriske forhold ble trukket fram av flere informanter som årsak til dilemmaene. Mange av informantene påpekte også manglende samhandling mellom safety og security, og spesielt i sikkerhetsstaben. Flere av informantene trakk fram at det innen security var uklarhet i rollene til flere stabsfunksjoner. Mangelen på tydelig prioritering i situasjoner der man må velge mellom safety og security ble også trukket fram, samt at ingen tør å ta avgjørelsen i slike situasjoner.

Et par av informantene anså det som uheldig at vaktfunksjonen ikke rapporterer til ledelsesfunksjonen med stedlig ansvar for sikkerheten på de to lokalitetene, eller som en av informantene utrykte det: «*Divisjonsledelsen har ansvar for security-oppgavene mens sektoren har ansvar for resultatene. Det er et problem at sektoren har ansvar uten å ha myndighet».* Den valgte organiseringen medfører bl.a. at vaktfunksjonen ikke er representert i ledergruppene ved de to lokalitetene.

At safety og security har ulikt mål ble i seg selv trukket fram av flere av informantene som årsak til målkonfliktene. I utgangspunktet har både safety og security et formål om å beskytte liv og helse. Innen safety beskytter man mot uhell og ulykker på anleggene. Innen security beskytter man anlegg og materialer mot ondsinnede villede handlinger og informasjonsverdier mot å kunne bli misbrukt til et slikt formål.

6.1.3.2 Ulikt kunnskapsgrunnlag og ulike vurderinger mellom safety og security

Kunnskapsmessige forhold, og spesielt ulikheter i betraktninger rundt risikoen for villede ondsinnede handlinger, ble trukket fram av flere av informantene som årsaksforklaring på dilemmaene. I dette var det flere av informantene som anså at man innen security hadde lite kunnskap om det nukleære, og derfor oppfatter mulige skadekonsekvenser som vesentlig større enn de i realiteten er. Dette, på tilsvarende måte som det generelt i samfunnet, er en tendens til at risiko knyttet til nukleære hendelser overvurderes. Samtidig har personer innen safety lite kunnskap om mulige trusler samt de verdivurderingene som ligger til grunn for beskyttelsen. Disse vurderingene er graderte, og personer innen safety er i liten grad gjort kjent med innholdet.

Det var et par av informantene som pekte på at det innen security er vesentlig vanskeligere, enn innen safety, å analysere seg fram til hva som vil være riktige sikkerhetstiltak og å kunne godtgjøre at de tiltakene man har valgt gir ønsket risikoreduserende effekt. Dette har sin bakgrunn bl.a. i at

tiltakene må adressere et risikobilde som er i stadig endring og som man også må anta som delvis ukjent. En av informantene vektla at det var viktig å diskutere problemstillinger, da det oftest innen security vil være flere mulige løsninger. Informanten påpekte også at regelverket (sikkerhetsloven), som et funksjonelt regelverk, legger opp til at virksomhetene har stor frihet til å velge tiltak og hvilken risiko man kan leve med, så lenge man har en klar vurdering av risiko og en tydelig styring.

Det var en av informantene som pekte på at safety er et langt mer etablert fagfelt og at det derfor er mer konsensus om hva som er riktige sikkerhetstiltak, eller som utrykt av informanten: *«Årsaken til målkonfliktene tror jeg i stor grad baserer seg på ulike tradisjoner. Safety er et veletablert fagområde basert på et etablert regelverk og som er vel forstått. Både regelverk og internasjonale standarder utarbeidet av faglige komiteer tar utgangspunkt i safety. Innenfor safety er man derfor enige om hva som er viktig. Security er et ferskere fagområde og som har kommet opp i nyere tid, spesielt i Norge. Det er et mindre utviklet regelverk. Det blir derfor veldig opp til den enkelte rådgiver, og litt tilfeldig hva som blir sikringstiltaket. Security mangler en felles plattform. Man får forskjellig svar avhengig av hvem man spør på security».*

6.1.3.3 Umodne administrative systemer og tekniske løsninger

Mens IFE over tiår har utviklet sine systemer innen safety, er kravene til security av nyere dato. Det var derfor flere av informantene som pekte på umodenhet i systemer som årsak til målkonfliktene og at security ikke var kommet langt nok «til at systemene glir». I tillegg trakk flere informanter fram mangelfulle IKT-løsninger for behandling av sikkerhetsgradert informasjon, samt at eksisterende løsninger ikke var egnet for alle formål. Enkelte informanter pekte også på mangler i ledelsessystemet innen security.

6.1.3.4 Ulike verdier og ulik kultur innen safety og security

En av informantene trakk fram ulikheter i tankegang mellom safety og security som årsak til dilemmaene og at tankegangen innen security bryter med verdier som åpenhet og toleranse, og som har lange tradisjoner i Norge. En del tiltak innen security ville derfor være vanskelig å gjennomføre, uavhengig av virksomhet. Som informanten utrykte det: «*I Norge vil man rive gjerder heller enn å bygge dem opp».*

Ulikheter knyttet til regelstyring og måten man håndterte og responderte på hendelser etc. (kapittel 6.1.1.6) ble av en av informantene forsøkt forklart gjennom kulturelle ulikheter mellom safety og security. Hva disse ulikhetene gikk på, ble ikke utdypet i intervjuet.

6.1.4 Hvordan håndteres dilemmaene i det daglige?

Det var flere informanter som mente at utfordringene i grensesnittet mellom safety og security hadde stort lederfokus og at ledergruppa brukte mye tid på å løse dem, samt at det var gjennomført strukturelle tiltak for å sikre at sikkerhetsstaben arbeider mer på tvers mellom safety og security. Det var også dem som mente at utfordringene i stor grad ble overlatt til linja og at det derfor ble en del ad-hoc løsninger, og der det ble noe personavhengig hvem som ble involvert og hva løsningen ble. Dialog og kunnskap ble også trukket fram som virkemidler som ble brukt til å håndtere dilemmaene. Flere av informantene anså at det var viktig med pragmatisme, og det ble vektlagt å ansette pragmatiske personer og å løse oppdukkende problemer på en pragmatisk måte.

I et litt mer langsiktig tidsperspektiv, trakk et par av informantene opp at det var valgt å forsere løsninger for å behandle sikkerhetsgradert informasjon.

6.1.5 Forskjellen mellom arbeid med farer innen safety og trusler innen security

På spørsmål om det var vesentlige forskjeller i måten man innenfor safety jobbet med farer og måten man innen security jobbet med trusler, var det flere av informantene som gav utrykk for usikkerhet ved at de hadde dårlig innsikt i hvordan den andre gruppen jobbet.

Flere av informantene pekte på at farene innen safety i stor grad er interne og stabile, godt kjent og kontrollerbare. Innen security er truslene eksterne, ukjente og abstrakte. I tillegg er trusselbildet innen security dynamisk, og aller mest innen digital sikkerhet. Vurdering av trusselbildet må i stor grad basere seg på informasjon fra myndighetsorganer. Informasjonen om trusler er i tillegg underlagt hemmelighold og en av informantene påpekte at myndighetene bare deler informasjon i den grad de anser det som nødvendig, slik at det er vanskelig å danne seg en dypere forståelse for trusselbildet.

Mens man innen safety jobber med å redusere risiko, (dvs. både sannsynlighets- og konsekvensreduserende tiltak), baserer arbeidet innen security seg på å redusere sårbarheter, da man i praksis ikke får gjort noe med truslene eller verdiene. Et par informanter påpekte at usikkerheten rundt trusselen gjør at man innen security må ha en mer kreativ tenkning rundt risiko, og det er heller ikke mulig å bruke historikk og statistikk på tilsvarende måte som innen safety. Det er også utfordrende å analysere seg fram til hva som vil være de mest hensiktsmessige sikringstiltakene og om sikringstiltakene er tilstrekkelige. Dette som utrykt av en av informantene: «*Innen security er man mer avhengig av en kontinuerlig vurdering av trusler. Dette krever en helt annen type årvåkenhet. Man kan bytte ut låser, flere låser, høyere gjerder etc., men kan ikke lukke en slik type risiko. Er intensjon og kapasiteten til stede, vil sikringstiltak kunne forseres. Det er derfor behov for en løpende risikovurdering basert på dialog for å vurdere hva som er tilstrekkelig. Denne vil i sin natur være mer kvalitativ enn kvantitativ. Det er derfor et dilemma knyttet til å vurdere når beskyttelsen er god nok. Dette gjelder særegent for sikringsfeltet. Alvorlige anslag er vanskelig å forutsi, og spesielt gjelder dette soloterrorister. Vi vet ikke når det skjer. Jeg tror dette er enklere når det gjelder utslipp, brann etc., som i større grad kan detekteres av sensorer o.l.*»

En av informantene anså også at man innen safety vektla forebyggende vedlikehold, daglig overvåking og kontroll over prosessen, i større grad enn man gjorde innen security. En annen informant framholdt at det krever en stor grad av årvåkenhet, for å være i stand til å avdekke hendelser innen security i tidlig fase. En informant anså også at man innen security hadde et hovedfokus på å forhindre at hendelser skjedde, mens det innen safety er en mer integrert del å være i stand til å kontrollere hendelser slik at de ikke får utviklet seg. Samtidig påpekte flere av informantene at det var forskjeller i termologi mellom safety og security, også for ting som i praksis betydde det samme.

6.2 Mulighetsrommet for å løse dilemmaene

Spørsmålene i denne delen av oppgaven relaterer seg til det andre forskningsspørsmålet og som går ut på å undersøke mulighetsrommet for løsninger på dilemmaene og som samtidig ivaretar hensynet til både safety og security på en god måte. Informantene ble innledningsvis bedt om å redegjøre for hvordan de selv anser at dilemmaene som har framkommet tidligere i intervjuet best kan løses (kapittel 6.2.1).

Gode samhandlingsarenaer mellom safety og security må generelt anses som hensiktsmessig for å skape dialog og kultur på tvers av fagområdene. Informantene ble derfor deretter bedt om å ta stilling til i hvilken grad de anser det er rom for samhandling mellom safety og security og med hvilken forventet effekt (kapittel 6.2.2). Til slutt ble informantene bedt om å ta stilling til hva de anser som viktigste begrensning for samhandling (kapittel 6.2.3).

6.2.1 Beste måten å løse dilemmaene

På spørsmål om hvordan man anså at dilemmaene best kunne løses, var det flere av informantene som pekte på at løsning av utfordringene er et ledelsesansvar, og at det var viktig å ha en organisasjon med tilstrekkelig kompetanse og ressurser, samt tydelig definerte roller og ansvar. Samarbeid, dialog, koordinering, involvering av riktige personell og å søke løsninger som er gode for både safety og security ble trukket fram som viktige deler av løsningen. Tilsvarende framkom det at det er viktig å informere om bakgrunnen for security-tiltakene. Felles kultur ble også trukket fram, da i form av at man innen safety er mer orientert mot en kultur der man skal kunne rapportere om egne og andres feil uten frykt for represalier. Aspektet med et felles og omforent ledelsessystem ble også trukket fram som viktig.

Særlig var det mange av informantene som trakk fram viktigheten av en omforent forståelse av bakgrunnen for at informasjon skal graderes etter sikkerhetsloven. Enkelte påpekte også viktigheten av en nøkternhet i hvilken informasjon som blir sikkerhetsgradert og at akkumulering av informasjon ikke er tilstrekkelig til at den graderes. Flere informanter påpekte viktigheten av gode løsninger som gjør det mulig å behandle informasjon på en forsvarlig måte. Tilsvarende ble det også trukket fram at man bør ha dialog opp mot myndigheter for å sikre forståelse for de behovene som IFE har for å kunne dele informasjon med utenlandsk kompetanse.

6.2.2 Mulighetsrommet for økt samhandling mellom safety og security

På spørsmål om i hvilken grad det var rom for mer samhandling mellom safety og security, var det flere av informantene som pekte på behovet for bedre samhandling horisontalt i organisasjonen. Dette inkluderer mellom safety stab og security stab, og også mellom de operative delene av organisasjonen, dvs. mellom anleggsdrift og operativ security. Det ble samtidig utrykt behov for bedre informasjonsflyt vertikalt i organisasjonen, og en av informantene hadde erfart at informasjon som kommer inn i virksomheten fra eksempelvis departementer og andre myndigheter, ikke kom ned i organisasjonen.

En av informantene etterlyste at safety og security i større grad utfordrer hverandre, eksempelvis i sikkerhetskomiteen. Områder som ble trukket fram som spesielt relevante for bedre samhandling var sikkerhetsvurderinger, risikovurderinger, beredskap, utvikling av ledelsessystem og verdivurderinger av informasjonsverdier og fysiske verdier. Tanken bak dette er en mer helhetlig

styring av sikkerheten, eller som utrykt av en av informantene: *«Vi er en sikkerhetsorganisasjon. Da må man tenke helhetlig både på safety og security i alt man gjør. Dette er en kulturendring».*

Forventet effekt av bedret samhandling var bedre utnyttelse av ressurser og læring på tvers av organisasjonen. En av informantene trakk spesielt fram hvordan safety var konstruert ut fra prinsippet om forsvar i dybden og hvordan hendelser ble klassifisert og håndtert deretter, som et område for erfaringsoverføring til security. Tilsvarende trakk en annen av informantene fram håndtering av operative hendelser som brannbekjempelse, spesielt på tidspunkt med tynnere bemanning, som et område der man hadde positive erfaringer med samarbeid. En tredje av informantene trakk også inn en forventet effekt i at man bedrer evnen til å oppdage security-hendelser på et tidlig tidspunkt («Flere øyne som ser og som vet hva de ser etter»).

