

UNIVERSITETET I STAVANGER

**MASTERGRADSSTUDIUM I
RISIKOSTYRING OG SIKKERHETSLEDELSE**

MASTEROPPGAVE

SEMESTER:

Vår og høst 2022

FORFATTER:

Erik Halvorsen

VEILEDER:

Bjørn Ivar Kruke

TITTEL PÅ MASTEROPPGAVE:

Hvordan er påliteligheten til perimetersikringen rundt Industriområdet?

EMNEORD/STIKKORD:

Trusselbilde, trusselaktører, scenarioer, tilsiktede uønskede handlinger, security, perimetersikring, barrierer, MTO, sikkerhetskultur, beredskap,

SIDETALL: 133

STAVANGER 30.06.2022.....
DATO/ÅR

Sammendrag

Hvordan er norske industriområder sikret mot uønsket adgang gjennom perimetersikringer?
Er norske industriområder tilstrekkelig sikret mot uønsket inntrenging og har man tilstrekkelig fokus på security, sikring mot vilde uønskede handlinger?

«Det var midt på natten mandag 21. september i 2020 at kvinnen fra Notodden og to menn tok seg inn på industriområdet i Gvarv i Midt-Telemark. De skal ha brukt en vinkelsliper for å skjære opp fem trafokiosker som tilhører Midt-Telemark Energi.»
(Løsnæs, 2022).

«Industribedriftene på Øra har sett seg kraftig lei på de mange innbruddene på området. I løpet av en 14-dagersperiode ble det loggført hele elleve innbrudd.»
(Bolstad, 2014).

«Natt til mandag måtte politiet ta hånd om to menn i 50-årene som hadde tatt seg inn på industriområde på Langstranda i Bodø. Dette meldte politiet i Nordland på Twitter like før klokken seks. I meldingen skriver politiet at de fant en kniv på den ene mannen.» (Stenbro, 2019).

I henhold til Nasjonal Sikkerhetsmyndighet er det slik at gapet mellom trusselen og sikkerhetsnivået i norske virksomheter og samfunnsfunksjoner øker, blant annet som følge av at bevisstheten og kompetansen om trussel- og risikobildet og hva som utgjør god nok sikkerhet er for svak. «Sikkerhetstiltakene er ikke dimensjonert for det reelle trusselbildet, eller innføres ikke raskt nok når nye sårbarheter oppstår» (Sikkerhetsmyndighet, 2022, s. 8).

Er det slik at norsk industri har så stort fokus på safety hendelser og HMS at fokuset på security har blitt nedprioritert og er kunnskapen om security i norsk industri for liten?

For å belyse dette har jeg i denne studien jobbet med å besvare følgende problemstilling ved et større industriområde i Norge:

«Hvordan er påliteligheten til perimetersikringen rundt Industriområdet?»

For å utdype denne problemstillingen har jeg utviklet følgende tre forskningsspørsmål som vil være med på å belyse problemstillingen:

- 1. «Hva slags barrierer etableres for å ivareta perimetersikringen?»***

2. «*Hvordan er informasjonsflyten blant samvirkerne som opprettholder barrierene?*»

3. «*Hva truer påliteligheten til dagens perimetersikring?*»

Metoder brukt i studien er dokumentanalyse, aktiv informantintervjuing, deltagende observasjoner og innhenting av relevant teori.

Sentrale begreper er *perimetersikring, barrierer, latente forhold og hull i barrierer*. Noen av teoriene benyttet for å belyse dette er følgende.

Haddon (1980) snakker i sin *barrieremodell* om barrierer som tette vegger mellom en trussel og en verdi. *Stranden* (2019) sitt sikringstrekløver, hvor *Mennesket, Organisasjon* og *Teknologi* hvor barrierer inngår. *Turner* (1976) sitt *informasjonsprossesseringsperspektiv* hvordan dette kan være med på å påvirke organisasjoner og mulige uønskede handlinger. *Sklet* (2006) deler opp barrierer i *Barriersystem, Barriereelement* og *Barrierefunksjon*. *Reason* (2016) sin *Swiss-cheese-modell* som sier at det i alle barrierer kan finnes hull eller latente forhold.

Funn viser at det ikke er forsterking i barrierene ved forhøyet trusselnivå mot Industriområdet. Industriområdet har samlet ansvaret for safety og security under en stilling. Funn fra teori og dokumentasjon, blant annet fra Statoil sin granskingsrapport «The In Amenas attack» fra 2013, viser at dette kan være en uheldig kombinasjon av roller og man bør i organisasjonen søke å dele safety og security inn i to likestilte ansvarsområder.

Det blir ikke satt i gang søk etter inntrengere dersom man oppdager hull i perimetersikringen. Man tetter hullet uten at det blir gjort forsøk på å finne, eller varslet om eventuelle inntrengere. Det er adgangskontroll som registrerer ansatte inn på, men ikke ut av Industriområdet. Dette kan føre til personell som kan oppholde seg på Industriområdet over lang tid og da ha tid til å planlegge, forberede og gjennomføre anslag.

Man ser behov for videre forskning. Studien viser det er forhold rundt perimetersikringens pålitelighet som bør jobbes videre med. Hva er rett nivå for en perimetersikring av et industriområde, sett opp imot de verdier man ønsker å sikre? Hva er hensiktsmessig sikkerhet for et industriområde, som hindrer uønsket inntrenging, men som allikevel gjør det effektivt å drifte daglige inn og utpasseringer av leveranser, ansatte og besøkende? For at dette videre skal forskes på krever dette dedikerte security kyndige ansatte som har denne oppgaven som sin hovedprioritet, og ikke i tillegg til fokus på safety relaterte arbeidsoppgaver.

Forord

Tenk at en samtale med en kasserer i skolemusikken kan føre til en masteroppgave skrevet fra et helt annet felt enn min egen profesjon, men slik har det altså blitt. Jeg vil selvfølgelig få lov til å takke kassereren for alle samtaler og hans oppriktige interesse for hva jeg har gjort underveis i studien og oppgaven.

Samtidig må jeg si at dette selvfølgelig ikke hadde blitt en realitet uten den mottakelsen, åpenheten, velviljen og tilliten som Industriområdet har vist meg underveis i studien. Alle dører har blitt åpnet på vidt gap og jeg har fått lov til å snoke rundt alle plasser jeg har ønsket. Samtidig vil jeg få takke alle informanter, som velvillig har stilt opp og besvart mine spørsmål både i intervjuer men også, og kanskje spesielt også, i situasjoner under deltakende observasjoner. Og sist men ikke minst min lokale veileder, samtalepartner og partner i crime, lokal HESQ-manager på Industriområdet. Uten ditt samarbeid, ville dette prosjektet ikke kunne vært realisert.

Jeg vil takke min veileder, professor Bjørn Ivar Kruke, som allerede før masteroppgaven ble en realitet, var med på å sortere tanker og skape refleksjoner rundt temaet. Takk for tålmodighet og diskusjoner gjennom hele prosessen og for at du har pushet meg gjennom dette. Samtidig vil jeg også takke en annen god samtalepartner og inspirasjonsbooster, når ting har virket litt svart, Beate Lauritzen.

Så vil jeg takke familien for at de har holdt ut med meg i de årene jeg har brukt på denne utdanningen. Hvem hadde vel trodd for 5 år siden at jeg skulle skrive en masteroppgave i noe som helst. Takk for støtte velvilje og hjelp gjennom studiet. Nå er jeg endelig ferdig!

Erik Halvorsen

Lillestrøm

Innholdsfortegnelse

| | |
|---|------|
| Sammendrag | i |
| Forord | iii |
| Figuroversikt | viii |
| Tabelloversikt | ix |
| 1. Innledning | 1 |
| 1.1 Hvorfor og hvordan denne oppgaven om Industriområdet? | 1 |
| 1.2 Tema for oppgaven, perimetersikring og tidligere forskning på dette | 2 |
| 1.3 Formålet med studien | 4 |
| 1.4 Studiens avgrensning | 5 |
| 1.5 Oppgavens oppbygging | 6 |
| 2. Teori | 8 |
| 2.1 Safety og security | 8 |
| 2.2 Risiko | 9 |
| 2.2.1 Risikovurderinger og risikoanalyser | 10 |
| 2.3 Verdier | 13 |
| 2.4 Trusler | 13 |
| 2.4.1 Trusselkategorier | 14 |
| 2.4.2 Trusselaktører | 14 |
| 2.4.3 Trusselnivå og trusselscenarioer | 15 |
| 2.5 Sikring | 16 |
| 2.5.1 Barrierer og tiltak | 18 |
| 2.5.2 Latente forhold | 24 |
| 2.5.3 Sikkerhetskultur | 25 |
| 2.6 Beredskap | 27 |
| 2.7 Oppsummering av teori | 30 |
| 3. Metode | 31 |

| | | |
|-------|---|----|
| 3.1 | Forskningsdesign | 31 |
| 3.2 | Casestudie | 32 |
| 3.3 | Datainnsamling | 34 |
| 3.3.1 | Observasjoner | 34 |
| 3.3.2 | Aktiv informant intervjuing/ samtaleintervju og semistrukturerte intervjuer | 37 |
| 3.3.3 | Dokumentanalyse | 40 |
| 3.3.4 | Internett søk etter relevante dokumenter | 41 |
| 3.3.5 | Utfordringer, pålitelighet og reliabilitet ved datainnsamlingen | 42 |
| 3.3.6 | Mottakelsen på industriområdet og av informantene | 42 |
| 3.4 | Bias – Forskerens forforståelse og virkelighetsoppfatning | 43 |
| 3.5 | Studiens troverdighet eller interne validitet | 45 |
| 3.5.1 | Troverdighet | 46 |
| 3.5.2 | Studiens overførbarhet | 48 |
| 3.5.3 | Studiens bekreftbarhet | 49 |
| 3.5.4 | Studiens pålitelighet (reliabilitet) | 50 |
| 3.6 | Etiske hensyn knyttet til studien | 51 |
| 3.7 | Styrker og svakheter ved studien | 51 |
| 4. | Empiri | 53 |
| 4.1 | Dokumentanalysen | 53 |
| 4.1.1 | Hva slags barrierer etableres for å ivareta perimetersikringen av Industriområdet? | 53 |
| 4.1.2 | Hva truer påliteligheten til dagens perimetersikring? | 54 |
| 4.1.3 | Hvordan er informasjonsflyten blant samvirkerne som opprettholder barrierene i perimetersikringen rundt Industriområdet? | 56 |
| 4.1.4 | Funn fra annen dokumentasjon rundt perimetersikring | 56 |
| 4.2. | Intervjuer | 59 |
| 4.2.1 | Hva slags barrierer etableres for å ivareta perimetersikringen av Industriområdet? | 59 |

| | | |
|-------|--|----|
| 4.2.2 | Hva truer påliteligheten til dagens perimetersikring? | 60 |
| 4.2.3 | Hvordan er informasjonsflyten blant samvirkerne som opprettholder barrierene i perimetersikringen rundt Industriområdet? | 63 |
| 4.3. | Deltakende observasjoner..... | 63 |
| 4.3.1 | Hva slags barrierer etableres for å ivareta perimetersikringen av Industriområdet? | 64 |
| 4.3.2 | Hva truer påliteligheten til dagens perimetersikring? | 66 |
| 4.3.3 | Hvordan er informasjonsflyten blant samvirkerne som opprettholder barrierene i perimetersikringen rundt Industriområdet?..... | 68 |
| 4.4. | Samtaler under deltakende observasjoner | 69 |
| 4.4.1 | Hva slags barrierer etableres for å ivareta perimetersikringen av Industriområdet? | 69 |
| 4.4.2 | Hva truer påliteligheten til dagens perimetersikring? | 71 |
| 4.4.3 | Hvordan er informasjonsflyten blant samvirkerne som opprettholder barrierene i perimetersikringen rundt Industriområdet? | 72 |
| 4.5. | Oppsummering empiri..... | 73 |
| 5. | Drøfting | 75 |
| 5.1 | Hva slags barrierer etableres for å ivareta perimetersikringen? | 75 |
| 5.1.1 | Industrigjerdet med porter | 77 |
| 5.1.2 | Adgangskontroll | 79 |
| 5.1.3 | Sikkerhetskurs | 80 |
| 5.1.4 | Kameraovervåking | 80 |
| 5.1.5 | Hovedresepsjonen, døgnbemannet vaktentral og havneport | 81 |
| 5.1.6 | Industriberedskapen | 82 |
| 5.1.7 | Oppsummering av barrierene som etableres for å ivareta perimetersikringen..... | 83 |
| 5.2. | Hvordan er informasjonsflyten blant samvirkerne som opprettholder barrierene?..... | 84 |
| 5.3. | Hva truer påliteligheten til dagens perimetersikring? | 87 |
| 5.3.1 | Industrigjerdet med diverse porter | 88 |

| | |
|---|------|
| 5.3.2 Adgangskontroll | 91 |
| 5.3.3 Sikkerhetskurs | 92 |
| 5.3.4 Kameraovervåking | 93 |
| 5.3.5 Hovedresepsjonen, døgnbemannet vaktsentral og havneport | 95 |
| 5.3.6 Industrieredskapen | 97 |
| 5.3.7 Hvordan er informasjonsflyten blant samvirkerne som opprettholder barrierene .. | 99 |
| 5.3.8 Oppsummering av barrierenes pålitelighet | 100 |
| 5.4. Hva er påliteligheten til perimetersikringen rundt Industriområdet? | 103 |
| 6. Konklusjon | 105 |
| 6.1 Viktige funn fra studien..... | 105 |
| 6.2 Forslag til videre forskning | 107 |
| 6.3 Anbefalinger..... | 107 |
| Referanser..... | 109 |
| Vedlegg 1: Informasjon til informanter i forkant av semistrukturert intervju..... | I |
| Vedlegg 2: Spørreskjema til semistrukturerte intervjuer..... | VI |
| Vedlegg 3: kopi av mailutveksling med NSB i forhold til meldepliktig oppgave..... | VIII |

Figuroversikt

| | |
|---|----|
| Figur 1: Matrise, tofaktormodellen | 10 |
| Figur 2: Bow-Tie | 11 |
| Figur 3: Trefaktormodellen | 12 |
| Figur 4: Tabell trusselvurdering | 16 |
| Figur 5: Gjengivelse av modellen Sikringstrekløveret - 1 | 17 |
| Figur 6: Gjengivelse av modellen Sikringstrekløveret - 2 | 17 |
| Figur 7: Haddon's 10 accident prevention strategies..... | 19 |
| Figur 8: Bilde av Emirates stadium I | 20 |
| Figur 9: Bilde av Roadblockers..... | 20 |
| Figur 10: Swiss Cheese | 21 |
| Figur 11: The sequence of events associated with a failure of foresight | 22 |
| Figur 12: Modell for utvikling og gransking av ulykker..... | 24 |
| Figur 13: Hudsons (2007) kulturelle stige..... | 26 |
| Figur 14: Gjengivelse av modellen Læringstrappen | 28 |
| Figur 15: Gjengivelse av modellen Øvelsestyper | 29 |
| Figur 16: Bilde av Emirates stadium II | 57 |
| Figur 17: Kjøretøysperrer..... | 57 |
| Figur 17: Haddon's 10 accident prevention strategies..... | 75 |
| Figur 18: Eksemplifisering av barrierenes formål..... | 76 |
| Figur 20: Forenklet versjon av Reason sin Swiss-Cheese modell som viser barrierene i perimetersikringen..... | 83 |
| Figur 219: The sequence of events associated with a failure of foresight | 84 |
| Figur 20: Samvirkerne som opprettholder informasjonsflyten rundt perimetersikringen..... | 85 |
| Figur 21: Gjengivelse av modellen Sikringstrekløveret - 2 | 87 |
| Figur 22: Hull og latente forhold i barrieren Industrigjerdet med porter. | 90 |
| Figur 23: Hull og latente forhold i barrieren Adgangskontroll. | 92 |

| | |
|--|-----|
| Figur 24: Hull og latente forhold i barrieren Sikkerhetskurs | 93 |
| Figur 25: Hull og latente forhold i barrieren Kameraovervåking. | 95 |
| Figur 26: Hull og latente forhold i barrieren Hovedresepsjonen, døgnbemannet vaktentral og havneport. | 97 |
| Figur 27: Gjengivelse av modellen Øvelsestyper | 98 |
| Figur 30: Hull og latente forhold i barrieren Industriberedskap | 99 |
| Figur 28: Hull og latente forhold i barrieren Hvordan er informasjonsflyten blant samvirkerne som opprettholder barrierene | 100 |
| Figur 29: Barrierer i en modell av Strandens (2019) sikringstrekløver | 102 |
| Figur 33: Swiss-cheese-modell tilpasset spesifikt for denne studien | 103 |

Tabelloversikt

| | |
|---|-----|
| Tabell 1: Oversikt over aktiviteter i studien | 37 |
| Tabell 2: Oversikt over informanter | 39 |
| Tabell 3: Oversikt over funn ved søk på internett | 41 |
| Tabell 4: Tabellvis fremstilling av Swiss-cheese av funn fra oppgaven | 102 |

1. Innledning

16. januar 2013 tok uautorisert personell seg inn gjennom perimetersikringen på Statoils industriområde i In Amenas i Algerie. Det som viste seg å være et terrorist-angrep, som varte fra 16. til 19. januar, resulterte i 40 drepte, hvorav 5 Statoil ansatte. Angrepet ble gjennomført ved at det 05:40 ble gjort anslag mot både bo- og produksjonsanlegget, noe som gjorde at terroristene fikk kontroll over produksjonen og de ansatte. Noe som igjen gjorde at produksjonen på anlegget ble stoppet (Statoil, 2013).