Det var også informanter som pekte på at økt samarbeid vil være positivt for nytenkning og ha positive effekter for trivsel, arbeidsmiljø og sikkerhetskultur, eller som utrykt av en av informantene: *«Sabla mye gøyere å jobbe. Arbeidsmiljøet og sikkerhetskulturen vil ha godt av det. Vi sitter og jobber og det er ofte vanskelig å vite om det vi gjør blir riktig eller galt».*

6.2.3 Begrensninger for samhandling

På spørsmålet om hva som er de viktigste begrensningene for samhandling, var det stort sprik i svarene fra informantene. Flere informanter trakk fram manglende helhetsforståelse og svak ledelsesstyring, men også «mindset» ble trukket fram som en forklaring. Organisatoriske forhold ble også trukket fram, spesielt at linjeorganisasjonen forventet tydeligere krav og mer «hands on» rådgivning til konkrete utfordringer enn de fikk fra sikkerhetsstaben. Tilsvarende ble også begrensninger i kapasitet og stor arbeidsbelastning trukket fram. Et par av informantene utrykte også uklarhet i roller og særlig for en del stabsfunksjoner som er definert som frie og uavhengige, eller som utrykt av en av informantene: «*Oppfatter at det er etablert flere frie og uavhengige roller og som er så fri og uavhengige at samhandling ikke finner sted».* Holdninger, manglende tillit og kompetanse om fagområdene på tvers av safety og security ble også trukket fram i enkeltintervjuer.

6.3 Kultur som virkemiddel for tettere integrering mellom safety og security?

Spørsmålene i dette kapitlet relaterer seg til det tredje forskingsspørsmålet, og som omhandler hva som bør være essensen i en omforent kultur og hvordan man bør gå fram for å etablere den.

Som det framgår i kapittel 4.3.1, er det ikke noen konsensus om hva som ligger i begrepet sikkerhetskultur og det er i utgangspunktet relativt fritt å fylle begrepet med det man selv ønsker. I arbeidet med denne oppgaven var det derfor, som utgangspunkt for en diskusjon rundt betydningen av en felles kultur, interessant å sjekke ut om informantene allerede hadde en omforent forståelse i hva som ligger i sikkerhetskulturbegrepet. Informantene ble derfor spurt om hva de legger i begrepet sikkerhetskultur (kapittel 6.3.1). Informantene ble deretter bedt om å gi et begrunnet svar på om de opplever at det er en felles kultur på IFE og som omfatter både safety og security (kapittel 6.3.2). Bakgrunnen for dette spørsmålet, er at en allerede omforent kultur ville gi et noe annet utgangspunkt for videre diskusjon enn om kulturen ikke er omforent.

Informantene ble deretter spurt om hva de oppfatter bør være essensen i en omforent kultur som inkluderer både safety og security (kapittel 6.3.3) og hvordan de anser IFE bør gå fram for å etablere

en omforent kultur (6.3.4). Begge disse spørsmålene tar for seg kjernen i det tredje forskingsspørsmålet.

Som det framgår av kapittel 4.3.4, er det svært krevende for en organisasjon å etablere og ivareta en homogen sikkerhetskultur på tvers av virksomheten. Det finnes også tungtveiende argumenter for at en organisasjonskultur vil kunne inneholde elementer av en profesjonsstyrt kultur og som varierer noe mellom ulike enheter i virksomheten. Informantene ble derfor avslutningsvis spurt om de synes det er viktig å ha en felles kultur, eller om det er ok om kulturen er litt ulik i ulike deler av den nukleære virksomheten (kapittel 6.3.5).

6.3.1 Hva man legger i begrepet sikkerhetskultur

På spørsmålet om hva man legger i begrepet «sikkerhetskultur», var det mellom informantene svært ulike meninger. Begreper som holdninger, tankesett, vaner og opptreden ble brukt av flere av informantene. Flere av informantene inkluderte også en beskrivelse av holdninger (f.eks. stolthet, selvrefleksjon, å være beredt, åpenhet for forslag og tillit og respekt for retningslinjene) i sine betraktninger rundt sikkerhetskultur. En av informantene inkluderte i tillegg ledelse, ledelsessystem, behandling av avvik og organisatorisk læring. En annen av informantene inkluderte også sikkerhetstiltak. Informantene gav følgende svar på hva de la i begrepet sikkerhetskultur:

- *«Sikkerhetskultur handler om holdning, som går ut på at man vil ha det sikkert og at man har en stolthet i at ting gjøres på en så sikker måte som man kan få det. Denne holdningen er felles for alle i organisasjonen. Da kan man også si at dette ikke er slik man vil ha ting ».*
- *«Generelt handler sikkerhetskultur om organisasjonskultur. Sikkerhetskultur-arbeidet ved IFE handler om å sette sikkerhet på agendaen. Sikkerhetskultur handler om forhold som ledelse, ledelsessystem, behandling av avvik og organisatorisk læring. Videre handler kultur om åpenhet, takhøyde, at man ikke skal være redd for å si fra, å respektere og forstå retningslinjene samt å ha tillit til retningslinjene»*
- *«Jeg mener en god kultur kjennetegnes av at alle i organisasjonen til enhver tid er beredt. Rede til å vente det uventede. Forstår hva de skal gjøre. Åpne for forslag. Tror på egne handlinger».*
- *«Sikkerhetskultur er slik vi som gruppe arbeider med sikkerhet. Tankesett, verdisett. Enkeltpersoner kan ikke ha sikkerhetskultur».*
- *«En hensiktsmessig og riktig adferd».*
- *«Kollektive vaner».*
- *«De ansatte i virksomhetens tanker og holdninger om sikkerhet. Inkludert hvordan de opptrer».*
- *«Vanene man har opparbeidet seg for ikke å risikere skader og uhell. At man i det daglige tenker på hvilke vaner man har».*
- *«Hva en organisasjon gjør av tiltak for å nå forsvarlig sikkerhet og hva enkeltpersoner tenker om sikkerhet, dvs. hvordan den enkelte ser sin rolle. Begge deler er avhengige av hverandre».*

6.3.2 Opplevelsen av felles kultur som omfatter både safety og security

På spørsmålet om informantene opplevde at det i dag var en omforent kultur på tvers av safety og security, framkom det synspunkt på hele skalaen. Flere av informantene anså også at det hadde vært en positiv utvikling mot en felles kultur. Følgende synspunkter blir her gjengitt for å illustrere spriket i synspunkt:

- *«I dag opplever jeg at den er høy sammenlignet med andre større bedrifter og som er underlagt sikkerhetsloven. Vi har kommet oss i riktig retning de siste 5 årene. Opplevde dette tidligere som en stor risiko, men ser det ikke nå. Har blitt en bedre kultur og som omfatter begge, men vi er ikke i mål».*
- *«Nei. Oppfatter det er et gap mellom security og resten av IFE. Føler at de som jobber med security har sin egen kultur og at den avviker fra resten. Organisasjonen forstår ikke, men de som jobber med security forstår det så veldig godt».*
- *«Oppfatter ikke at vi i dag har en felles kultur, men mange subkulturer. Vi har i det siste fått en felles lederforståelse for hva vi ønsker, men det er noe annet å skape det».*
- *«Er en felles kultur, men litt ulike innfallsvinkler».*

6.3.3 Essensen i en omforent kultur mellom safety og security

På spørsmål om hva som bør være essensen i en omforent kultur, var det mellom informantene ulike oppfatninger. Dette henger rimeligvis sammen med at informantene i utgangspunktet har svært ulik oppfatning av hva som ligger i begrepet «sikkerhetskultur». Elementer som ble trukket fram av informantene var gjensidig forståelse og respekt for hverandres fagområder, samhandling, deling av informasjon, forståelse og respekt for sikkerhetstiltakene, felles forståelse for hva som er hensiktsmessig og riktig adferd og felles begrepsbruk. Videre var det også informanter som la vekt på viktigheten av lojalitet til egne arbeidsoppgaver, samt å bli bedre på det man må være gode på.

Videre var den en av informantene som mente man i større grad bør vektlegge prinsippet om kontinuerlig forbedring og resillienstankegang, heller enn ensidig vektlegging av de negative sidene ved hendelser. Vilje til å ta eierskap til problemstillinger og gjensidig involvering ble også nevnt. Enkelte av informantene trakk fram at en kultur må bygge på tillit og åpenhet. Videre ble det trukket fram at en spørrende holdning var viktig og at det var viktig at en kultur skulle legge til rette for rapportering, uten frykt for negative konsekvenser.

6.3.4 Prosess for å skape en omforent kultur mellom safety og security

På spørsmålet om hvordan IFE bør gå fram for å etablere en felles kultur var det flere av informantene som vektla at det var svært viktig å konkretisere hva man mener er en god sikkerhetskultur, og også tydeliggjøre forventninger til den enkelte medarbeider. Et eksempel på hvordan dette ble utrykt av en informant er: «Vi må g*jøre mer enn å snakke om at det er viktig, og bli enig om hva det faktisk betyr og medfører for hver enkelt medarbeider. Vi må også sørge for at enkeltpersoner ikke får ansvar for noe enkeltpersoner ikke har forutsetninger for å kunne gjøre alene».* Motsatt, var det samtidig informanter (på ledelsesnivå) som anså at ledelsen var enige om hva slags sikkerhetskultur man ønsket og at det allerede var etablert en god prosess. Det var også en informant på ledelsesnivå som framhevde viktigheten av at alle burde føle seg velkomment til å bidra i prosessen med å definere en omforent kultur.

Samhandling og dialog ble av flere informanter framhevd som forutsetninger for å etablere kultur. Det var flere informanter som vektla viktigheten av god forankring av sikkerhetstiltak, slik at ansatte har en tydelig forståelse for bakgrunnen for tiltaket og er i stand til å koble det opp mot en fare/trussel. Et par av informantene pekte på viktigheten av at stabsfunksjoner er nærværende, er tilgjengelige for å rådgi og at disse blir aktivt involvert av linjeorganisasjonen. Videre ble viktigheten av å rose korrekt adferd vektlagt, eller som informanten utrykte det «*Å ta folk på fersken i å gjøre noe riktig*». Coaching ble også framhevet som viktig, og tilsvarende også *«oppmuntrende drypp og å*

«pep-talte» folk opp». En informant trakk også inn historiefortelling, i form av at det er viktig å formidle security-hendelser som har skjedd i andre organisasjoner.

Det var et par av informantene som vektla viktigheten av å være i stand til å måle utviklingen av sikkerhetskulturen for å ha et objektivt grunnlag for å vurdere framgang. Et eksempel hentet fra et intervju er: *«Man må først beskrive hvilken sikkerhetskultur man vil ha. I dette må man involvere ledere som skal være med på å utforme kulturen. Vi må dra kulturbegrepet inn i ledergruppene. Vi må sette oss mål som man kan måle på, etablere KPI-er og definere tiltak innen de ulike områdene. Deretter måle framgang. Kompetanse og coaching er viktig. Vi må få sikkerhetskultur inn i et ledelsesperspektiv. Jeg har stor tro på at lederne er viktige. Å rapportere og lære er veldig viktig for å utvikle kulturen».*

Samtidig var det noen av informantene som dro fram strukturelle og organisatoriske forhold. Enkelte av informantene anså det som viktig at både safety og security rapporterer til samme ledelsesnivå, hvilket i praksis bør være den stedlige lederen på hver av de to lokasjonene. En informant påpekte viktigheten av utvikling av fagmiljøene «in house», heller enn å bruke innleide. Videre at ledelsen i større grad burde lære seg å stole på fagmiljøene og i større grad delegere beslutninger. Samtidig med dette burde ledelsen forvisse seg om at informasjonen flyter nedover i organisasjonen og at fagmiljøene har riktig kompetanse og ressurser, slik at de har nødvendige forutsetninger for å foreta beslutninger. Følgende er et eksempel på hvordan dette ble utrykt av en informant: *«Vi må etablere en organisasjon som støtter ledelsen og som ledelsen skal ha tillit til. I dag virker det som om ledelsen tviholder på å være involvert i alt. De må lære seg å stole på fagekspertene. Lederne må også forvisse seg om at vedkommende har delt det som trenges å deles. Ledelsesansvar er å få delegert informasjon til rett nivå av organisasjon. I dag er informasjonsflyten stykkevis og delt».*

6.3.5 Viktigheten av en omforent kultur mellom safety og security

På spørsmålet om i hvilken grad det var viktig å ha en felles kultur på tvers av virksomheten, svarte de alle fleste informantene bekreftende. Flere av informantene tok imidlertid forbehold om at en helt lik kultur ikke var mulig, da de ulike organisatoriske enhetene hadde ulike arbeidsoppgaver. En av informantene utrykte i tillegg at kulturen vil være levende og dynamisk.

7 Diskusjon

Diskusjonen i denne oppgaven er lagt opp slik at forskingsspørsmålene diskuteres i kronologisk rekkefølge.

Det første forskningsspørsmålet går på å diskutere hvilke dilemmaer som oppstår mellom safety og security og hvilket opphav disse har. Dilemmaene identifisert gjennom empirien er utførlig beskrevet i kapittel 6.1.1. Av hensyn til lesbarheten til oppgaven er det allikevel gitt en kort oppsummering av dem i kapittel 7.1, samtidig som kapitlet inneholder en kort diskusjon av dem opp mot et tidligere arbeid på virksomhetsnivå gjennomført av (Pettersen & Bjørnskau, 2014).

Mulige årsaker til dilemmaene beskrevet i kapittel 7.1, er diskutert i kapittel 7.2. Det har i diskusjonen blitt lagt hovedvekt på de forklaringene som har blitt fremmet av informantene og som en del av empirien gitt i kapittel 6.1.3. Forklaringene er imidlertid, så langt som mulig, diskutert innenfor rammene av teorikapitlet (kapittel 4). I disse diskusjonene er det spesielt lagt vekt på å forklare hvorfor tankesett, tilnærminger og verdier er ulike mellom safety og security.

Det andre forskningsspørsmålet, knyttet til mulighetsrommet for å løse dilemmaene mellom safety og security, er diskutert i kapittel 7.3. Kapitlet innleder med en kort diskusjon rundt det generelle mulighetsrommet for bedret samhandling mellom safety og security, mens det i kapittel 7.3.1 er valgt å gå mer konkret inn på mulige løsninger for de enkelte dilemmaene.

En omforent kultur som virkemiddel for tettere integrering mellom safety og security er diskutert i kapittel 7.4. Også dette kapitlet er todelt, og der kapittel 7.4.1 tar for seg essensen i en omforent kultur mens kapittel 7.4.2. går inn på prosessen for etablering. I begge tilfeller bygger diskusjonen på forslagene framkommet gjennom empirien (kapittel 6.3.3 og 6.3.4), men der disse blir diskutert innenfor rammene av anerkjente teorier rundt sikkerhetskultur (kapittel 4.3).