Statoil hadde vurdert at perimetersikringen rundt anlegget i In Amenas skulle detektere og hindre angrep eller anslag på en slik måte at eventuelle angripere skulle bli oppholdt eller hindret i tilstrekkelig tid til at Algeriske militærstyrker kom til unnsetning. Ved dette terrorangrepet viste det seg at den dimensjoneringen som var tatt inn i perimetersikringen ikke var tilstrekkelig til at intensjonen ble opprettholdt og terroristene fikk kontroll over anlegget.

Angrepet var på forhånd vurdert som en hendelse «lite sannsynlig med høy konsekvens». Perimetersikringen i samarbeid med militærstyrker fra Algerie var vurdert som tilstrekkelig sikkerhet mot slike anslag. Rapporten i etterkant av terrorangrepet peker på flere funn rundt perimetersikringen og vurderingene rundt denne som medvirkende årsaker til at dette angrepet kunne finne sted. Rapporten «The In Amenas attack» (Statoil, 2013), kommer med 19 anbefalinger i etterkant av sin gransking av hendelsen for å bedre sikkerheten rundt Statoil sine anlegg og også videre i organisasjonen. Noen av disse anbefalingene vil bli tatt inn videre i denne oppgaven.

Selv om vi ikke har opplevd liknende anslag eller angrep som dette på installasjoner eller industriområder i Norge, er funnene og anbefalingene fra granskingsrapporten etter In Amenas angrepet viktige. Man ser ikke bare anbefalingene knyttet mot industriområdet i Algerie, men kommer med anbefalinger rundt sikkerhet, sikkerhetsledelse og sikkerhetskultur som kan tas inn i liknende organisasjoner og industriområder.

1.1 Hvorfor og hvordan denne oppgaven om Industriområdet?

Som fengselsbetjent har jeg i mange år interessert meg for perimetersikring. Hvordan sikre områder mot inntrenging og eller anslag fra uautorisert personell og kjøretøy. Dette være seg anslag mot perimetersikringer, eller aksjoner inne på områder etter inntrenging via perimetersikringer. Samtidig har jeg lenge vært interessert i perimetersikring av store

industriområder i Norge, hva som foregår der og hvordan man kan klare å sikre så store områder på en tilfredsstillende måte. Et lite søk i media gir meg følgende oppslag:

«Innbrudd på industriområde. En port er brutt opp på industriområdet på Opofta i Kvinesdal. Tatt kompressor og noe verktøy.» (Bakka, 2020)

«En mann klippet seg inn på industriområdet. Tatt på fersk gjerning med ca 70 kilo kobber» (Johansen, 2020)

«Industribedriftene på Øra har sett seg kraftig lei på de mange innbruddene på området. I løpet av en 14-dagersperiode ble det loggført hele elleve innbrudd.» (Bolstad, 2014)

«Et titalls ungdommer har lenket seg fast, med mål om å stanse det omstridte gruveprosjektet ved Førdefjorden. Demonstrantene er forberedt på bøter. Sammen med ti andre er hun på plass ved Engebøfjellet, der de tok seg inn på anleggsområdet og lenket seg fast for å protestere mot prosjektet.» (Endal, 2022)

Disse oppslagene viser at man i Norge har tilfeller av inntrenging gjennom perimetersikringer rundt industriområder. Det viser at man har uønskede hendelser knyttet til slike inntrenginger. Med bakgrunn i dette ønsket jeg å se på kvaliteten på slik perimetersikring. Når sjansen bød seg for å skrive masteroppgaven knyttet til et stort industriområde i Norge, så jeg muligheten til å undersøke kvaliteten på dette grundig. For å anonymisere dette industriområdet, vil det videre i studien kalles Industriområdet. Det kom tidlig frem i møter med representanter for Industriområdet at denne typen oppgaver, med dette temaet, var noe de ønsket seg og prioriterte å legge til rette for. Dette gjorde tilnærmingen til planleggingen av oppgaven enklere, da jeg hadde døråpnere inn til området, tilgang til data om perimetersikringen, en oversikt over Industriområdet, dets utstrekning og hvilke aktører som er plassert der.

1.2 Tema for oppgaven, perimetersikring og tidligere forskning på dette

Ytre perimetersikring er et begrep knyttet til security. Hvordan skjerme seg mot villede uønskede handlinger gjennom å etablere en ytre sikring. Engen et al. (2016, kap. 2) sier at historisk har dette blitt gjort med vollgraver rundt borger, murer rundt byer og kanskje den mest kjente av alle, den Kinesiske mur, for å holde fiender unna. Man skulle tro at et slikt fagfelt var godt belyst i tidligere forskning. Jeg regnet dermed med at søk via søkemotorer på Internett ville gi meg eksempler fra tidligere forskning rundt tema for denne studien. Etter søk på flere søkemotorer kom jeg frem til flere funn knyttet til tidligere forskning og utgivelser. Et

utdrag fra disse funnene følger her: Toward a North American Security Perimeter? Assessing the trade, FDI, and welfare impacts of liberalizing 9/11 security measures (Georges & Merette, 2012); The impact of strategic planning on institutional integration toward patrimonial and perimeter security planning of the 2016 Olympic games (Cunha, Marcineiro, Forcellini, & (...), 2018); *Securing the Security System* (Al-Fedaghi, 2017); *Virtual perimeter security (VPS) in a physical protection system* (Norman & Adams, 2007); Evolution of a Hybrid Model for an Effective Perimeter Security Device (Vasudevan & Selvakumar, 2015); Criminal profiling and industrial security (Lee C. , 2015); A Meta-Analysis of Industrial Security Research for Sustainable Organizational Growth (Yu & Chang, 2020); Shaping a Novel Security Approach in chemical Industrial Clusters to Prevent Large-Scale Domino Events (Reniers, Dullaert, & Soudan, 2009); *Risk assessment method of power plant industrial control information security based on Bayesian attack graph Systems* (Xie, Sun, & Lei, 2021); Ranking chemical industrial clusters with respect to safety and security using analytic network process (Casciano, Khakzad, (...), & Cozzani, 2019); A Security-Aware Framework for Designing Industrial Engineering Processes (Dedousis, Stergiopoulos, (...), & Gritzalis, 2021); *Terrorism security in the chemical industry: Results of a qualitative investigation* (Reniers G. , 2011); Securing SCADA and critical industrial systems: From needs to security mechanisms (Kalam, 2021); Management of Schemes and Threat Prevention in ICS Partner Companies Security (Lee & Huh, 2021); An advanced approach to security measurement system (You, Cho, & Lee, 2016); *Security vulnerability assessment in the chemical industry* (Dunbobbin, Medovich, & Murphy, 2004); *A study on the performance assessment of anti-terrorism physical protection systems in chemical plants* (Argenti, Landucci, Cizzani, & Reniers, 2017); Urbanisation control around industrial Seveso sites: the French context (Merad, Rodrigues, & Salvi, 2008); New methodologies for security risk assessment of oil and gas industry (Srivastava & Gupta, 2010); Evaluation of Various Perimeter Barrier Products (Bhattarai, Zhang, & Wood, 2021); *A systems level approach to perimeter protection* (Tu, Yu, Nevatia, Gao, & Lee, 2012); *Vurdering av konsekvenser ved etablering av ytre perimeter rundt nytt regjeringskvartal* (Jore, Kruke, & Olsen, 2020); Fysisk terrorsikring i byens uterom: en studie av fysiske terrorsikringstiltak og hvordan slike kan integreres i byens uterom, hvor Oslo Rådhus brukes som arena for å teste ut, og diskutere ulike tilnærminger (Bakke, 2015).

Som man ser av disse funnene er det mindre forskning på sikring av industriområder i Norge. Denne oppgaven kommer til å ha fokus på og ta for seg nettopp det. Selv om ikke alle

funnene over er direkte knyttet til min problemstilling, gir de inspirasjon til videre jobbing med denne studien.

Et søk på «Perimetersikring» på Brage UiS ga fire treff. Ingen av dem med utgangspunkt i perimetersikring av industriområder. «Sikring av industriområder» ga 85 treff og «Sikring av industri» ga meg 1447, da var begrepet sikring ikke lenger spisset nok og veldig mange av treffene ikke relevante for min problemstilling. Likevel fant jeg oppgaver som belyser mitt tema, selv om de ikke er spisset mot perimetersikring av industriområder. Barrierer for beskyttelsen av sensitiv informasjon (Kruke, 2017), rollefordeling og ansvar knyttet til håndtering av uønskede hendelser i industriområdet (Miøen, 2016), utviklingen av barrierestyring mot tilsiktede uønskede hendelser (Sørensen, 2018), samvirke mellom industrivernet og lokale beredskapsaktører (Mustaparta, 2016) analysemetodikk når det gjelder ikke-intenderte uønskede hendelser (Egeli, 2014). Disse oppgavene viser at barrierer og hendelser har vært studert flere ganger. Imidlertid viser treffene også mangelfull forskning rundt både perimetersikring av industriområder og brudd på perimetersikringene. På denne måten er temaet for denne oppgaven aktuelt og eksplorativt.

1.3 Formålet med studien

Fra min profesjonelle hverdag, som fengselsbetjent, er jeg vant til at en perimetersikring er tett, det skal ikke være huller hverken i mur eller gjerde rundt fengsler. Samtidig er jeg vant til at en perimetersikring er et «totalforsvar», en sikring med mange elementer som overlapper hverandre. Dette er barrierer i sikringen som gjør at man får varsler og kan gjøre tiltak dersom man blir truet og man oppdager anslag eller angrep så tidlig at man klarer å få varslet og gjort tiltak. I denne studien ønsket jeg å forske på hva påliteligheten til perimetersikringen betyr for et industriområde. Jeg har valgt å samle inn data i et stort industriområde i Norge. Oppgavens egenart gjør at navnet på industriområdet anonymiseres. Er det slik at sikring og security har sin plass inne på Industriområdet, eller er man kun opptatt av safety-hendelser og ulykker og hendelser knyttet til produksjonen.

Denne studien kom i stand ved at det ble knyttet kontakt mellom representanter for industriområdet og meg. Gjennom felles møter rundt tema for oppgaven ble vi enige om at formålet med denne studien var å forske på/studere påliteligheten til Industriområdets perimetersikring. Dette skulle gjøres gjennom observasjoner av nåværende perimetersikring, samt observasjoner og intervjuer med relevante medarbeidere som arbeidet med perimetersikring og operasjonaliseringen av denne, samt se dette opp mot relevant teori og

forskning rundt temaet. Jeg skulle forske på/studere påliteligheten til perimetersikringen for å vurdere om denne er hensiktsmessig og tilstrekkelig i forhold til Industriområdet, de verdiene som skal vernes og leietakernes krav til perimetersikring.

Jeg forsket på/studerte dette gjennom å analysere dagens perimetersikring og tilhørende barrierer og stille spørsmål rundt disse. Er det samsvar mellom kravet til perimetersikringen og dens faktiske ytelse? Er barrierene, drift, vedlikehold og dimensjonering av perimetersikringen i tråd med de verdier man ønsker å beskytte og således hensiktsmessig og tilstrekkelig som perimetersikring? Har Industriområdet en realistisk vurdering av hva som er tilstrekkelig og hensiktsmessig perimetersikring i forhold til de krav som er satt til drift og dimensjonering av perimetersikringen?

For å svare ut disse spørsmålene og komme med en belysing av temaet som også imøtekommer Industriområdets ønsker er oppgaven bygget rundt følgende hovedproblemstilling:

«Hvordan er påliteligheten til perimetersikringen rundt Industriområdet?»

For å belyse studiens problemstilling mer utfyllende har jeg kommet frem til følgende tre forskningsspørsmål:

- 1. Hva slags barrierer etableres for å ivareta perimetersikringen?**
- 2. Hvordan er informasjonsflyten blant samvirkerne som opprettholder barrierene?**
- 3. Hva truer påliteligheten til dagens perimetersikring?**

1.4 Studiens avgrensing

For å kunne studere påliteligheten til perimetersikringen må man analysere hva som ligger i perimetersikringen. Hvordan er den dimensjonert, hvilke krav ligger til den, hvilke barrierer ligger implementert i den og hvordan operasjonaliseres, driftes og vedlikeholdes den? Hvilke vurderinger ligger bak beslutningene som er tatt? En god perimetersikring er en helhetlig sikring av et område, hvor barrierer, dimensjonering, krav, operasjonalisering, drift og vedlikehold alle er brikker som jobber sammen mot et felles mål om å sikre området innenfor perimetersikringen mot uønsket inntrenging og med det hindre uønskede hendelser.

Studien er avgrenset til å gjelde perimetersikringen på land. Industriområdet har også store kaianlegg, men disse ligger ikke inne i denne studien. Det vil ikke være mulig å svare på en

problemstilling som tok for seg både land- og kaiområdene innenfor de rammer som ligger til grunn for denne oppgaven. Bakgrunnen for valget av perimetersikringen på land, er at Industriområdet ikke har hatt samme fokus på risikovurdering av denne som de har hatt på kaiområdene. Sjø- og kaiområdene er regulert under ISPS¹-regelverket og derav vurdert av sjøfartsmyndighetene og Sjøfartstilsynet. Industriområdet mente derfor innledningsvis at dette, gjennom disse regelverkene, var tilstrekkelig belyst i forhold til perimetersikring. Oppgaven vil ikke ta for seg eller beskrive trusselaktører i noen større grad, men holde seg til å beskrive sikringstiltakene og barrierene som ligger i perimetersikringen. Det vil si at studien er knyttet til security-aspektet ved sikkerhet og ikke andre aspekter ved sikkerhet, som for eksempel ulykker og naturødeleggelser. Oppgaven har fokus på sikringen av Industriområdet mot uautorisert adgang gjennom å fokusere på perimetersikringen og dens dimensjonering og ytelse.

1.5 Oppgavens oppbygging

Oppgaven vil videre bygges opp ved å ta leseren gjennom kapitlene to til seks. Kapitlene to og tre viser relevant teori fra sikkerhet og metode. Kapitlene fire og fem er bygd opp med lik struktur, slik at det skal være enkelt for leseren å se funnene i disse opp imot hverandre. Følgende er en kort beskrivelse av innholdet i de forskjellige kapitlene.

Kapittel to, vil være en redegjørelse av relevant teori knyttet til studiens problemstilling og dens forskningsspørsmål. Hvor man har forsøkt å velge ut teori som beskriver perimetersikringer og hva som pekes på som avgjørende for å bygge fungerende perimetersikringer med relevante barrierer.

Kapittel tre, vil være en gjennomgang av studiens metoder. Hvilke metoder er brukt for å belyse og besvare studiens problemstilling og forskningsspørsmål. I dette kapitlet er det også belyst relevant metodeteori for å understreke de valg som er tatt i forhold til studiens metoder.

Kapittel fire, viser studiens empiri. Kapitlet er delt inn med studiens forskningsspørsmål som overskrifter, slik at det skal være enkelt for leseren å følge de funn som blir lagt frem fra dokumenter, intervjuer, observasjoner og samtaler. Hva som kommer frem fra de forskjellige settingene er igjen delt inn i underkapitler under hvert forskningsspørsmål. Samtidig vil

¹ ISPS; International Ship and Port Facility Security. Dette er et regelverk for havner som tar imot noen definerte typer skip. Disse havnene styres av ISPS-koden, som er et eget regelverk for denne typen havner. I Norge er denne ISPS-koden forankret i Forskrift om sikring av havneanlegg (Samferdselsdepartementet, 2013).

leseren kunne se eventuelle avvik av informasjon som kommer frem fra de forskjellige settingene i studien. Eller viser det seg at det er samsvar med den informasjonen som blir gitt fra de forskjellige informantene.

Kapittel fem, er studiens drøftingskapittel. Her vil funn fra teori og empiri drøftes opp imot hverandre. Dette kapitlet vil også deles inn med de forskjellige forskningsspørsmålene som overskrifter, slik at det skal være enkelt for leseren å følge drøftingen og det som kommer frem i denne.

Kapittel seks, vil være en konklusjon av studien og dens funn. Her vil det kort konkluderes, basert på drøftingskapitlet, rundt studiens problemstilling.

2. Teori

I dette kapitlet vil det bli lagt frem teori som er med på å belyse studiens problemstilling og forskningsspørsmål. Grunnlaget for at denne teorien er hentet inn og belyst er dens nærhet til studien og dens problemstilling. Teoriene som benyttes er blant annet hentet fra Reason (2016), Haddon (1980), Aven et al. (2017), Stranden (2019) og Sklet (2006). Kapitlet er bygget opp slik at man får en innføring i begrepene safety og security, for å se studiens fokus knyttet til security begrepet. Videre vil begrepet risiko belyses, slik at begrepet settes i sammenheng med oppbygging og planlegging av perimetersikringer. Begrepene trusler, trusselscenarioer og trusselaktører vil bli belyst for å vise hva som kan være truslene mot perimetersikringen og hva denne da må dimensjoneres for. Videre vil det bli vist til teori rundt sikring, barrierer, tiltak og sikkerhetskultur, noe som også vil knyttes til hvordan bygge perimetersikringer og hva som kan gjøre en perimetersikring pålitelig.