7.1 Dilemmaer mellom safety og security og hva de resulterer i

Dilemmaene som er identifisert gjennom intervjuer med informanter, og som beskrevet i kapittel 6.1.2, er oppsummert i tabell 6.

Tabell 6: *Oppsummering av dilemmaene som framkom i intervjuene med informantene.*

Nr.	Dilemma	Innhold
1	Åpenhet kontra hemmelighold.	Behovet for at ansatte skal forstå bakgrunnen for etablerte security-tiltak opp mot risikoen ved å dele informasjon.
2	Konfidensialitet kontra tilgjengelighet for informasjon.	Behovet for effektiv tilgang og enkel håndtering av informasjon opp mot behovet for å beskytte informasjonens konfidensialitet.
3	Insiderproblematikken.	Hvor langt virksomheten bør gå i kontrolltiltak ovenfor de ansatte for å kunne avdekke insidervirksomhet opp mot hensyn som arbeidsmiljø og personvern.
4	Beredskap.	Hvilke risikoer man vektlegger i beredskapsplanlegging og ved håndtering av hendelser.

5	Risikostyring.	Ulik metodikk mellom safety og security for vurdering av risiko og ulike prinsipper for risikohåndtering. Utfordringer med å etablere samlet risikobilde på tvers av safety og security.
6	Sikkerhetsstyring.	Regelstyring kontra enkeltvurderinger. Virkemidler for å sikre etterlevelse og sanksjonering av brudd på internt regelverk.

Som det framgår av kapittel 6.1.2, er konsekvensene av dilemmaene i hovedsak at:

- Safety blir påvirket negativt i form at samhandling blir vanskeligere. Dette kan igjen medfører dårligere kvalitet f.eks. i sikkerhetsvurderinger og forsinkelse i prosjekter.
- Security blir påvirket negativt om informasjonssikkerhetsrutiner ikke blir fulgt.
- Frustrasjon og friksjon mellom medarbeidere og faggrupper og som medfører dårlig samhandling
- Utfordringer knyttet til risikostyring som følge av at det er utfordrende å få oversikt over det samlede risikobildet.

Sammenlignet med studien av effekter av nye security-tiltak innen luftfarten gjennomført av (Pettersen & Bjørnskau, 2014), ser vi vesentlige likheter ved at security-tiltak har medført endringer i informasjonsflyt og som har hatt negativ påvirkning på safety. Tilsvarende synes det også å være likheter når det kommer til hemmelighold rundt bakgrunnen for security-tiltakene og at personell har hatt utfordringer i forståelsen av bakgrunn og dimensjonering av security-tiltakene. Pettersen & Bjørnskau rapporterte om at security-tiltakene innen luftfarten medførte en del utfordringer relatert til arbeidsmiljø. Tilsvarende framkom i intervjuene med informantene. I motsetning til (Pettersen & Bjørnskau, 2014), er det i empirien ikke gått detaljert inn på hva denne frustrasjonen består i og hvor omfattende den er.

En klar likhet mellom egen studie og studien til (Pettersen & Bjørnskau, 2014), er at risikostyringsprosessene innen safety og security er separate. For luftfarten ble risikostyringen innen security utført på et sentralisert nivå i EU og som også definerte utformingen av tiltak, ut fra vurderinger som var ukjente på et lokalt nivå. På IFE blir risikovurderinger innen safety og security gjennomført av ulike personer og i ulik del av organisasjonen. Om safety og security blir to uavhengige risikostyringsprosesser og som håndteres av ulike deler av organisasjonen, vanskeliggjør dette styringen for optimal risiko.

7.2 Årsaker til dilemmaene mellom safety og security

Dilemma vil i utgangspunktet kunne årsaksforklares på ulike måter og ut fra ulike perspektiver. Det er i oppgaven valgt å avgrense diskusjonen til de forklaringene som har framkommet i intervju med informantene, og som inkluderer følgende:

1. Organisatoriske og styringsmessige forhold.
2. Ulik kunnskap og ulike vurderinger mellom safety og security.
3. Umodne administrative systemer og tekniske løsninger.
4. Ulike verdier innen safety og security.
5. Ulik kultur innen safety og security.

7.2.1 Organisatoriske og styringsmessige forhold

Som det vil bli redegjort for senere i dette kapitlet, finnes det flere mulige faglige, kulturelle og verdimessige forklaringer på dilemmaene mellom safety og security. Organisatoriske og styringsmessige forhold vi derfor neppe kunne anses som den primære årsaken bak dilemmaene, men må imidlertid antas som viktige for om en organisasjon klarer å løse dilemmaene mellom fagområdene og for kvaliteten i løsningen.

I den studerte virksomheten virker det å være stor grad av uavhengighet i styringen mellom safety og security, og der hvert av fagområdene ivaretas av en dedikert organisasjon, med egne prinsipper og faglige tilnærminger, egen kunnskap og kompetanse, egen metodikk og med utgangspunkt i ulikt regelverk. I mange sammenhenger kan et slikt skille være hensiktsmessig, da begge fagområdene er komplekse og baserer seg på spesialisert kunnskap. Utfordringene oppstår ved sprik mellom fagområdene, eksempelvis i form av de dilemmaene som er beskrevet i denne oppgaven. Fra et NAT-perspektiv vil dette være å anse som interaksjoner mellom fagområdene. Disse interaksjonene må samtidig anses som relativt komplekse, spesielt i tilfeller der de berører kommunikasjon og samhandling i virksomheten og der det er vanskelig på forhånd å forutsi nøyaktig hvordan en endring vil påvirke.

Samhandling og kommunikasjon er viktig innen safety. Tar man eksempelvis utgangspunkt i den menneskelige konvolutten (Westerum & Adimski, 2009), blir ikke safety kun ivaretatt av den aktuelle virksomheten, men også av økosystemet rundt. For driften av et system vil det være en konstant pågående dialog og som på en god måte integrerer driften opp mot vedlikehold og konstruksjon/forbedringer. Det legges videre opp til at utfordringer bør løses ved hjelp av den beste tilgjengelige kompetansen. I mange tilfeller vil denne måtte hentes fra økosystemet som omgir virksomheten. Beste praksis for å løse en feil/svakhet vil være en «global fix», og som også gjerne forutsetter erfaringsutveksling mellom operatører. Tiltak som begrenser flyten av informasjon vil derfor lett kunne få en negativ påvirkning på safety, selv om slik påvirkning vil kunne være krevende å kvantifisere. Det vil også i dette være et element i at kommunikasjon ikke nødvendigvis er strengt formalisert, men eksempelvis vil kunne omfatte at en person deltar på fagkonferanse eller diskuterer en problemstilling med fagekspert i annen virksomhet.

Problemstillingen fra empirien der informasjonssikkerhetstiltak skapte utfordringer for kommunikasjon og samhandling innen safety (og med fare for negativt å påvirker framdrift og kvalitet), er et eksempel på det som i henhold til Perrow vil defineres som en kompleks interaksjon, og der det vil være behov for sentralisert styring og kontroll. Problemstillingen er også et eksempel på at tiltak for å redusere en risiko innen et område vil kunne medføre en økt risiko innenfor et annet område, og som ikke nødvendigvis internt i virksomheten har samme risikoeier. Det vil derfor også være behov for en overordnet risikostyring, og som ligger på et nivå høyere enn de to fagområdene. Ved å løfte styringen av risiko, kan man sikre at tiltak samlet sett har en risikoreduserende effekt og at det er en «rettferdighet» i hvordan kostnader og gevinster ved tiltak blir fordelt i organisasjonen.

En tydelig styring av grensesnittet mellom safety og security vil være en forutsetning for å kunne balansere ulike mål og hensyn opp mot hverandre. Risikoen ved svak styring av grensesnittet mellom safety og security er at de respektive fagmiljøene ikke i stor nok grad utfordres og at avgjørelser blir basert på makt (kapittel 4.3.1). En opplagt fare med dette er at definisjonsmakten over innholdet i sikkerhetskulturen vil da kunne (miss)brukes i en argumentasjon for gjennomslag for synspunkter fra de to fagmiljøene. Dette vil stå i motsetning til en helhetlig styring basert på kompromisser og ut fra et ideal om en samlet risikooptimalisering. Styring av grensesnittet mellom safety og security er også

vel anerkjent i nukleær virksomhet å ha vesentlig betydning for sikkerheten (International Atomic Energy Agency, 2021). Dette utelukker ikke at det samtidig bør være en desentralisert styring av de to fagområdene. Fagområdenes egenart og at det tidvis vil kunne være sterke koblinger, eksempelvis ved hendelser, er argumenter for autonom styring.

7.2.2 Ulik kunnskap og ulike vurderinger mellom safety og security

Ulikheter i vurderinger mellom safety og security kan anses som en troverdig forklaring på alle de identifiserte dilemmaene. Dette kan igjen tilskrives ulik kunnskap og som igjen medfører ulikheter i mål og prioriteringer. Som redegjort for i teoridelen, er det også noe ulikheter i teoretisk grunnlag og perspektiver mellom safety og security. Områdene reguleres også av ulike regelverk og involverer delvis ulike myndighetsaktører. Ulikheter i hvordan man innen de to fagområdene oppfatter risiko og hvilke risikoreduserende tiltak som er påkrevd, er derfor ikke unaturlig. Ei heller er det unaturlig om de vil ha ulikt synspunkt på hvordan balansepunktet, eksempelvis i et dilemma mellom tilgjengelighet av informasjon kontra beskyttelse av informasjon, bør ligge.

Mens truslene innen security i stor grad er eksternt fra omgivelsene og rettet mot systemet, vil farene innen safety i stor grad være interne i systemet og rettet mot omgivelsene. Energi-barriere perspektivet representer en felles tilnærming som blir brukt til å forstå og analysere hendelser innen safety og security. Det er imidlertid en fundamental forskjell mellom safety og security i forståelsen for hvorfor hendelser skjer og hvordan de utvikler seg. Innen security er den grunnleggende antagelsen at hendelser er resultat av forsettlige handlinger og med et motiv om å forårsake skade. Videre utvikling og dynamikk i hendelsen vil drives av en kjede av bevisste handlinger og som har til hensikt å omgå etablerte barrierer for slik å optimalisere konsekvensen av hendelsen.

Innen safety vil hendelser være forårsaket av teknisk svikt eller menneskelig feilhandling. Utviklingen av hendelsen vil forverres gjennom latente forhold, og som eksempelvis kan være forårsaket av komplekse interaksjoner mellom systemer. At ulykker anses å være forårsaket av feil som oppstår og får utvikle seg innenfor rammen av et sosioteknisk system, kan forklare at man innen safety har et utpreget systemperspektiv og samtidig legger stor vekt på arbeidsmessige og organisatoriske forhold for å unngå at personer gjør feil. Flere av informantene var opptatt av at ansatte innen safety skulle ha en helhetlig systemforståelse, og ikke kun forstå egen rolle og arbeidsoppgaver. Ut fra NAT og HRO teori er dette logisk ved at det vil være interaksjoner mellom personer og funksjoner på kryss og tvers av organisasjonen og der dialog ikke nødvendigvis følger formaliserte organisasjonsstrukturer. Prosesser kan gjerne styres desentralisert gjennom interaksjon er mellom fagpersoner på lavere organisatorisk nivå. Denne typen dialog er ikke nødvendigvis strengt formalisert, men allikevel svært viktig innen safety. Det framkom også i intervjuer at man innen safety er svært opptatt av forebyggende vedlikehold, tilstandskontroll og testing. Dette vil kunne forklares ut fra at latente feil gjerne aktiveres som følge av en feilhandling og teoriene rundt degradering av dybdeforsvaret over tid i en «unrocked boat» (kapittel 4.2).

Siden man innen security anser at hendelser forårsakes av intensjonelle handlinger, og ikke av hverken arbeidsmessige eller organisasjonsmessige forhold, interaksjoner og koblinger i systemer eller latente feil, blir Reasons teorier, NAT og HRO mindre viktige innen security. Samtidig kan det være verd å merke seg at alle disse perspektivene vil være relevante for evnen en security-organisasjon vil kunne ha for å håndtere en hendelse, selv om de ikke er en bakenforliggende årsak til hendelsen. Det vil derfor ikke være unaturlig om disse teoriene framover også innen security tillegges mer vekt.

Flere informanter påpekte vesentlige forskjeller i måten risikostyring skjer på innen de to fagområdene. Innen safety er farene i stor grad kjent og man har en stor grad av forståelse for hvordan anlegget fungerer i ulike situasjoner og for hvordan ulike strukturer, systemer og komponenter bidrar til den totale sikkerheten. Det vil oftest være mulig å analysere seg fram til hva som vil være effektive tiltak, ofte ned til et komponentnivå, og også for sjeldne hendelser.

Innenfor security står man ovenfor et trusselbilde og som til en stor grad er ukjent, dynamisk og i tillegg vil være i stand til å utnytte svakheter i beskyttelsen for å omgå forbyggende og konsekvensreduserende barrierer. Trusselbildet er i stor grad også eksternt og ukontrollerbart, selv om det vil kunne argumenteres for en viss grad av kontroll over en eventuell insidertrussel. Det er oftest usikkert om det finnes noen der ute med mål om å skade virksomheten, hvem disse er, hvilken intensjon de har, hvilke kapasiteter de har for å lykkes med sin intensjon og hvilken strategi de ønsker å benytte for å nå sine mål. Tilsvarende er det stor usikkerhet rundt hvordan trusselbildet vil utvikle seg i tiden framover, da dette gjerne er styrt av begivenheter andre steder i verden. Ved at trusselelementet innen security er særs usikkert, er det også vanskelig å kvantifisere risiko. Den metodiske tilnærmingen blir derfor at risikoanalysene i større grad blir brukt til å avdekke sårbarheter og tiltak blir gjennomført for å avbøte disse. Risikostyringen blir derfor mer et spørsmål om hvilke sårbarheter man kan leve med, heller enn hva som er akseptabel risiko. Gitt at usikkerhetene er såpass store, blir det i liten grad meningsbærende å snakke om sannsynligheter.