Teoriene vil være med på å belyse problemstillingen:

«Hvordan er påliteligheten til perimetersikringen rundt Industriområdet?»

For å belyse problemstillingen ytterligere, knyttes følgende tre forskningsspørsmål til studien:

- 1. «Hva slags barrierer etableres for å ivareta perimetersikringen?»***
- 2. «Hvordan er informasjonsflyten blant samvirkerne som opprettholder barrierene?»***
- 3. «Hva truer påliteligheten til dagens perimetersikring?»***

Industriområdet bygger sin perimetersikkerhet rundt planverk, tekniske installasjoner og menneskelig kontroll. For å begrense studien vil det være nødvendig å gjøre et utvalg av teoretiske perspektiver, som spesifikt belyser problemstillingen og forskningsspørsmålene. Innledende vil det defineres teoretisk rundt safety og security, for å vise begrensingen i teoriperspektivene videre i studien. Studien vil inneholde flere teoretiske perspektiver, valgt ut for å belyse studiens problemstilling. Det vil bli tatt inn teoriperspektiver rundt barrierer, sikkerhetskultur, beredskap, beredskapskultur, risiko og risikovurderinger.

2.1 Safety og security

«I Skandinavia har det oppstått en forståelse av at safety handler om ulykker, mens security handler om ondsinnede handlinger som krig eller terrorisme ...» (Engen, et al., 2019, s. 26). Man deler her sikkerhetsbegrepet inn i to deler og knytter en del til ulykker og en til

ondsinnede handlinger. Videre sier Aven et al. (2017) at *safety* kan, innenfor samfunnssikkerhet, forstås som sikkerhet som tilstand og sikkerhet som følelse. Ordet *security* forstås som fysisk sikkerhet og faktisk tilstand mer enn følelsen. «Safety er sivil sikkerhetstenking og *security* er tenking omkring sikring mot vilde handlinger» (Njå, Sommer, Rake, & Braut, 2020, s. 23). Njå et al. (2020) tar her inn ordet tenking i sine definisjoner rundt begrepene. Hvilket begrep man bruker blir knyttet til tanken rundt den sikkerhetsutfordringen man står overfor.

«Security betyr å sikre seg mot tilsiktede uønskede handlinger, mens *safety* betyr å beskytte seg mot uhell eller andre tilfeldige uønskede hendelser» (Stranden, 2019, s. 32). Stranden (2019) sier videre at begrepene kan by på utfordringer, da man ikke har tilstrekkelig presise norske ord for de to begrepene, noe som kan føre til misforståelser og feil bruk av begrepene i forskjellige situasjoner. Stranden mener dette i kritiske situasjoner kan få uønskede utfall.

Aven et al. (2017) snakker om forståelse, Stranden (2019) peker på at uklarheter i begrepene kan gi utfordringer i bruk og Njå et al. (2020) tar frem tankeprosessen rundt bruken av begrepene. Det man ser er at de tre perspektivene peker på at begrepet *Security*, omhandler hendelser som er vilde og tilsiktet.

Videre i denne studien vil det derfor være begrepet *security*, siden det omhandler tilsiktede uønskede handlinger, som vil være førende for resten av de teoriperspektivene som belyses.

2.2 Risiko

Aven og Renn (2009) diskuterer risikobegrepet og lister opp ti forskjellige definisjoner av begrepet, hentet fra andre teoretikere på området. I sin artikkel diskuterer de to av disse definisjonene, ni og ti, og ut ifra dette kommer de med sin egen definisjon av begrepet.

«Risiko refererer til usikkerhet om og alvorlighetsgraden av konsekvensene (eller resultatene) av en aktivitet med hensyn til noe som mennesker verdsetter» (Aven & Renn, On risk defined as an event where the outcome is uncertain, 2009, s. 6). Denne definisjonen blir sett på som Aven og Renn sin klassiske definisjon av risikobegrepet.

«Risiko handler om hendelser (A), og konsekvenser(C) av disse, som kan skje i fremtiden» (Aven, Røed, & Wiencke, Risikoanalyse, 2017, s. 29). Videre sier Aven et al. (2017) det er knyttet usikkerhet til både hendelsene og konsekvensene. Mens Aven et al. (2017) knytter risiko til hendelser og konsekvenser, knytter Stranden (2019) også begrepene trussel, verdi og sårbarhet til definisjonen i sin bok.

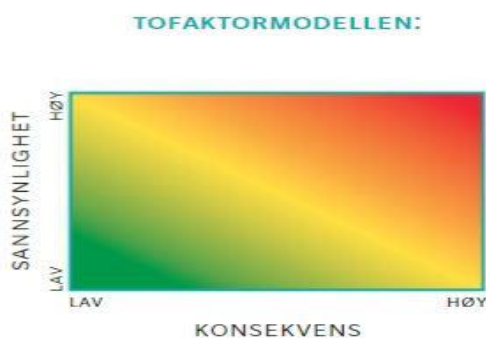
Stranden (2019) viser til Norsk standard (NS 5830:2012) når han definerer risiko på følgende måte: «uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen» (Stranden, 2019, s. 53). Lunde (2019) peker på enda et moment når han skriver inn usikkerhet i sine forståelser av risiko.

Lunde (2019) sier at risiko kan forstås på to måter: «kombinasjon av konsekvensene av aktiviteten og tilhørende usikkerhet» eller, «usikkerhet om og alvorligheten av konsekvensene av aktiviteten» (Lunde, 2019, s. 27).

Hvis man sammenfatter de tre siste definisjonene av risiko, ser man begrepene usikkerhet, konsekvens, hendelse, aktivitet og sårbarhet, alle brukes for å forklare begrepet risiko fra forskjellige ståsted. Aven et al. (2017) og Lunde (2019) bruker begge aktivt usikkerhetsbegrepet, mens Stranden (2019) bruker begrepet sårbarhet. Risikobegrepet og definisjonen av dette, vil i denne studien brukes for å avdekke trusler mot og sårbarhet i perimetersikringen rundt Industriområdet, gjennom risikovurderinger og risikoanalyser.

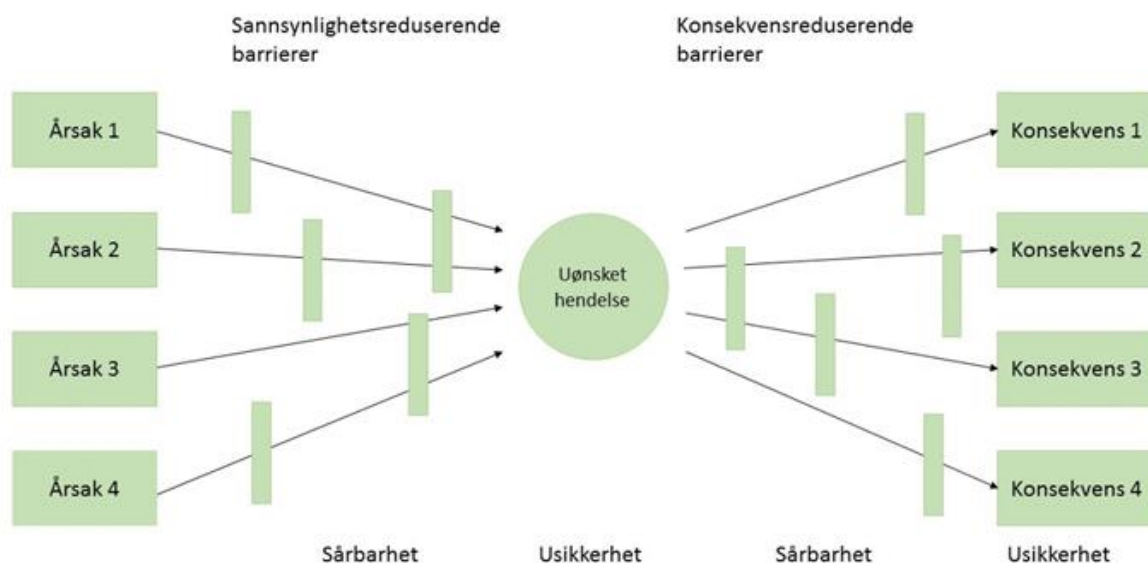
2.2.1 Risikovurderinger og risikoanalyser

Ser man risikovurderinger i et tradisjonelt lys, ved å anvende sårbarhet og konsekvens som måleparametre, gjennomfører vi risikovurderingen i en såkalt tofaktor modell. Modellen viser risiko ved å plassere kryss i matrisen basert på formelen. Risiko = Sårbarhet x Konsekvens. Lav sårbarhet x lav konsekvens = lav risiko grønn sone. Høy sårbarhet x høy konsekvens = høy risiko rød sone. Man vil i denne modellen få spredt ulike aktiviteter utover i matrisen basert på utgangsverdiene til aktivitetene i forhold til sårbarhet og konsekvens



Figur 1: Matrise, tofaktormodellen (Sommer, Pollestad & Steinnes, 2020, s.23)

En annen modell, basert på tofaktormodellen, er Bow-Tie modellen også kalt sløyfediagram.