Siden de epistemiske usikkerhetene innen security ofte er langt høyere enn i safety, må man gjerne ha en mer generisk tilnærming til risiko, og som beskrevet av en av informantene. Eksempelvis gjelder dette beskyttelse av informasjon, der man kan ha svake forutsetninger for å gi en nøyaktig vurdering av hvilken informasjon som vil kunne misbrukes. Resultatet kan da bli at man ønsker å strekke hemmeligholdet så langt som mulig.

En av informantene framholdt at man innen security var opptatt av årvåkenhet, i form av å kunne tolke svake signaler for således å på et tidlig tidspunkt kunne avdekke hendelser. Dette motsvarer det som innen HRO-termologien betegnes som «mindfullness» og som også vil være et element innen safety, men vil sannsynligvis være rettet mot andre farer. Ulikheten, som beskrevet av en av informantene, relatert til at man i safety vektlegger å kunne kontrollere hendelser etter at de har skjedd mens man i security primært konsentrer seg om at hendelser ikke skal skje, lar seg vanskeligere forklare i teorien.

Selv om det ikke framkom fra intervjuene, vet vi fra teorien (kapittel 4.2) at uforutsigbarhet vil være et element innen security. Dette gjelder spesielt for kontrolltiltak og der man f.eks. ønsker å unngå at en trusselaktør planlegger en aksjon ut fra tiden for vaktrunden. Tilsvarende er ikke nødvendig innen safety, der inspeksjoner i større grad baserer seg på rene tekniske vurderinger. Uforutsigbarhet er generelt noe man i størst mulig grad prøver å unngå innen safety og er gjerne forbundet med en risiko for interaksjoner som blir oversett. Tekniske sikkerhetsmiljøer vil derfor fort kunne oppfattes som konservative, da alle endringer må vurderes grundig på forhånd.

7.2.3 Umodne administrative systemer og tekniske løsninger

Umodne administrative systemer og tekniske løsninger må antas tett knyttet opp til, og muligens forårsaket, av «Organisatoriske og styringsmessige forhold». I likhet med sistnevnte kan neppe denne årsaksforklare dilemmaene, men vil nok i stor grad være medvirkende til utfordringer knyttet til å løse dilemmaene. Eksempelvis må man anta det som uunngåelig at tiltak for å beskytte

informasjonens konfidensialitet vil måtte medføre begrensninger på informasjonsflyt og -deling, men at gode systemer og løsninger vesentlig vil redusere utfordringene.

7.2.4 Ulikheter i verdier mellom safety og security

*Verdier som tillit og åpenhet vil rimeligvis spille en rolle i forhold til dilemmaene knyttet til «*Åpenhet kontra hemmelighold» og «Insiderproblematikken». *At det er en grunnleggende ulikhet i hvordan man innen henholdsvis safety og security ser på verdien tillit er også dokumentert i litteraturen* (Bieder & Pettersen Gould, 2020).

At det innen security er et element av mistillit har en naturlig forklaring ut fra at security pr. definisjon handler om å beskytte seg mot menneskelig intensjon om å forårsake skade. Security kan derfor betraktes som en kamp mellom de onde som vil forårsake skade og de gode som vil forhindre det. Suksesskriteriene vil da bestå i på et tidlig tidspunkt å være i stand til å avdekke en slik intensjon, samt å forhindre at en slik intensjon materialiserer seg i form av skade. Erfaring har også vist at ondsinnet intensjon ikke er avgrenset til eksterne trusselaktører, men også vil kunne innehas av virksomhetens ansatte. Insidere vil ofte ha både tilganger og kunnskap om sårbarheter og derfor ofte høy kapasitet til (uoppdaget) å forvolde og maksimere skade. Å stole på færrest mulig og å begrense spredningen av informasjon til dem man har valgt å stole på er derfor en rasjonell tilnærming til å gjøre seg mindre sårbar ovenfor ondsinnede intensjoner.

Mens security handler om å beskytte systemet (objektet) mot menneskelig intensjon, vil menneskelig intensjon innen safety i større grad være knyttet til å forhindre at systemet forårsaker skade på mennesker. Intensjon spiller en vesentlig rolle også i safety, da alle bevisste handlinger bygger på en intensjon. Feilhandling kjennetegnes av at mennesker følger en plan, men der planen ikke gir et forventet utkomme. Dette i motsetning til glipp eller uvørenhet der personer ubevisst feiler i å gjennomføre en plan og der planen ville gitt det ønskede resultatet, om vedkommende hadde lykkes i gjennomføringen. Feilhandlinger kan videre klassifiseres som regelbaserte eller kunnskapsbaserte (Reason, 1997), (s71).

Den menneskelige faktoren, inkludert menneskelig intensjon, vil sannsynligvis kunne tillegges noe ulik betydning for å ivareta sikkerheten innen de ulike teoriretningene som beskrevet i kapittel 4.2, og tillegges eksempelvis en rolle:

- som en barriere innen energi-barriere-perspektivet,
- i å styre og kontrollere systemet innen NAT,
- som en integrert del av det sosioteknologiske systemet innen HRO,
- som fortolker av informasjon om systemet innenfor informasjonsprosesseserings-perspektivet,
- i å balansere systemet innenfor beslutningsperspektivet.

Betraktet ut fra energi-barriere-perspektivet, som er det perspektivet som er mest utbredt innen security, vil det primært være de funksjonene i organisasjonen som har en direkte rolle i å avdekke og respondere på ondsinnet intensjon og handlinger som vil ha en rolle i å ivareta security. Dette vil også være den gruppen man er avhengig av å ha tillit til og som også må informeres. Legger man de andre perspektivene til grunn for tenkningen innen security, blir kretsen vesentlig videre.

Innen safety handler sikkerhet i større grad om å forebygge tekniske feil og feilhandlinger. Samtidig legger man stor vekt på at feil er unngåelig og at feil i så stor grad som mulig skal være en kilde til

erfaringslæring, helst også på tvers av organisasjonen og ut over organisasjonens grenser. Åpenhet, samarbeid, dialog og erfaringsutveksling blir derfor sentrale aspekter innen safety.

Verdien åpenhet vil rimeligvis henge tett sammen med verdien tillit. Tillit vil rimeligvis være en forutsetning for åpenhet, og man kan neppe forente en vesentlig åpenhet uten at denne er basert på tillit. Samtidig vil åpenhet bidra til å bygge tillit. Man vil nok innen begge fagområder utvise åpenhet mot dem man har tillit til.

7.2.5 Ulik kultur mellom safety og security

Ulikheter i kultur mellom safety og security kan være en troverdig forklaring på flere av dilemmaene, men kanskje i første rekke dilemmaet «sikkerhetsstyring». Innholdet i dette dilemmaet er at man innen security i større grad ønsker å praktisere en regelstyring, mens man innen safety i større grad ønsker å gjøre vurderinger for hvert enkelt tilfelle. Samtidig virker det å være ulikheter i synet på hvordan regelbrudd skal sanksjoneres og der man innen security i større grad er tilhenger av hardere virkemidler.

(Pettersen & Bjørnskau, 2014) peker i sin forskning på kulturelle og strukturelle ulikheter mellom safety og security (tabell 1). Eksempelvis betrakter de organisatoriske strukturer innen safety som funksjonelle og med lokale nettverk, mens de innenfor security anses som autokratiske. De anser at klima innen safety retter seg mot å søke tillit, mens det innen security er preget av mistenksomhet. I tillegg konkluderer de med at makt innen safety formes gjennom legitimitet og ekspertise, mens innen security i større grad handler om korrektiv makt. Slike kulturelle forskjeller vil kunne forklares i at security historisk har utviklet seg innenfor det militære og nasjonal sikkerhet og derfor har et avtrykk av hieratiske militære strukturer, og som baserer seg på kommando og kontroll. Innen det militære er regelstyring essensielt, spesielt på et lavere tjenestenivå, da personer ofte ikke oppholder seg på samme sted lenge nok til å utvikle en dypere forståelse som er nødvendig for å foreta selvstendige vurderinger. Safety har nok i større grad et avtrykk fra en mer sivil tradisjon knyttet til industri og tjenesteyting. Som redegjort for i kapittel 6.1.3.1 er nok antagelig samhandling og informasjonsflyten veldig annerledes innen safety enn i security, og vil nok lett innen security kunne omfattes som en fremmed fugl, og som vil kunne gi opphav til kulturelle motsetninger.

Regelstyring kontra vurderinger i hvert enkelt tilfelle motsvarer det som hos (Reason, 1997)(s 69) beskrives som henholdsvis regelbasert og kunnskapsbasert gjennomførelse. Begge deler betraktes i utgangspunktet som gode strategier, dog for hver sin type problemstillinger. Mens litt enklere og gjenkjennbare problemstillinger best vil kunne løses ved hjelp av regler, vil nye og mer komplekse problemstillinger kreve en kunnskapsbasert tilnærming. En regelbasert tilnærming vil rimeligvis også kunne ha sine fordeler, eksempelvis ved at et velfungerende regelsett vil forenkle og effektivisere vurderingsprosessen for brukerne.

Bakgrunnen for at man innen security synes å ha en preferanse for regelbasert gjennomføring, mens man innen safety synes å ha en preferanse for kunnskapsbasert gjennomføring er ikke kjent. Empirien i denne oppgaven er også for svak til å konkludere med at det faktisk er slik og at dette er et allment skille i tilnærming mellom de to fagområdene. En mulig forklaring, om så er tilfelle, kan være at security historisk har vært betraktet som et enklere fagområde og som har vært regulert gjennom et preskriptivt regelverk og som har gitt lite rom for og behov for tilpassinger etter virksomhetens egenart. I henhold til nyere tenkning er security et særdeles komplisert fagområde og der det er store usikkerheter rundt både hvilke trusler man skal beskytte seg mot, hvordan de vil opptre og effekten av mulig mottiltak.

Ulikheter i tilnærming til regelbasert kontra kunnskapsbasert gjennomføring, vil kunne forklare ulikheter i tilnærming til sanksjoner knyttet til regelbrudd mellom safety og security. Å sikre samsvar med reglene innenfor en regelbasert gjennomføring vil i stor grad handle om at ansatte er kjent med og følger reglene. Det vil også være relativt enkelt å identifisere og sanksjonere et regelbrudd. Utfordringer vil dog oppstå i situasjoner der man bruke rigide regler på problemstillinger der disse ikke passer, og kanskje ikke var tenkt på da reglene ble skrevet. Innen kunnskapsbasert gjennomførelse vil viktige forutsetninger være at den eller de som er gitt et ansvar for problemløsningen også er gitt kompetanse og andre nødvendige forutsetninger. Å skulle sanksjonere personer fordi de er gitt oppgaver de ikke har hatt forutsetning til å løse vil være urimelig.

Uttrykket «Står man med en hammer i hånden vil det meste se ut som spiker» blir brukt som et bilde på at man gjerne fortolker virkeligheten ut fra de redskapene man har for hånden. Det er ikke urimelig å anta at ulikheter i synet på den menneskelige intensjon har en påvirkning på hvordan man innen henholdsvis safety og security fortolker og forholder seg til handlinger og hendelser. Ved at man innen security har oppmerksomhet på å avdekke intensjoner om ondsinnede handlinger, er det ikke usannsynlig at man tenderer til å ville fortolke en ondsinnet intensjon inn i en hendelse. Dette i motsetning til safety der man i større grad vil betrakte menneskelige handlinger inn i et systemperspektiv, og sannsynligvis vil ha større tendens til å fortolke feil som en svakhet i systemet. En slik ulikhet i fortolkning vil igjen kunne medføre ulikhet i hvordan man ønsker å sanksjonere regelbrudd.

7.3 Mulighetsrommet for å løse dilemma mellom safety og security

Samarbeid, dialog, koordinering, involvering av riktige personell og å søke løsninger som er gode for både safety og security ble trukket fram som viktig virkemidler for å løse motsetningene mellom safety og security (kapittel 6.2.1). Områder som av informantene ble trukket fram som spesielt relevante for samarbeid var sikkerhetsvurderinger, risikovurderinger, beredskap, utvikling av ledelsessystem og verdivurderinger av informasjonsverdier og fysiske verdier.

Tabell 7 gir en forenklet framstilling av formål, strategi, metodikk og tiltak for safety og security for et nukleært anlegg. Som beskrevet i kapittel 4.1.2, deler fagområdene et formål om å beskytte liv og helse og det er også store likheter når det kommer til ledelse av fagfeltene samt at begge deler en risikobasert tilnærming, selv om metodikken er ulik. Tilsvarende vil det være vesentlige likheter når det kommer til organisatoriske og menneskelige tiltak. Strategien for sikkerhet og de fysiske tiltakene vil i stor grad være ulike mellom fagområdene, men det vil også for disse være et vesentlig behov for samarbeid da mange av tiltakene påvirker på tvers av fagområdene. Løsninger som ensidig ivaretar ett fagområde på bekostning av det andre vil neppe være det som best ivaretar formålet om beskyttelse av liv og helse.

Det vil i alle organisasjoner være målkonflikter mellom økonomi og sikkerhet. Rene safety-dilemma er heller ikke utenkelige, eksempelvis i valget mellom løsninger med ulikt sikkerhetsnivå og ulik implementeringstid. Rene security-dilemma vil også kunne forekomme, eksempelvis at sikringstiltak forhindrer en effektiv respons på en hendelse. Utgangspunktet for diskusjonen i denne masteroppgaven er derfor at safety-security-dilemma neppe skiller seg fra andre dilemmaer, og som enhver organisasjon må forholde seg til på daglig basis. Løsningen vil som regel være i form av et kompromiss og som balanserer ut ulike hensyn og der man søker å ivareta det overordnede formålet på en best mulig måte.

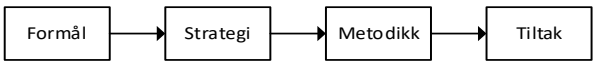
Tabell 7: *Sammenligning av sentrale deler ved sikkerhetsarbeid innen safety og security slik man typisk vil forvente å finne ved et nukleært anlegg.*

	Safety	**Security**
Formål:	Beskyttelse av liv og helse.	
Årsak til hendelse/ulykke	Flere komplementære teorier. Se tabell 2.	Ekstern eller intern trusselaktør med intensjon om å forårsake skade og optimalisere konsekvenser.
Strategier for sikkerhet	Konstruksjon, drift og vedlikehold optimaliseres for å redusere risiko for hendelse og konsekvens av hendelse.	Forhindre uautorisert tilgang til materialer og anlegg. Forhindre skade på anlegg, samt uautorisert fjerning av materialer. Beskytte informasjon.
Metodikk for etablering av tiltak	Sikkerhetsvurdering. Risikovurdering.	Trusselvurdering. Verdivurdering. Sårbarhetsvurdering. Risikovurdering.
Tiltak (fysiske)	Robust konstruksjon, redundans, diversitet og separasjon.	Herding av objekter og IKT infrastruktur. Beskyttelse av informasjon.
Tiltak (organisatoriske)	Drift, vedlikehold, overvåking, inspeksjoner, aldringskontroll, prosedyreverk, driftsgrenser, beredskapsplaner.	Kontrollrutiner, vakthold, prosedyreverk, beskyttelse av informasjon, beredskapsplaner.
Tiltak (menneskelige)	Opplæring/kompetanse.	Opplæring/kompetanse, Personellsikkerhet, Vurdering av tillit.

7.3.1 Mulighetsrommet for å løse de identifiserte dilemmaene

I intervjuene med informantene framkom det flere forhold som var viktige for å løse utfordringene mellom safety og security. Mye av dette var ledelsesmessige og organisatoriske tiltak i form av kompetanse, ressurser, tydeliggjøring av roller og ansvar, tilrettelegging for bedre samarbeid og involvering samt utvikling av et omforent ledelsessystem. I tillegg ble en felles kultur trukket fram og det ble også påpekt som viktig å informere organisasjonen om bakgrunnen for gjennomføringen av security-tiltak.

Tiltakene foreslått av informantene vil alle være viktige som forutsetning for en robust sikkerhetsorganisasjon og et godt sikkerhetsarbeid, men er i mindre grad målrettede mot det enkelte dilemma. Det er derfor viktig å analysere det enkelte dilemma og se på handlingsrommet før man kan løse det. Til bruk i denne oppgaven er det valgt en forenklet framstilling som beskrevet i figur 5 for å betrakte dilemmaene. Modellen tar utgangspunkt i at man med ut fra et formål etablerer en strategi. Man bruker deretter en metodikk (f.eks. risikoanalyse) til å bestemme tiltak.



Figur 5: *En generisk prosess for etablering av sikkerhetstiltak*.

Tanken bak denne inndelingen er at ikke alle dilemma er like, der noen vil ligge på et «dypere nivå» enn andre. Konflikt mellom to uforenelige formål vil være krevende å håndtere og forutsetter i prinsippet en prioritering fra høyeste nivå i organisasjonen. En konflikt mellom sikkerhet kontra

økonomi vil kunne falle inn i denne kategorien, selv om det her bør nyanseres at god sikkerhet forutsetter økonomi og at dårlig sikkerhet vil kunne ødelegge økonomien.

I begrepet strategi, legges her de prinsipper man velger for beskyttelsen. Denne vil i stor grad være faglig fundert ut fra anerkjent teori innen safety eller security. Handlingsrommet for endringer er begrenset, men til en viss grad vil det være mulig å vektlegge ulike elementer ulikt. Eksempelvis er det vanskelig å se for seg en full åpenhet innen security, men man kan til en viss grad kompensere for åpenhet gjennom andre tiltak. Et eksempel på dette er å gjøre vurderinger av personers pålitelighet og gi klare føringer for hvordan informasjonen forventes håndtert før informasjon deles.

Metodikken beskriver de metodene man bruker for å analysere seg fram til sikkerhetstiltakene. Innenfor utforming av tiltak vil man ofte ha relativt stor frihetsgrad. I vurderingen av tiltak er det imidlertid viktig å ha gode rutiner for endringshåndtering, slik at man så tidlig som mulig er i stand til å identifisere og adressere eventuelle utfordringer knyttet til tiltakene man planlegger.

Tabell 8: *Kategorisering av identifiserte dilemmaer.*

	Dilemma	**Type dilemma**
1	Åpenhet kontra hemmelighold.	Strategi
2	Konfidensialitet kontra tilgjengelighet for informasjon.	Tiltak
3	Insiderproblematikken.	Strategi
4	Beredskap.	Strategi
5	Risikostyring.	Metodikk
6	Sikkerhetsstyring.	Strategi

I tabell 8 er det forsøkt visualisert hvor dypt de ulike dilemmaene kan antas å ligge. Dilemmaene 1,3,4 og 6 kan nok i stor grad knyttes til ulikheter i faglige tilnærminger mellom safety og security. Dilemma 2 er i større grad på tiltaksnivå, i form av inkompabilitet mellom tiltak. Dilemma 5 handler mest om metodiske tilnærminger. Dilemmaene på et strateginivå hører naturlig hjemme på et høyt nivå i organisasjonen, mens de andre i større grad vil kunne håndteres på et lavere organisatorisk nivå.

7.3.1.1 Åpenhet kontra hemmelighold

Som utrykt av (Bieder & Pettersen Gould, 2020), er security å oppfatte som en verden av hemmelighold. Samtidig er det viktig å erkjenne at hemmelighold innen security i gitte tilfeller er av avgjørende betydning, eksempelvis ved etterretning og kontraetterretning. Det vil allikevel være rimelig å stille spørsmål ved hvor langt det er hensiktsmessig å strekke hemmelighold internt i en virksomhet.

For informasjon om trusler mot en virksomhet må det generelt anses å innebære vesentlige fordeler om denne er godt kjent innenfor virksomheten. Dette fordi medarbeidere skal kunne være i stand til selv å identifisere og vurdere situasjoner som representerer en securitymessig risiko. Dette vil videre være en forutsetning for å skape en årvåkenhet i form av «flere øyne som ser og vet hva de ser etter», slik det ble utrykt av en av informantene. Informasjon rundt eventuelle insidertrusler må rimeligvis forbeholdes noen få utvalgte. Informasjon om hvilke verdier virksomheten sitter på og som sikkerhetstiltakene er ment å beskytte, vil det sannsynligvis være mindre hensiktsmessig å hemmeligholde internt i virksomheten, da man i stor grad må anta at ansatte er kjent med dem allerede. Informasjon om sårbarheter er derimot mer tvetydig. Samtidig som åpenhet vil kunne

medføre at sårbarheter eksponeres for eventuelle insidere, må man anta at ansatte selv gjør seg sine refleksjoner og vil kunne være en viktig kilde til informasjon.

Gevinsten ved å vektlegge åpenhet internt i virksomheten, kan være høyere aksept for tiltak. Åpenhet om bakgrunnen for tiltakene vil også være viktig for å utvikle en kultur der de ansatte selv er i stand til å reflektere i situasjoner som ligger i ytterkant av hva reglene var ment å dekke, istedenfor kun å handle etter regler. Spesielt innen security, der det er store usikkerheter knyttet til trusler og hvordan disse vil kunne materialisere seg, må man anta at det vil være formålstjenlig at personer gis kunnskap som gjør dem i stand til å foreta selvstendige vurderinger.

En egnet prosess for å løse dilemmaet mellom åpenhet og hemmelighold, kan være gjennom å vurdere fordeler og ulemper med å dele ulik informasjon. En spesiell utfordring innen security vil være å kommunisere usikkerheter. Ved at truslene ofte kan være mer abstrakte innen security sammenlignet med farer innen security, vil man sannsynligvis i større grad kunne forvente spørsmål ved motivasjonen og utforming av sikkerhetstiltakene. En slik spørrende holdning er også noe som vanligvis motiveres innen safety, og vil ikke nødvendigvis være utrykk for at vedkommende ikke anerkjenner verdien av security. Det vil være viktig å betrakte denne typen tilbakemelding med åpenhet da de vil kunne være en mulig kilde til forbedringer og optimaliseringer.

7.3.1.2 Konfidensialitet kontra tilgjengelighet for informasjon

Som diskutert i kapittel 7.2.1, kan det synes å være ulikheter i kommunikasjon og samhandling mellom safety og security, og der informasjonsflyten innen security sannsynligvis i større grad følger hieratiske strukturer, mens den i safety i større grad går på tvers av virksomheten og også omfatter økosystemet rundt. Fra empirien ser vi at man innen security har bekymringer rundt informasjonsflyten innen safety, da man anser at den vil kunne eksponere eventuelle sårbarheter og som vil kunne utnyttes til å skade virksomheten. Fra empirien (kapittel 6.1.1.2) synes det samtidig å være enighet om behovet for informasjonssikkerhetstiltak på tvers av fagområdene, men divergerende oppfatninger rundt dimensjonering av tiltakene. Dimensjonering handler i denne sammenheng både om hvilken informasjon som må beskyttes og utformingen av tiltakene. Samtidig framkom det (kapittel 6.1.2.1) at eksisterende dimensjonering skaper vesentlige utfordringer for samhandling og kommunikasjon og som negativt vil kunne påvirke kvalitet og leveringsdyktighet innen safety. Det framkom også utfordringer i form av umodne administrative og tekniske systemer for håndtering og av informasjon (kapittel 6.1.3.3).

Som beskrevet i kapittel 7.2.1 er det i den studerte virksomheten et tydelig organisatorisk skille mellom safety og security. Eierskap til risiko som følge av tap av konfidensialitet vil derfor ligge hos security og det er også security som definerer tiltakene. Security er imidlertid ikke eier av den risikoen som tiltakene medfører i form av konsekvenser som følger av redusert kommunikasjon og samhandling innen safety. Det framkommer ikke i empirien en tydelig forståelse innen security for hvilke utfordringer som tiltakene medfører, og det argumenteres også i kapittel 7.2.5 for mulig ulikheter i kultur mellom safety og security når det kommer til samhandling og kommunikasjon. Samtidig legger regulatoriske krav (sikkerhetsloven) føringer for behandlingen av informasjonen, noe som også påvirker mulighetsrommet for løsninger. Dilemmaet om konfidensialitet kontra tilgjengelighet for informasjon er derfor ikke enkelt løsbart.

En forutsetning for en løsning må være god dialog mellom fagområdene. Prinsipper for security (kapittel 4.1.2) tar utgangspunkt i at security skal være samarbeidene og informert, samt at løsninger skal være hensiktsmessige og aksepterbare. I kapittel 7.3.1 argumenteres det for at dilemmaer bør

løses ved kompromiss og som balanserer ut ulike hensyn og der man søker å ivareta det overordnede formålet på en best mulig måte. Ved at det realiteten vil være vanskelig å gi en eksakt vurdering både av den faktiske effekten av informasjonssikkerhetstiltakene og av de negative konsekvensene disse medfører for kommunikasjon og samhandling innen safety, vil dette i realiteten være krevende. Dette er også diskutert videre i kapittel 7.3.1.5.

Nøkkelen til å finne en løsning på dilemmaet må være gjennom at man på tvers av fagområdene skaper en felles problemforståelse. Man bør deretter systematisk undersøke ulike løsninger for hvordan man best ivaretar behovet for beskyttelse av informasjon samtidig som man også ivaretar virksomhetens behov for kommunikasjon og samhandling. Tekniske og administrative systemer vil være et viktig element i dette, da gode systemer må antas å redusere de negative effektene på kommunikasjon og samhandling. Regelverket (sikkerhetsloven) vil sannsynligvis sette begrensning på valg av løsning, men det må allikevel antas innen rammen av et funksjonelt regelverk å være et vesentlig rom for tilpasninger. Det er også verd å merke seg at regelverket legger til grunn et proporsjonalitetsprinsipp, og som tilsier at kostnadene ved gjennomføringen av sikkerhetstiltak skal stå i forhold til det som oppnås med tiltakene.

7.3.1.3 Insiderproblematikken

Begrepet «insider» er særegent for security og blir ikke brukt i safety. Insider-problematikken representerer et vidt spekter av handlinger og med ulike motivasjoner. I den ene enden av skalaen har man personer med forsett om å alvorlige konsekvenser fra innsiden av en organisasjon. I andre enden har man personer som lekker informasjon, og som ikke nødvendigvis har en god forståelse for hvordan denne vil bli misbrukt. Personer kan også være insidere ufrivillig. Insidere vil i mange tilfeller ha god kunnskap om systemer, rutiner og eventuelle sårbarheter og vil derfor kunne omgå kontrolltiltak og forårsake stor skade. Det vil bestandig være en usikkerhet til mulig insidertrussel, og det er innen security en rasjonell strategi å begrense hvem man gir tillit til. Innen safety vil denne kretsen ofte være vesentlig videre. Dette blir i kapittel 7.2.4 forklart med forskjeller mellom safety og security når det kommer til involvering og informasjonsflyt, og der økosystemene rundt synes å ha en viktig rolle i å ivareta sikkerheten innen safety.

Man vil innen begge fagområder være avhengig av å ha tillit til mennesker. Et interessant spørsmål er imidlertid i hvor stor grad man på tvers av fagområdene har en omforent forståelse for hva man legger i tillit og grunnlaget for å kunne gi tillit. Innen safety vil tillit sannsynligvis i stor grad være relatert til om en person innehar evner, kunnskap og ferdigheter som vil bidra positivt for å unngå hendelser og ulykker. Tillit er gjerne noe man utvikler over tid og ansatte vil over tid opparbeide seg mer tillit etter hvert som vedkommende utvikler erfaring og viser å beherske oppgaver. Dette vil kunne medføre at personer blir gitt ansvar for mer kritiske oppgaver. I mange tilfeller vil dette også være en del av formaliserte programmer og der medarbeidere må oppfylle gitte krav for gitte oppgaver. Det blir i kapittel 7.3.1.6 argumentert for at feil innen safety gjerne blir betraktet i et systemperspektiv og en kilde til læring, men dette betyr ikke at det innen safety er en aksept for handlinger og opptreden som innebærer eksempelvis risikoadferd eller neglekt for regler. Slik adferd vil fort redusere den kapitalen vedkommende har bygd opp i form av tillit.

Grunnlaget for å tildele tillit innen security er nok i større grad en vurdering av kandidaten som en mulig insidertrussel. Vurderinger av evner, kunnskap og ferdigheter når det kommer til å unngå security-hendelser vil naturlig nok være en del av vurderingene. Innenfor en regelbasert gjennomførelse, vil dette rimeligvis omfatte i hvilken grad man har tiltro til at vedkommende er kjent med og motivert for å følge reglene. Grunnlaget for deling av tillit vil innen security ofte være en

formalisert prosess og med et binært svar. Eksempler på dette er en sikkerhetsklarering som enten innvilges eller ikke innvilges.