Figur 2: Bow-Tie https://www.dsb.no/globalassets/bilder/brann-og-eksplosjonsvern/temaveileder-kap-4-forskrift-om-brannforebygging/temaveil_kap4_brannforebygging_fig10.jpg

Stranden (2019) beskriver at sløyfediagrammet er egnet til å analysere enkelthendelser, og bruker modellen videre til å utforske hendelsen med tilhørende årsaker, konsekvenser og barrierer. Lunde (2019) har en annen betegnelse for sløyfediagrammet. Han kaller det «risikobilde for en identifisert uønsket hendelse».

Lunde (2019) og Stranden (2019) forklarer modellene likt. Ved å legge identifiserte årsaker til den uønskede hendelsen lengst ut til venstre, konsekvensene lengst ut til høyre og barrierene i mellomrommet på hver side. En forskjell i beskrivelsene, er Lundes (2019) presisering av barrierene. Han skriver: «Mellom den uønskede hendelsen og konsekvensene blir tiltak som er egnet til å forebygge eller redusere konsekvensene av den uønskede hendelsen identifisert.» (Lunde, 2019, s. 30). Lunde viser her altså til viktigheten av egnetheten av barrierene man setter inn. At barrierene faktisk er i stand til å forebygge årsakene de er satt inn for å forebygge og/eller redusere konsekvensene de er satt inn for å redusere.

«Det er viktig å velge en tilnærming for risikovurdering som passer virksomheten og formålet» (Nasjonalsikkerhetsmyndighet, 2016, s. 4). Videre skriver NSM «I risikovurderinger med fokus på *tilsiktete uønskede handlinger*, er det ofte mer nyttig å beskrive risiko som en funksjon av verdi, trussel og sårbarhet». I 2017 skriver NSM om Risikotrekanten i sin rapport «Risiko 2017». «De grunnleggende sammenhengene mellom

verdier, trusler og sårbarheter er illustrert i modellen nedenfor. NSM bruker begrepene verdi, trussel og sårbarhet i sine risikovurderinger. Risiko defineres som forholdet mellom disse tre faktorene» (Nasjonal sikkerhetsmyndighet, 2017, s. 7).



Figur 3: Trefaktormodellen (Sommer, Pollestad & Steinnes, 2020, s. 23)

Sommer et al. (2020) bruker også denne modellen og sier at ved å ha klart for seg hvilke verdier man skal sikre, kan man sette disse opp mot truslene mot verdien og sårbarheten til verdien eller barrierene som beskytter den. Ved å kartlegge de tre faktorene vil man kunne iverksette tiltak, dersom man ser at verdier er for svakt sikret i forhold til den trusselen verdien står overfor.

NSM (2016) skriver at det alltid vil være knyttet usikkerhet til risikovurderinger og analyse. Videre sier man: «Det er viktig å forstå usikkerheten knyttet til risikovurderingen, slik at det blir troverdig beslutningsgrunnlag.» (Nasjonalsikkerhetsmyndighet, 2016, s. 5).

Usikkerhetsbegrepet blir her igjen belyst på lik linje som det blir over, i avsnittet om risiko. «Det kan også være riktig å gjøre vurderingen i flere trinn, ved at man først gjør en overordnet vurdering, og deretter går i dybden der det fremkommer behov for å gjøre det» (Nasjonal sikkerhetsmyndighet, 2016, s. 5). Dette fører oss til et risikovurderingsverktøy som også brukes ved Industriområdet, Risiko og Sårbarhetsanalyse (ROS).

«Risiko- og sårbarhetsanalyser omfatter en systematisk identifisering og kategorisering av risiko, og skal være til hjelp for å kartlegge behovet for sikkerhetsstyring» (Aven, Boyesen, Njå, Olsen, & Sandve, 2019, s. 31). Dette er et verktøy som bruker både tofaktor- og trefaktormodeller for å gi et helhetlig bilde av risiko og sikkerhet i en organisasjon.

Innholdet i analysen beskrives på følgende måte: «a. Kartlegging av uønskede hendelser, b. Årsaker og sannsynlighet, c. Konsekvenser, d. Systematisering. Risikobeskrivelse, e. Forslag

til tiltak» (Aven, Boyesen, Njå, Olsen, & Sandve, 2019, ss. 99-100). Analysen jobbes frem gjennom bruk av tabeller, matriser og modeller, som for eksempel sløyfediagram.

Disse analysene vil være et hjelpemiddel til å identifisere risiko og sårbarheter i organisasjoner, og gjennom det, si noe om hva risiko- eller, som Lunde (2019) viste til, trusselbildet for virksomheten er. Ved å bruke disse kategoriene og legge til grunn risikovurderinger gjort i virksomheten, kan dette legge til rette for å gjøre trusselvurderinger.

Når vurderingene er tatt, må man se på hva i vår organisasjon som kan trues. Hvilke verdier ønsker vi å verne om.

2.3 Verdier

For å kunne dimensjonere perimetersikringen riktig må man se på hvilke verdier man skal skjerme. Hvilke verdier ønsker vi å beskytte og hvordan kan man best beskytte dem? Stranden (2019) deler verdier inn i to hovedgrupper; materielle og immaterielle. «Materielle verdier er gjenstander, personer, data, infrastruktur, penger og markedsandeler. Immaterielle verdier er informasjon, operativ evne, funksjon, tillit, omdømme, frihet og goodwill.» (Stranden, 2019, s. 116). En perimetersikring vil, fysisk, kunne verne de materielle verdiene og holde verdier, gjenstander osv. trygge. Samtidig vil en god perimetersikring som verner om disse materielle verdiene, gjennom det, også verne de immaterielle verdiene. En synergieffekt av å verne materielle verdier vil for eksempel kunne være et godt omdømme. Eller at man ved å verne om personer, data og infrastruktur, også vil verne om organisasjonens operative evne og funksjon.

Når man har fastsatt og definert organisasjonens verdier, må man se på hva som truer disse verdiene. Det å identifisere truslene, vil være et viktig verktøy for å kunne dimensjonere perimetersikringen riktig.

2.4 Trusler

For å kunne si noe om hva perimetersikringen bør dimensjoneres for og hva påliteligheten i perimetersikringen skal være, må man se på hvilke trusler som perimetersikringen og dens pålitelighet kan stå overfor. Hva og hvem er det som truer perimetersikringen? Jeg vil i det følgende gå inn på trusselbegrepet og komponenter i dette for å belyse hva perimetersikringen og dens pålitelighet bør dimensjoneres for.

Stranden (2019) sier trusler og farer kan deles i to forskjellige grupper. Men sier også at de sett i sammenheng med uønskede tilsiktede handlinger, ofte blir sett under ett. «Med trusler

menes personer eller grupper av personer som vil og kan påvirke noens verdier negativt. Med farer menes fenomener som kan skade noens verdier.» (Stranden, 2019, s. 67).

NSM deler dette videre inn i trusselkategorier.

2.4.1 Trusselkategorier

Enhver industri bør sette seg inn i hva som kan være en trussel for deres virksomhet og gjennomføre risikovurderinger som sier noe om de truslene de mener er relevante for sin virksomhet. Basert på gjennomførte risikovurderinger kan man så se på hvilke trusler virksomheten kan utsettes for. NSM (2016) deler inn i tre trusselkategorier og definerer disse på følgende måte.

«**Spionasje**, målrettet informasjonstyveri ved bruk av fordekte metoder. Tyveriet kan skje ved fysisk eller menneskebasert innhenting, ved å utnytte IKT-systemer, eller en kombinasjon av disse.

Sabotasje, målrettet skade på store datamengder eller infrastruktur, herunder lokaler og informasjonssystemer. Sabotasje rammer tilgjengelighet og integritet til informasjon og infrastruktur.

Terrorhandlinger, omfatter å sette menneskers liv eller helse i fare, ødeleggelse av eller alvorlig skade på eiendom, å forstyrre prosesser eller systemer som opprettholder et demokratisk styre eller samfunnets økonomiske velferd og virkemåte.»