Situasjoner der personer blir møtt med tillit innen det ene fagområdet og mistillit innen det andre vil være uheldig. Et eksempel er flygere med ansvar for hundrevis av flypassasjerer som må gjennomgå sikkerhetskontroll (Pettersen & Bjørnskau, 2014). Da begge fagområder er avhengig av å være i stand til å vurdere tillit, bør vurdering av tillit være et område med mulighet for samarbeid på tvers av fagområdene, heller enn å utgjøre et vesentlig dilemma. Innholdet i et samarbeid vil eksempelvis kunne omfatte kriterier og systemer for å vurdere tillit.

Et litt grunnleggende spørsmål er i hvilken grad kontroll vil være et utrykk for mistillit. Det er innen safety vanlig at kritiske arbeidsoperasjoner kontrolleres opptil flere ganger uten at mennesker oppfatter det som problematisk. I mange tilfeller vil folk oppfatte en trygghet i dette, fordi de forstår motivasjonen bak kontrollen, ofte å unngå menneskelig feil, og har en forståelse for at kontrollen ikke er motivert i en personlig mistillit. Mennesker vil derfor antagelig i stor grad kunne akseptere kontrolltiltak. Det vil samtidig være noen legale føringer for hvor langt tiltakene vil kunne gå bl.a. gjennom virksomhetssikkerhetsforskriften (§15), og som stiller krav til at tiltakene ikke skal gå lenger enn det som er nødvendig for å håndtere en aktuell risiko og at virksomheten skal ta særlig hensyn til enkeltpersoners rettsikkerhet og personvern. Tilsvarende stiller også arbeidsmiljøloven krav bl.a. til at kontrolltiltak i virksomheten og skal ha en berettigelse, at tiltakene ikke skal innebære en uforholdsmessig belastning for de ansatte og at tiltakene må drøftes med arbeidstakerne.

I sum er det ikke gitt at insiderproblematikken representerer et vesentlig dilemma mellom safety og security, men at godt implementerte tiltak vil kunne ha gjensidig nytteverdi på tvers av fagområdene. Mye vil sannsynligvis kunne ivaretas innenfor rammene av en rapporterende kultur, en rettferdig kultur, en lærende kultur og en fleksibel kultur og som beskrevet i kapittel 4.3.3. I dette ligger at medarbeidere har en årvåkenhet og føler trygghet ved å rapportere om avvikende forhold, samt at virksomheten er i stand til å gjøre seg nytte av slik informasjon. Samtidig må virksomheten ha et godt system for å granske årsaker, og der man på en god måte hensyntar både intensjonen bak handlingen og konteksten den ble gjennomført under, og som diskutert i kapittel 7.2.5.

7.3.1.4 Beredskap

Dilemmaet er beskrevet i kapittel 6.1.1.4, og handler om hvor mye man vektlegger safety kontra security i beredskapsplanleggingen og ved håndtering av hendelser. Dette inkluderer blant annet hvilke responskapabiliteter man bygger opp og hva slags typer scenarier man øver på. Samtidig er det viktig å være klar over at beredskap ofte vil kunne havne innen det såkalte «grå området» mellom safety og security, da man ofte tidlig i hendelser ikke har noen forutsetning for å vurdere om det er en ondsinnet intensjon bak. Årsaken til en hendelse er også av underordnet betydning i en beredskapssituasjon, der hovedprioriteten må være å utnytte tilgjengelige ressurser best mulig for å håndtere hendelsen. Ut fra et likhetsprinsipp er det også hensiktsmessig at personene i organisasjonen har en rolle som er mest mulig lik den de har i normale situasjoner.

Utfordringen med beredskap vil sannsynligvis kunne reduseres om man har en god prosess for beredskapsplanlegging. Et eksempel på en prosess er gitt i (Lunde, 2014), og der beredskapsplanleggingen følger en trinnvis prosess og der dimensjoneringen og planarbeidet bygger på risikoanalyse og beredskapsanalyse. Beredskapsplan vil da dekke alle relevante deler av risikobildet og prosessen for å kravstille og tilegne ressurser vil da være lik for alle hendelsene som virksomheten velger å inkludere i beredskapsområdet.

Dilemmaet er mest sannsynlig å betrakte som et skinndilemma, så lenge man har lagt en god prosess til grunn for dimensjoneringen av beredskap. Det er også vanskelig å se noen tungtveiende grunn til at safety og security ikke skulle la seg inkludere i en felles beredskapsplan.

7.3.1.5 Risikostyring

Det framkom i empirien (kapittel 6.1.5) at man innen security, på grunn av store usikkerheter rundt trusselen virksomheten til enhver tid står ovenfor, anser det som vanskelig å estimere sannsynligheter. Man får derfor en mer kvalitativ tilnærming til risikostyring og baserer seg i stor grad på å identifisere og lukke sårbarheter. Risiko betraktes innen safety i større grad som kvantifiserbar, og som muliggjør en mer tradisjonell risikostyring. Denne ulikheten i tilnærming til risikostyring gjør det også vanskelig å etablere et overordnet risikobilde og å sammenligne risiko på tvers av fagområdene og å styre ressurser dit de har høyest risikoreduserende effekt.

Risiko handler om usikkerhet i forhold til om en gitt konsekvens inntrer eller ikke (Aven, 2015). Innenfor en kritisk realistisk vitenskapstradisjon anser man at det det vil finnes en objektiv fare eller tussel, men at denne forstås innenfor rammen av sosiale og kulturelle prosesser. Man betrakter derfor ikke risiko som en direkte målbar størrelse, slik man gjør innenfor en naiv realistisk tradisjon (Lupton, 2013). Vurderinger av individuelle risiko vil derfor være farget av hvem som gjør vurderingene og hvilken kunnskap som ligger bak vurderingene. Et risikobilde vil derfor bestandig ha usikkerhet, uavhengig av om det handler om safety eller security, og vil kanskje i beste fall representere en omforent persepsjon av risiko blant dem som har deltatt i arbeidet. Ideen om en objektiv og matematisk risikostyring er derfor lite realistisk, selv om det for ledelsen er viktig å ha en god forståelse for risikobildet til virksomheten.

Å skulle vurdere risiko for svært sjeldne hendelser/ulykker med svært høy konsekvens vil være krevende da man ofte ikke har noe empirisk grunnlag. (Rasmussen, 1997) argumenterer for at man i slike tilfeller bør basere vurderingene på modellering av systemene. Slike vurderinger vil ta utgangspunkt i energi-barriere-perspektivet, og resultater visualiseres typisk i form av sløyfediagrammer, feiltrær og hendelsestrær. Innholdet i vurderingene vil typisk omfatte robusthet og uavhengighet til de forebyggende barrierene og deres evne til å forhindre situasjon med tap av kontroll som følge av en hendelse, samt om konsekvensreduserende barrierer er tilstrekkelige for å forhindre at en situasjon med tap av kontroll medfører en uakseptabel konsekvens. En slik tilnærming til vurdering av risiko vil være vesentlig annerledes enn den man typisk følger for å vurdere mer sannsynlige hendelser og der man vil kunne basere seg på statistikk eller erfaring fra enkeltulykker.

Analyser som beskrevet over, er en del av de sikkerhetsvurderinger som brukes innen nukleær safety og som danner grunnlag for lisensiering av anlegg. Det bør derfor være rom for bedre samarbeid mellom safety og security og en mer felles tilnærming til bruk av analysemetodikk. En mulig effekt av et slikt samarbeid, vil kunne være en dypere forståelse av barriereforsvaret innen security, og som skal forhindre alvorlige konsekvenser om det skulle oppstå en hendelse. Det vil også i en slik metodisk tilnærming være mulig å betrakte beskyttelse av informasjon som en barriere, og på en systematisk måte vurdere viktigheten av å beskytte informasjon. Det vil da være mulig å analysere seg fram til om tilsvarende eller bedre effekt kan nås ved å styrke andre barrierer, og der kostnader i form av vanskeligere samhandling og kommunikasjon vil være lavere.

Den deterministiske tilnærming til sikkerhetsanalyser som beskrives her, vil kunne være til god hjelp til å vurdere sikkerhetstiltak innen security. Man vil imidlertid neppe få til en god helhetlig

risikostyring uten å inkludere sannsynligheter. En mulig løsning for å hensynta usikkerhet ved en probabilistisk tilnærming vil være ved å reflektere disse i sensitivitetsanalyser.

7.3.1.6 Sikkerhetsstyring

Enkelte informanter gav i empirien (kapittel 6.1.1.6) utrykk for at de oppfattet at det mellom safety og security var ulikheter rundt regelstyring og på måten fagområdene agerer på og sanksjonerer feil og avvik.

Som beskrevet i kapittel 7.2.3, er det flere typer feil som kan oppstå og man må også forvente at feil vil oppstå. Feil vil samtidig være en viktig kilde til informasjon om hvordan systemene eller prosesser vil kunne forbedres. En kultur som er i stand til å utnytte feil til organisatorisk læring, betegnes av Reason som en lærende kultur. Tilsvarende vil også fravær av feil kunne gi viktig innsikt til hvordan man vil kunne forbedre systemer og prosesser (noe som bl.a. er et vesentlig element innen SAFETY-2.0). Det er derfor viktig at feil rapporteres og at erfaringer blir tilbakeført. Til grunn for dette, må ligge det som Reason definerer som en rapporterende kultur og som igjen forutsetter en rettferdig kultur. Personer må derfor både oppmuntres til å rapportere om feil og forvente en rettferdig behandling om de gjør det. En viktig presisering er at en rettferdig kultur handler om en forutsigbarhet i at rapportering av feil skal bli håndtert på en rettferdig måte. En rettferdig kultur handler, med andre ord, ikke om et generelt amnesti mot konsekvenser av handlinger. Det er imidlertid viktig innenfor en rettferdig kultur på forhånd å definere hvilke handlinger som er akseptable og uakseptable. Videre er det også viktig at sanksjoner er forutsigbare og uavhengige av hvilke personer som har utført feilhandlingen. Det er rimeligvis også viktig at sanksjoner har en proporsjonalitet i forhold til feilens alvorlighet og er uavhengig av om feilen medfører en skade eller ikke. Det vil også være noen føringer bl.a. i arbeidsmiljøloven for hvordan feil kan sanksjoneres.

En handling vil iht. (Reason, 1997) bygge på en intensjon, resultere i en konsekvens og gjennomføres innenfor en kontekst. I vurderingen av sanksjonering er det viktig å skille mellom vellykket og feilet resultat på den ene siden, og riktige og gale handlinger på den andre siden. En gal handling kan godt medføre et vellykket resultat. I tillegg til kun å forholde seg til i hvilken grad regler blir overholdt eller ikke, må virksomheter i sin respons og sanksjoner av handlinger, måtte ta hensyn til bl.a. hva som er intensjonen bak handlingen og i hvilken kontekst vurderingene ble foretatt. Tilsvarende vil det måtte tas i betraktning om handlingen innebærer en uakseptabel forsømmelse eller om handlingen har basert seg på en bevisst og uberettiget risikotakning.

I utgangspunktet er det rimelig å anta at det bør være hensiktsmessig at virksomheter legger mange av de samme prinsippene til grunn for å sikre samsvar med bedriftsinterne regler, uavhengig av om disse relaterer seg til safety, security eller f.eks. etiske retningslinjer.

7.4 Kultur som virkemiddel for tettere integrering mellom safety og security.

En majoritet av informantene anså at det var viktig å ha en felles kultur og der et mindretall anså at en helt lik kultur i hele organisasjonen neppe var praktisk realistisk å få til. At god kulturell integrering på tvers av fagområdene vil kunne bidra til en tettere integrering mellom safety og security, virker også å være i henhold til teorien som beskrevet i kapittel 4.3.1. Ved at kultur handler om å dele virkelighetsoppfatning, verdier, normer etc., vil en delt kultur bidra til at mennesker tenker likt på tvers av organisasjonen. Det er derfor rimelig å anta at en omforent kultur vil fjerne mye av grunnlaget for motsetninger i en organisasjon.

I arbeidet med sikkerhetskultur er det viktig å gjøre seg noen refleksjoner rundt hvilken rolle kulturen skal ha i organisasjonen. Kulturbegrepet anses av (Guldenmund, 2018) å ha en vesentlig verdi om det av organisasjonen blir brukt som et redskap til refleksjon rundt eget sikkerhetsarbeid. Ved at kultur i seg selv ikke er en målbar størrelse, bør man utvise stor forsiktighet i å skulle sammenligne sikkerhetskultur mellom virksomheter. Sammenligning av egen sikkerhetsmessige praksis opp mot andre virksomheter og andre sektorer er imidlertid utelukkende positivt, og samsvarer godt mot prinsippet om en lærende kultur. Samtidig finnes det mange gode argumenter for i en sikkerhetsorganisasjon å sette mål og å måle framdrift i form av indikatorer. Legger vi Scheins modell (figur 3) til grunn, er det kun de to ytterste lagene av kulturen (artefakter og eksponerte verdier) som er synlig. Faren er derfor stor for at det er organisasjonens egen persepsjon av sikkerhetskulturen som måles.

7.4.1 Essensen i en kultur

B. Journé (2018) anser at en god kultur må være en balanse mellom en toppstyrt kultur vs. en profesjonsstyrt kultur. Den toppstyrte kulturen vil være felles for hele organisasjonen, mens den profesjonsstyrte kulturen i stor grad vil være ulik mellom fagavdelingene. Mange av de elementene som ble trukket fram av informantene fremstår som fornuftige i en felles overgripende kultur, f.eks.

- Gjensidig forståelse og respekt for hverandres fagområder,
- Samhandling og deling av informasjon,
- Forståelse og respekt for sikkerhetstiltakene,
- Felles forståelse for hva som er hensiktsmessig og riktig adferd
- Kontinuerlig forbedring og resillienstankegang,
- Vilje til å ta eierskap til problemstillinger og gjensidig involvering,
- Tillit og åpenhet.
- En spørrende holdning samt å legge til rette for rapportering, uten frykt for negative konsekvenser.