(Nasjonalsikkerhetsmyndighet, 2016, s. 14)

NSM viser i sin håndbok til sikkerhetslovens kapittel 3 for ytterligere definisjon av begrepene.

Sett i lys av disse gruppene og kategoriene, snakker vi om trusselaktører.

2.4.2 Trusselaktører

Hvem er en trussel for hvilken virksomhet? Hva er det som gjør virksomheten interessant og hvem er den interessant for. NSM (2022) bruker i sin rapport «Risiko 22» begrepene sivilt og militært. Er virksomheten med sin produksjon interessant for både sivile og militære aktører? Når man har kartlagt dette, kan man si man har dannet seg et trusselbilde.

«Usikkerheten knyttet til om en tilsiktet handling vil skje eller ikke, beskrives som identifiserte trusselaktører sin *intensjon* om og *kapasitet* til å ramme virksomheten» (Lunde,

2019, s. 36). Trusselaktører er aktører man mener kan gjennomføre de truslene man har definert i sitt trusselbilde. Aktører som gjennomfører vilde tilsiktede uønskede handlinger.

Stranden (2019) kommer med følgende eksempler på trusselaktører; nasjonalstater, internasjonale aktører, regionale aktører, lokale individer, innsidere og nære relasjoner. Alle i stand til å gjennomføre truslene som er vurdert gjennom definisjonen av trusselbildet, som omtalt tidligere i oppgaven.

«Tilstedeværelse – er det noen som kan utføre trusselen på virksomheten, systemet eller den samfunnskritiske funksjonen vi studerer?, Kapasitet – er de som ønsker å utføre trusselen i stand til å gjøre det?, Intensjon – har de som er vurdert, vilje til å utføre trusselen?» (Njå, Sommer, Rake, & Braut, 2020, s. 258). Lunde (2019) sier noe om intensjon og kapasitet.

Stranden (2019) tar dette to steg videre og nevner historie og forestående angrep som intensjoner. I tillegg tar Stranden med seg begrepet attraktivitet. Og stiller spørsmålet om målet/virksomheten er attraktivt nok for den trusselaktøren vi har vurdert er en trussel.

Etter å ha kartlagt trusselkategorier og trusselaktører går man videre til å se på trusselscenarioer.

2.4.3 Trusselnivå og trusselscenarioer

Ved fastsettelse av dette brukes standardiserte sannsynlighetsord. «Meget sannsynlig: det er meget god grunn til å forvente; Sannsynlig: Det er grunn til å forvente; Mulig: Det er like sannsynlig som usannsynlig; Lite sannsynlig: Det er liten grunn til å forvente; Svært lite sannsynlig: Det er svært liten grunn til å forvente.» (Njå, Sommer, Rake, & Braut, 2020, s. 260).

Stranden (2019) velger å bruke denne tabellen på side 122 i sin bok. Tabellen er en modifisert utgave av Department of the Army (2001) threat levels. Tabellen er en gjengivelse av modellen i Strandens bok.

| Rangering | Beskrivelse |
|---|--|
| Nivå 4 Svært høy | Indikatorene a, b, c og e eller a, b, d og e er til stede. |
| Nivå 3 Høy | Indikatorene a, b, c og d er til stede. |
| Nivå 2 Moderat | Indikatorene a og b er til stede. |
| Nivå 1 Lav | Indikatorene a eller b er til stede |
| Beskrivelse av indikatorer | |
| <p>A) Tilstedeværelse: Aktøren er til stede, antas å være til stede eller kan forflytte seg til området eller regionen, eller kan på annen måte nå verdiene.</p> <p>B) Kapasitet: Tilegnet, antatt eller demonstrert evne til å utføre handlingene som kan ramme virksomhetens verdier.</p> <p>C) Intensjon: Det eksisterer, eller det kan antas at det eksisterer, en vilje og/eller ønske til handling om å rammevirksomhetens verdier.</p> <p>D) Historie: Det eksisterer påviselig aktivitet over tid.</p> <p>E) Forestående angrep: Det eksisterer ny og pålitelig informasjon som indikerer forberedelsen av et nær forestående angrep.</p> | |

Figur 4: Tabell trusselvurdering (Stranden, 2019, s. 122)

NSM, velger å sette intensjon og kapasitet inn i egne matriser, med forskjellige nivåer av klassifisering, fra A til D.

Man må bruke disse risiko- og trusselvurderingene sammen med trusselkategoriene, trusselaktørene og de forskjellige indikatorene. For så å sette dette inn i det analyseverktøyet man velger å bruke for å fastsette trusselnivået eller trusselscenarioet for sin virksomhet.

Hva man kommer frem til i dette arbeidet vil sette målene for hvilken sikring virksomheten skal ha.

2.5 Sikring

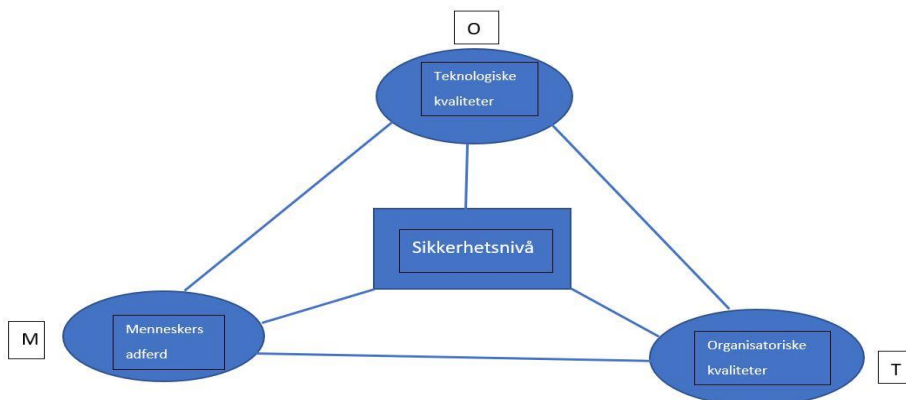
I denne studien vil sikringen bli sett i lys av tre komponenter. Menneske – Teknologi – Organisasjon. Stranden (2019) viser oss dette i en modell kalt sikringstrekløveret, hvor de tre delene er satt inn i en modell. Under vises en gjengivelse av modellen laget til denne studien



Figur 5: Gjengivelse av modellen Sikringstrekløveret - 1 (Stranden, 2019, s. 125)

Som man ser i modellen, er de tre hovedelementene igjen delt inn i flere underkategorier. Disse underkategoriene vil bli nevnt videre i oppgaven.

Antonsen et al. (2017) viser en enklere MTO modell, men de velger å synliggjøre hvordan de tenker sikkerhetsnivå inn i modellen. Vises her ved en gjenskaping av modellen laget til denne studien:



Figur 6: Gjengivelse av modellen Sikringstrekløveret - 2 (Antonsen, Heldal & Kvalheim, 2017, s. 283)

I denne modellen ser man to andre begreper knyttet til modellen og kategoriene. Her er begrepet kvaliteter, knyttet til det Organisatoriske og Teknologiske, mens atferd er knyttet til mennesker. «En måte å sammenstille perspektivene fra epokene på, er å si at sikkerhet dreier seg om et samspill mellom teknologiske, menneskelige og organisatoriske forhold.»

(Antonsen, Heldal, & Kvalheim, 2017, s. 282)

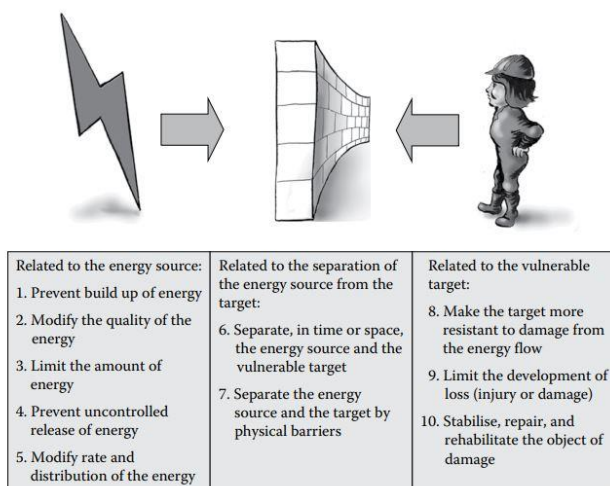
Sikring mot trusler eller villedte tilsiktede uønskede handlinger, kan refereres til som barrierer. Man setter inn sikringer eller barrierer mot at noe skal kunne skje.