Disse elementene er gjenkjennelige opp mot teorien (kapittel 4.3.2), der spesielt Reasons prinsipper rundt rapporterende, rettferdig og lærende kultur synes å være reflektert i listen. Fleksibel kultur er ikke spesifikt nevnt, men en fleksibel kultur vil sannsynligvis være viktig for evnen til å løse utfordringene som identifiseres gjennom en rapporterende, rettferdig og lærende kultur. Det kan derfor argumenteres for at skille mellom byråkratiske og generative organisasjoner, er tilstedeværelsen av en fleksibel kultur i sistnevnte. Tillit og åpenhet vil samtidig være verdier som bygger opp under en slik kultur og der resultatet vil være en kontinuerlig forbedring. Tilsvarende er det flere av elementene for en felles kultur som handler om samhandling, respekt for hverandres fagområder, involvering, deling av informasjon etc. En tolkning av at disse framstår som såpass sentrale, er at det er en erkjennelse i organisasjonen av at det finnes interaksjoner og behov for samarbeid på tvers av fagområdene.

Sikkerhetskultur er ikke «one size fits all» og det er derfor viktig for organisasjonen selv å definere hva man legger i begrepet. Dette vil igjen være avhengig av farene knyttet til virksomheten. Eksempelvis vil en virksomhet der risikobildet domineres av høyfrekvente risikoer for personskade, eksempelvis en byggeplass, sannsynligvis være tjent med en annen type sikkerhetskultur enn et komplisert nukleært anlegg og der mye av oppmerksomheten ligger på å unngå lite sannsynlige hendelser og med svært alvorlig konsekvens.

Flere av sikkerhetsperspektivene som er diskutert er utviklet på bakgrunn av litt større ulykker og med komplekse årsakssammenhenger. Perspektivene vil sannsynligvis også måtte vektlegges noe ulikt basert på hvilke farer som er assosiert med ulik type virksomhet. Eksempelvis vil NAT være et

viktig perspektiv i virksomhet med tette koblinger og komplekse interaksjoner, noe som gjør at eksempelvis endringskontroll («management of change») framstår som særdeles viktig. For anlegg som er komplekse å drifte framstår HRO-perspektivet som viktig, med mye direkte dialog, endringer i driftstilstander etc. Perspektiver knyttet til sikkerhet vil typisk også kunne avhenge av hvilken rolle ulike personer har i organisasjonen, eksempelvis framstår:

- Beslutningsperspektivet som viktig for ledere og som kontinuerlig vil måtte veie ulike hensyn opp mot hverandre.
- NAT som viktig for konstruktører som skal sikre at en konstruksjon ikke har komplekse interaksjoner eller tette koblinger.
- HRO-perspektivet som viktig for en driftsorganisasjon for et komplekst anlegg.
- Informasjonsprosesseringsperspektivet som viktig for en sikkerhetsstab og som skal følge opp sikkerhetstilstanden i virksomheten.
- Energi-barriereperspektivet som viktig for analytikere og som skal vurdere designet av et sosioteknisk system.

Flere av disse perspektivene vil i utgangspunktet kunne brukes på tvers av safety og security. En god vaktfunksjon kjennetegnes av mange av de samme egenskapene som en HRO-organisasjon. Koblinger og interaksjoner vil også finnes innen security. Ikke minst gjelder dette innen digital sikkerhet. Som beskrevet i kapittel 4.1.2, er det ikke uvanlig at organisasjoner innen security utvikler en praksis basert på sedvane, regler og lovverk. Organisasjonen kan i slike tilfeller bygge seg opp rigid tro på fortreffeligheten til egne systemer - og som kan bli utfordret om en alvorlig hendelse inntreffer.

Samtidig med den ledelsesstyrte kulturen er det viktig å gi tilstrekkelig rom for utviklingen av en profesjonsstyrt kultur. Både safety og security bør være en integrert del av det daglige arbeidet for medarbeidere med svært ulike oppgaver, men og som hver ivaretar sine deler av de to fagområdene på sin egen måte og som bør være formidlet og forstått. Eksempelvis vil det være store ulikheter i rollene til en sikkerhetsvakt, en elektriker og en beredskapsrådgiver. Felles for dem alle bør være en profesjonalitet innen eget fagområde. Utviklingen av en sterk profesjonskultur forutsetter derfor en høy oppmerksomhet på utvikling av faglig kompetanse, men også en gjensidig erkjennelse av hverandres fagområder og deres egenart. I tråd med HRO-tankegang, vil viktige beslutninger i mange tilfeller bli fortatt av de beste fagekspertene. Dette forutsetter rimeligvis at ledelsen føler trygghet i den jobben de har gjort for å bygge opp fagmiljøene, og at det er en åpen og tillitsbasert dialog mellom ledelse og fageksperter.

Legger vi et informasjonsprosesseringsperspektiv til grunn, vil det være opplagte farer knyttet til om kulturen i en organisasjon blir for homogen. Dette perspektivet handler på mange måter om kulturelt ensrettede organisasjoner og med en sementert virkelighetsoppfatning, og som derfor ikke er i stand til å forstå og respondere på farer som utvikler seg over tid. Samtidig kan det argumenteres for at motsetninger i en organisasjon, om de ikke blir for store, vil kunne skape en dynamikk ved at «etablerte sannheter» i organisasjonen kontinuerlig utfordres. Dette forutsetter igjen en generativ organisasjon (kapittel 4.3.2), og som legger til rette for en spørrende holdning til etablert sikkerhetsmessig praksis og evner å omsette tilbakemeldinger til konkrete forbedringer. Dette i motsetning til patologiske organisasjoner, som ikke er åpne for tilbakemeldinger, og byråkratiske organisasjoner som ikke evner å prosessere dem og omsette dem i konkrete endringer.

7.4.2 Prosessen med å etablere kultur.

Teorien (kapittel 4.3.3) er entydig på at sikkerhetskultur ikke er en frittstående aktivitet. (Hopkins, 2018) trekker fram struktur og lederskap som grunnleggende forutsetninger for utvikling av kultur, mens (Westerum & Adimski, 2009) betrakter sikkerhetskultur som en del av den menneskelige konvolutten som omgir de sosiotekniske systemene. Som redegjort for i kapittel 4.3.3, er det innenfor forskningen ingen dekkende forståelse for hvordan kultur etableres og formes. Det virker imidlertid å være holdepunkter for at den beste framgangsmåten vil være gjennom å endre praksis, og at dette vil medføre at kulturen endres for å være kongruent med praksisen. Samtidig virker den primære arenaen for å bygge kultur, å være i måten organisasjonen jobber med sikkerhet i det daglige.

Det framkom i empirien (kapittel 6.3.4), at informantene hadde svært ulik oppfatning av om kulturen i den studerte virksomheten var felles mellom safety og security. Det kom også i empirien fram interessante forslag til hvordan man bør gå fram for å (videre)utvikle en felles kultur. Eksempelvis trakk informanter fram viktigheten av enighet om hva slags kultur man ønsker, positiv forsterkning av ønsket adferd og å måle utvikling av kulturen. Felles for mange av informantene, var imidlertid synet på kulturutviklingen som en ledelsessyrt prosess og der ledelsens rolle ble framhevd som viktig.

Viktig for ledelsen vil være å sette en tydelig retning for sikkerhetsarbeidet, ressurssette og å prioritere, men også å definere innholdet i kulturen som skal understøtte sikkerhetsarbeidet. Ledelsen vil også ha en særskilt rolle i å identifisere og håndtere dilemma og målkonflikter. I tillegg definerer og operasjonaliserer ledelsen verdigrunnlaget for virksomheten. Sannsynligvis vil alt dette være ekstra viktig i sikkerhetsorganisasjoner, der kultur vil være viktig for hvordan en organisasjon forstår farer, hvordan man forholder seg til dem, men også for valg av tiltak og aksept av tiltak. Tilsvarende vil ledelsens opptreden være viktig i forhold til om en kultur er rapporterende, rettferdig, fleksibel og lærende. Ledelsen vil generelt ha stor påvirkning på kulturen i en organisasjon, og kan påvirke kulturen både i positiv og negativ retning. Negativ påvirkning vil neppe være intensjonelt, men kan eksempelvis skje om ledelsen ikke i tilstrekkelig grad klarer å sette en retning for sikkerhetsarbeidet, ressurssette, prioritere eller løse målkonflikter.

Det framkom i kapittel 7.4.1 blant informantene synspunkt på strukturelle og organisatoriske forhold i den studerte virksomheten. Disse gikk blant annet på at det var uklarheter knyttet til organisering, ansvar, manglende ressurssetting, stor grad av bruk av innleide til fordel for utvikling av fagmiljøer «in house», manglende delegering av beslutning nedover i organisasjonen, etc. Alt dette er strukturelle problemstillinger som bør løses på ledernivå og der løsningen vil bygge opp omkring en sikkerhetskultur. Det må forventes å være svært krevende å skulle bygge kultur uten samtidig å skulle bygge struktur, systemer og ledelse. Et konkret eksempel vil være kultur for informasjonssikkerhet, og som neppe vil kunne bygges uten at det eksisterer gode tekniske og administrative løsninger for å ivareta sikkerheten, og som samtidig oppleves som hensiktsmessige og effektive. Tekniske løsninger må i denne sammenheng følges av administrative systemer, rutiner, opplæring etc. Ansvar må være definert, og det må også være mulighet for å videreutvikle løsningen basert på erfaringer og endringer i behov.

Felles kultur handler om å dele en virkelighetsforståelse, noe som blant annet inkluderer en felles forståelse for farer og hvordan man skal håndtere disse. Samhandling og dialog er derfor viktig for å skape felles kultur, og deling av informasjon mellom fagområdene er nødvendig for å få i stand en informert dialog. Dette forutsetter igjen åpenhet og tillit.

Samhandlingsarenaer mellom safety og security kan eksempelvis være utvikling av styringsdokumenter, sikkerhetsvurderinger og risikoanalyser eller i gjennomføringen av prosjekter. Ut over å bidra til omforent kultur, vil dette kunne gi positive effekter i form av at komplementerende kunnskap og perspektiver bringes inn i prosessene og at fagområdene gjensidig utfordrer hverandre. Videre er det viktig at organisasjonen har en felles forståelse og oppmerksomhet på de oppgaver organisasjonen er satt til å løse. I den aktuelle casen vil dette være en trygg nedbygging og avvikling av den norske nukleære virksomheten, og der ivaretagelse av både safety og security vil være en grunnleggende forutsetning for at dette skal kunne skje fram til det ikke er behov for noen av delene lenger.

I sum kan sikkerhetskultur forstås som å etablere en god sikkerhetsmessig praksis og der man integrerer alle elementene i den menneskelige konvolutten (kapittel 4.3.3) på en god måte. Til grunn for dette må ligge en god systemforståelse og der man ved hjelp av ulike perspektiver på sikkerhet er i stand til å identifisere farer og utfordringer, samt møte dem med menneskelige, tekniske og organisatoriske sikkerhetstiltak. For å være i stand til å vurdere om man er på riktig vei, bør man så langt som råd, ha nøye utvalgte indikatorer for å måle ulike aspekter ved sikkerheten. Samtidig må man være åpen for at de løsningene man velger vil kunne forbedres. Da er det viktig at prosessene støttes av en fleksibel kultur.

8 Konklusjon

Safety og security har et felles formål om å beskytte mennesker og miljø. Fagområdene har vesentlige likheter i metodiske tilnærminger der begge baserer seg på styring av risiko, og det er også store likheter i ledelse, organisatoriske og menneskelige tiltak. Strategier for forebygging og teknologiske tiltak er i stor grad ulike. Denne masteroppgaven har gjennom strukturerte intervjuer av medarbeidere og ledere i en utvalgt virksomhet identifisert dilemma mellom fagområdene knyttet til åpenhet/hemmelighold, konfidensialitet/tilgjengelighet for informasjon, insiderproblematikken, beredskap, risikostyring samt sikkerhetsstyring.

Dilemmaene lar seg i stor grad forklare gjennom faglige ulikheter mellom safety og security og forventes derfor også å være relevante i andre organisasjoner. Grunnleggende i dette er at man innen security anser at hendelser er et resultat av forsettlige handlinger om å forårsake skade og å maksimere skadevirkningen, mens man innen safety betrakter ulykker som forårsaket av feil. Innen safety kan ulykker videre forstås innenfor rammen av flere komplementerende teoretiske perspektiver og som tilbyr distinkt ulik forklaring på hvorfor ulykker oppstår og utvikler seg. Selv om disse perspektivene er en del av et delt kunnskapsgrunnlag mellom safety og security, er det kun det såkalte energi-barriere-perspektivet som i vesentlig grad har sin anvendelse i security. En plausibel årsak til dette er at perspektivene er utviklet for å forstå utviklingen av komplekse og alvorlige ulykker innen safety og ikke hensyntar at mennesker kan ha et forsett om å forårsake skade. Dette «lånet» av perspektiver fra safety kan forklares med at security er en framvoksende fagdisiplin og med kortere historikk som akademisk disiplin enn det safety er.

Ulikhet i hva man anser som årsaken bak hendelser/ulykker og hvilke teoretiske perspektiver man legger til grunn, vil kunne forklare mange av de faglige ulikhetene mellom safety og security. Eksempelvis vil utpreget systemtilnærming innen safety og med stor vekt på forebyggende vedlikehold, overvåking og kontroll over prosessen, kunne forklares i en oppfatning av at alvorlige

ulykker vil kunne forårsakes av *f.eks. latente patogener i systemene, koblinger og interaksjoner, drift i adferd og institusjonaliserte feiloppfatninger. At kommunikasjon innen safety ikke følger strenge organisasjonsstrukturer og også inkluderer økosystemet rundt virksomhetene, kan forklares ut fra HRO-teori. Det er heller ikke unaturlig at fagområdene har ulik fortolking av feil og avvik og hvordan disse bør sanksjoneres, avhengig av om disse anses som en kilde til organisatorisk læring eller om man er mer opptatt av å fastslå i hvilken grad reglene har blitt fulgt.*

Mens tillit og åpenhet anses som svært viktige verdier innen safety, er security i større grad kjennetegnet av mistenksomhet og hemmelighold, noe som sannsynligvis vil kunne forklares ved at man innen security vil ha en kontinuerlig årvåkenhet mot insidervirksomhet og der å avstå fra deling av informasjon vil være en rasjonell strategi for å redusere sårbarheten mot insidere. I dette ligger rimeligvis en målkonflikt i hvor langt det er hensiktsmessig å strekke hemmeligholdet opp mot gevinster i form av aksept for sikkerhetstiltakene, samt at ansatte på en informert måte skal være i stand til å handle i tråd med intensjonen bak sikkerhetstiltakene heller enn kun å handle etter regler.

Fagområdene synes å ha et felles behov i å være i stand til å vurdere tillit, men det synes samtidig å være noen nyanser i hva man legger i tillit og i hvordan tillit vurderes. Innen safety vil tillit sannsynligvis basere seg på en vurdering av om vedkommende utgjør en fare, og vil sannsynligvis i stor grad basere seg på kunnskap, ferdigheter og egenskaper hos vedkommende. En slik vurdering kan gjerne være avhengig av kontekst, f.eks. om vedkommende skal kunne utføre gitte arbeidsoppgaver. Innen security vil en vurdering av tillit sannsynligvis i stor grad basere seg på en vurdering av vedkommende som mulig insidertrussel. Vurderingsprosessen er gjerne strengt formalisert og har et binært utkomme (f.eks. at en sikkerhetsklarering innvilges eller ikke).

En utfordring med å generalisere ulikheter mellom safety og security, er at det rent vitenskapsteoretisk ikke er gjort en klar avgrensing mellom fagområdene. Samtidig kan man tenke seg flere typer handlinger som vil kunne falle i en gråsone mellom områdene, og hverken er forårsaket av rene feilhandlinger eller av en bevisst intensjon om å forårsake skade. De teoretiske perspektivene som er brukt i denne oppgaven er ikke egnet til å vurdere denne typen hendelser som ligger i «det grå området» mellom safety og security. Perspektivene er heller ikke egnet for å vurdere rene security-hendelser, eller til å forstå fagområdene i sammenheng.

Mens risiko innen safety ofte vil være intern i systemet, stabil, forståelig og håndterbar, står man innen security ofte ovenfor en ekstern trussel og som i stor grad er ukjent, dynamisk og ukontrollerbar. Det framkom derfor i empirien vesentlige forskjeller i risikostyring mellom de to fagområdene. Det er innen security generelt vanskelig å vurdere sannsynligheter, og risikostyringen baserer seg derfor i stor grad på vurdering og håndtering av sårbarheter. Dette i motsetning til safety og der det i stor grad er mulig å kvantifisere både sannsynlighet og konsekvens. Dette skaper utfordringer for en helhetlig risikostyring, der man ønsker å sette inn ressursene der de har størst risikoreduserende effekt. I tillegg skaper det utfordringer i tilfeller der håndtering av risiko innen ett av fagområdene kan medføre en risiko i det andre. Et eksempel fra den studerte virksomheten, er at tiltak for å sikre konfidensialiteten til informasjon reduserer tilgjengeligheten og dermed negativt kan påvirke samhandling, kvalitet og framdrift innen safety. Interaksjoner mellom fagområdene medfører derfor et behov for en tydelig overordnet styring av grensesnittet mellom områdene.

Med sikkerhetskultur mener vi den delen av organisasjonskulturen som har betydning for hvordan organisasjonen ivaretar sikkerheten. Begrepet skaper en forbindelse mellom institusjonaliserte holdninger, verdier, virkelighetsforståelse etc. og sikkerhetsmessig adferd. Sikkerhetskultur skapes i hverdagen gjennom dialog og interaksjoner mellom virksomhetens medarbeidere. Sikkerhetskulturen endres primært gjennom å endre sikkerhetsmessig praksis. Samtidig er det viktig å være bevisst på at

sikkerhetskultur ikke er et isolert fenomen, men henger tett sammen med f.eks. ledelse, organisasjonsstrukturer og teknologi. Ledelsen har derfor en avgjørende påvirkning på hvordan kultur formes og utvikler seg. Kultur handler i stor grad om å dele en virkelighetsforståelse, verdier, tilnærminger etc., og det er derfor rimelig å anta at felles kultur på tvers av virksomheten vil gi tettere integrering og dempe motsetninger mellom safety og security.

Innholdet i en sikkerhetskultur må tilpasses den enkelte organisasjon, dens virksomhet, farepotensial, og relevante sikkerhetsperspektiver. Det har gjennom intervjuene med informantene framkommet flere interessante tanker knyttet til essensen i en virksomhetsovergripende kultur, og der Reasons konsepter om en rapporterende, en rettferdig, en fleksibel og en lærende kultur framstår sentrale.

I en organisasjon der medarbeidere har ulike arbeidsoppgaver og roller, vil det neppe være realistisk å skape en fullstendig lik kultur på tvers av virksomheten. Samtidig som ulikheter i kultur på tvers av organisasjoner tidligere har vist seg å være en medvirkende årsak til ulykker, er det grunn til å stille spørsmål til om ikke kulturell ensrettethet også vil være en risiko for en virksomhet. Tidligere forskning argumenterer for at en sterk virksomhetsovergripende kultur bør balanseres opp mot en sterk profesjonskultur og der fagmiljøene får tilstrekkelig rom for å utvikle en særegen kultur basert på sunne faglige prinsipper. En god sikkerhetskultur handler ikke om en tilstand av harmoni der alle i organisasjonen til enhver tid tenker likt, men heller om at organisasjonen er i stand til å bruke ulikheter i oppfatninger på en konstruktiv måte til å forbedre sin sikkerhetsmessige praksis.

8.1 Forslag til videre arbeid

Som det framkommer i kapittel 4.2 tar diskusjonene i denne oppgaven utgangspunkt i fem sentrale perspektiver rundt sikkerhet og bruker disse til å forklare forskjeller i tilnærminger og praksis mellom safety og security. Det teoretiske grunnlaget rundt sikkerhet er generelt vesentlig videre enn som så, og spesielt makt-perspektivet framstår i denne forbindelse som spesielt interessant. Dette er et perspektiv som er anerkjent som viktig innen sikkerhet, og gransking bl.a. av Challanger-ulykken viste også at makt har en avgjørende betydning for hvordan organisasjoner vurderer og håndterer risiko. Sentrale maktforskere anser også at makt er av vital betydning for hvordan rasjonalitet defineres. Til tross for dette, er forholdet mellom makt og sikkerhet i liten grad forsket på. Det er videre kjent at makt vil kunne utøves på flere måter. Definisjonsmakt, kunnskap og kontroll over informasjon og tilgangen på informasjon er blant disse. Innen security blir beslutninger i stor grad foretatt av mektige aktører og gjennom lukkede prosesser. Å studere maktens påvirkning på risikotenkning og risikohåndtering mellom safety og security ville derfor vært et interessant tema.

9 Referanser

Antonsen, S., 2009. Safety Culture and the issue of power. *Safety science*, pp. 183-191.

Antonsen, S., 2018. Key Issues in Understanding. I: C. Gilbert, H. Laroche, B. Journé & C. Bieder, red. *Safety Cultures, Safety Models. Taking Stock and Mowing Forward.* Cham: Springer Nature Switzerland AG, pp. 127-136.

Aven, T., 2014. What is safety science?. *Safety Science 67*, pp. 15-20.

Aven, T., 2015. *Risikostyring*. 2.utgave red. s.l.:Universitetsforlaget.

Bieder, C. & Pettersen Gould, K., 2020. Exploring the Interrelations Between Safety and Security: Reseach and Management Challanges. I: C. Bieder & K. Pettersen Gould, red. *The Coupling of Safety and Security: Exploring Interrelations in Theory and Practice.* Cham: Springer Nature Switzerland AG, pp. 105-112.

Blokland, P. B. & Reiners, G. L., 2020. The Consept of Risk, Safety and Security: A Fundamental Exploration and Understanding of Similarities and Differences. I: C. Bieder & K. Pettersen Gould, red. *The Coupling of Safety and Secuiry: Exploring Interrelations in Theory and Practice.* Toulouse: France, pp. 9-16.

Blokland, P. J. & Reniers, G. L., 2020. The Concepts of Risk, Safety and Security: A Fundamental Exploration and Understanding of SImilarites and Differences. I: C. B. a. K. P. Gould, red. *The Coupling of Safety.* Cham, Switzerland: SpringerBriefs in Safety Management,, pp. 9-16.

Brooks, D. J. & Coole, M., 2020. Divergence of Safety and Security. I: C. Bider & K. Pettersen Gould, red. *The Coupling of Safety and Security: Exploring Interrelations in Theory and Practice.* Cham: Springer Nature Switzerland AG, pp. 63-74.

Cooper, M. D., 2018. The Safety Culture Construct: Theory and Practice. I: C. Gilbert, B. Journé, L. Hervé & C. Bieder, red. *Safety Culture, Safety Models. Taking Stock and Moving Forward.* Cham: Springer Nature Switzerland AG, pp. 47-62.

Guldenmund, F. W., 2018. Understanding Safety Culture Trough Models and Metaphors. I: E. Gilbert & H. Laroche, red. *Safety Cultures, Safety Models. Taking Stock and Moving Forward.* Cham: Springer Nature Switzerland AG, pp. 21-34.

Hopkins, A., 2018. The Use and Abuse of "Culture". I: C. Gilbert, H. Laroche, B. Journé & C. Bieder, red. *Safety Cultures, Safety Models.Taking Stock and Moving Forward.* Cham: Springer Nature Switzerland AG, pp. 35-46.

International Atomic Energy Agency, 2021. *The Nuclear Safety and Nuclear Security Interface: Approaches and National Experiences,* Wien: International Atomic Energy Agency.

International Organisation for Standardization, 2018. *Risikostyring Retningslinjer, NS-ISO 31000,* s.l.: Standard Norge.

Jore, S. H., 2019. The Conceptual and Scientific Demarcation of Security in Contrast to Safety. *Eur J Secur Res 4*, pp. 157-174.

Journé, B., 2018. A Pluralist Approach to Safety Culture. I: C. Gilbert, H. Laroche, B. Journé & C. Bieder, red. *Safety Cultures, Safety Models. Taking Stock and Moving Forward.* Cham: Springer Nature Switzerland AG, pp. 63-70.

Leveson, N., 2020. Safety and Secuiry AAre Two Sides of the Same Coin. I: C. Bieder & K. Pettersen Gould, red. *The Coupling of Safety and Security: Exploring Interrelations in Theory and Practice.* Cham: Springer Nature Switzerland AG, pp. 17-28.

Lunde, I. K., 2014. *Praktisk krise- og beredskapsledelse.* 2 red. Oslo: Universitetsforlaget.

Lupton, D., 2013. *Risk.* 2. Edition red. Oxford: Taylor & Francis Group,.

Marx, D., 2018. The Use and Abuse of "Culture". I: C. Gilbert, H. Laroche, B. Journé & C. Bieder, red. *Safety Cultures, Safaty Models. Taking Stock and Moving Forward.* Cham: Springer Nature Switzerland AG, pp. 71-80.

Möller, N., Hansson, S. O. & Peterson, M., 2006. Safety is more than the antonym of risk. *Journal of Applied Philosophy, Vol 23, No. 4*, pp. 419-432.

Pettersen Gould, K. & Bieder, C., 2020. Safety and Security: The Challanges of Bringing Them Together. I: C. B. a. K. P. Gould, red. *The Coupling of Safety.* Toulouse, France: SpringerBriefs in Safety Management,, pp. 1-7.

Pettersen, K. A. & Bjørnskau, T., 2014. Organizational contradictions between safety and security - Percieved challanges and ways of integrating critical infrastructure protection in civil aviation. *Safety Science 71*, pp. 167-177.

Rasmussen, J., 1997. Risk Management in a Dydamic Society: A Modelling Probalm. *Safety Science Vol 27, No 2/3*, pp. 183-213.

Reason, J., 1997. *Managing the Risk of Organizational Accidents.* 1 red. New York: Routledge.

Rosness, R. et al., 2004. *Organisational Accidents and Resillient Organisations: Five Perspectives,* Trondheim: Sintef Industrial Management.

Smith, C. L. & Brooks, D. J., 2013. *Security Science. The Theory and Practice of Security.* 1 red. Oxford: Elsevvier.

Westerum, R. & Adimski, A. J., 2009. Organizational Factors Assocciatedwith Safety and Mission Success in Aviation Environment. I: J. A. Wise, V. D. Hopkin & D. J. Garland, red. *Handbook of Aviation Human Factors, 2. edition.* s.l.:Taylor & Francis Inc, pp. Chapter 5: 1 -37.

Vedlegg 1: Intervjuguide

Undersøke hvilke dilemmaer det er mellom safety og security og mulig opphav til disse.

Hvilke dilemma mellom safety og security obeserverer du i organisasjonen?

- Hva består disse i?
- Hva resulterer de i?
- Hva tror du årsaken kan være?
- Hvordan håndterer du dem i det daglige?

Oppfatter du det er vesentlige forskjeller på hvordan man arbeider innenfor safety med farer og hvordan man innenfor security arbeider med trusler?

- Hva består disse forskjellene i?

Undersøke mulighetsrommet for samhandling mellom safety og security, for å sikre synergier og unngå motsetninger.

Målkonfliktene, som diskutert over, på hvilken måte kan de best løses?

I hvilken grad anser du at det er rom for mer og bedre samhandling mellom safety og security?

- På hvilke områder?
- Hvilke effekter vil det ha?

Hva anser du som viktigste begrensning for samhandling?

Diskutere om, og eventuelt hvordan, en felles virksomhetsovergripende kultur vil kunne bidra til en tettere integrering mellom safety og security.

Hva legger du i begrepet sikkerhetskultur?

Opplever du at det er en felles kultur på IFE og som omfatter både safety og security?

- Hvorfor/hvorfor ikke?

Diskutere hva som bør være essensen i en omforent kultur og hvordan man bør gå fram for å etablere den.

Hva oppfatter du bør være essensen i en omforent kultur som inkluderer både safety og security?

Hvordan bør IFE gå fram for å etablere en slik omforent kultur?

Er det viktig å ha en felles kultur, eller er det ok om kulturen er litt ulik i ulike deler av den nukleære virksomheten?