2.5.1 Barrierer og tiltak

«Barrierer har blitt brukt til å beskytte mennesker og eiendom fra fiender og naturlige farer, siden opprinnelsen av mennesker» (Sklet, 2006, s. 494) Barrierer kan ha mange ulike utforminger og tiltenkte funksjoner. «Barriere: Tiltak som reduserer sannsynligheten for å utløse en fares potensial for skade, eller reduserer skadepotensialet.» (Johnsen, 2019, s. 158) Oxford English Dictionary (OED 2005) definerer ordet barriere slik: «Fence of material obstruction of any kind erected (or serving) to bar the advance of persons or things, or to prevent access to a place». Sklet (2006) sier: «Safety barriers are physical and/or non-physical means planned to prevent, control or mitigate undesired events or accidents. » (Sklet, 2006, s. 496). Reason (2016) deler videre barrierer inn i to hoveddeler. Den første er Harde, som i tekniske installasjoner, alarmer, gjerder, låser nøkler osv. Den andre er myke, som en kombinasjon mellom papirer og mennesker.

Barrierer kan være alt fra brannmurer i datasystemer, forsterkede betongvegger som beskyttelse mot trykk ved eksplosjoner, til gjerder, porter, roadblockere og kameraovervåking i en helhetlig perimetersikring. Perimetersikringer settes opp for å holde uvedkommende borte fra det området perimetersikringen sikrer. For at denne sikringen skal være pålitelig er det viktig at det ligger barrierer i denne. «Med pålitelighet til en enhet forstås dens evne til å utføre en tiltenkt funksjon. I en driftssituasjon måles denne evnen ved å se på om barrieren virker eller ikke virker ved behov eller ved tester. Det relative antall ganger barrieren virker, gir et uttrykk for den observerte eller målte pålitelighet.» (Aven, Boyesen, Njå, Olsen, & Sandve, 2019, s. 122) Barrierer er hindringer som, satt i system, er med på at perimetersikringen klarer å holde uvedkommende ute av området. Barrierene og barrieresystemet skal gjøre at perimetersikringen blir en helhet og samspillet mellom de forskjellige barrierene skal være med på å detektere og hindre forsøk på inntrenging på det området som perimetersikringen skal beskytte. Dette kan være barrierer på forskjellige nivå og med forskjellig utforming. Barrierene kan også være rettet mot enkelt deler av perimetersikringen og kan være rettet mot forskjellige trusler mot perimetersikringen. «A barrier system may consist of several barrier elements, and the elements may be of different types (e.g., technical, operational, human, and software). » (Sklet, 2006, s. 496).

Et perspektiv som er aktuelt i forhold til barrierer og tiltak er energi og barriereperspektivet. Kjellén og Albrechtsen (2017) viser til Haddons 10 strategier for forebygging av ulykker.



Figur 7: Haddon's 10 accident prevention strategies. (Adapted from Haddon, W., *Hazard Prev.*, 16, 8-12, 1980) (Kjellen & Albrechtsen, 2017, s. 25)

Haddons strategier er også anvendbare knyttet til ytre perimetersikring. Modellen er delt inn i tre hoveddeler; energikilden, adskillelse av energikilden fra målet og det utsatte målet.

Del en, med de første fem strategiene, omhandler energikilden og beskriver begrensingen av energikilden og hvordan begrense denne. I tillegg til å forsøke å påvirke hvordan energien skal spre seg og om dette er mulig å styre.

Del to, med strategi seks og syv, omhandler hvordan man kan skille energikilden og målet. Hvordan skille i tid og rom eller sette barrierer mellom energikilden og målet.

Del tre, med strategi åtte til 10, omhandler hvordan man kan gjøre målet mer resistent mot skade og hvordan man kan begrense de skadene som eventuelt måtte oppstå. Strategi 10 omhandler hvordan man kan stabilisere, reparere og rehabilitere målet etter inntruffen skade.

Haddon (1980) beskriver i sin modell strategier og ikke konkrete barrierer. Allikevel er disse strategiene retningsgivende for hva slags og hvilke barrierer som er relevante for forskjellige typer virksomheter.

Coaffee og Boshier (2008) beskriver barrierer knyttet til terrorsikring av områder og anlegg. De viser til at barrierer ikke bare er stengsler i tradisjonell stil og utforming, men også kan være en dekorativ installasjon med forankring dypt ned i bakken og med et materiale som tåler angrep av tyngre kjøretøy. Eksempelet de bruker i sin artikkel er, er barrierene rundt Emirates Stadium i London, hvor bokstavene ARSENAL er forankret ned i bakken og tåler nettopp slike anslag.



Fig. 5. The reinforced concrete barrier at an entrance to the Emirates stadium, north London

Figur 8: Bilde av Emirates stadium I (Coaffee & Bosher, 2008, s. 79)

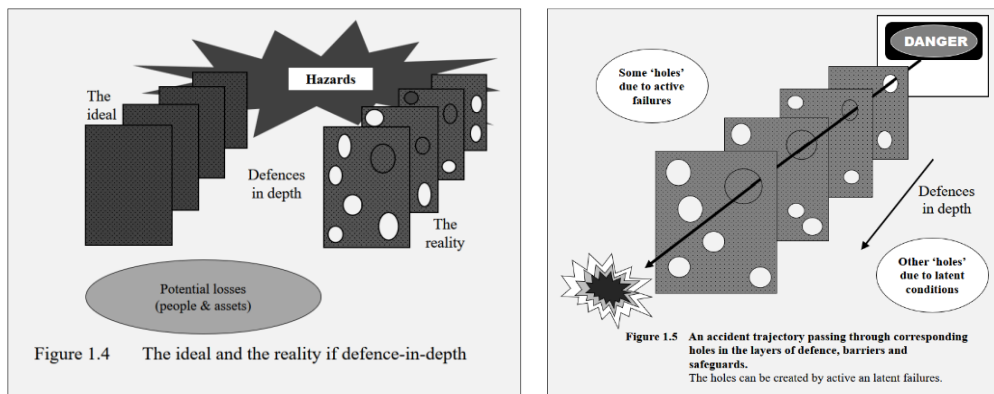
En mer tradisjonell form for barrierer er roadblockers. Disse kan være elektronisk styrte og ligge nede i bakken ved normal situasjon for så å kjøres opp ved forhøyet trusselnivå eller annet behov.



Fig. 1. A system of retractable bollards, which encircle Manchester city centre and limit access to vehicular traffic

Figur 9: Bilde av Roadblockers (Coaffee & Bosher, 2008, s. 77)

Barrierer beskrives også av flere teoretikere. James Reason (2016) fremstiller barrierer i sin Swiss-cheese-modell. I denne fremstillingen av modellen, vist i figur 10, ser man idealet til venstre med tette barrierer i alle lag, mens realiteten til høyre viser barrierer med hull i alle lag. I modellen til høyre, ser man hvordan Reason mener at hull i barrierer er årsaken til uønskede handlinger.



Figur 10: Swiss Cheese (Reason, 2016, (s. 9 og 12))

Reason (2016) snakker om hullene i barrierene som aktive feil, eller latente forhold. Han sier at aktive feil er noe som skjer i enden av et system. En operatør eller en arbeider som med vilje enten gjør en feil for å spare tid eller gjøre arbeidsoppgaven mer komfortabel. Aktive feil kan også skje høyt oppe i en virksomhet, hvor ledere bevisst kan velge bort enkelte viktige oppgaver for å ha bedre inntjening. Et eksempel på dette kan være å kutte ned tid og ressurser til opplæring. Reason (2016) sier at dette igjen kan føre til det han kaller latente forhold. Latente forhold, sier Reason (2016), er forhold som ligger skjult i organisasjonen, men som leder til aktive feil. Den som gjør feilen i enden av systemet, er ikke nødvendigvis klar over at det vedkommende gjør er feil. Både aktive feil og latente forhold kan være hull i barrierene i Reason (2016) sin modell.

Reason (2016) hevder at god sikkerhetskultur i en organisasjon vil kunne oppdage latente forhold og tette hull i barrierer. Han mener at man ved stadig å jobbe målrettet med sikkerhet vil kunne redusere antallet eller unngå at alvorlige hendelser skjer. Jeg vil komme inn på sikkerhetskultur senere i dette kapittelet.

En annen teoretiker som også har med latente feil i sin modell er Barry Turner (1976). Hans perspektiv understøtter Reason (2016) sine tanker om latente feil og at dette kan være grunnlag for hendelser. I motsetning til Reason (2016), hevder Turner (1976) at latente forhold ikke kan oppdages, de inkuberes i organisasjonene og kommer først til syne når uønskede hendelser oppstår. Informasjonsprosesseringsperspektivet til Turner (1976) sier noe om hvordan informasjon innhentes, bearbeides og brukes. Hvordan prosesserer vi informasjon vi tilegner oss fra lover, regler, normer, praksis og kultur? Hvordan forstår og tolker vi denne informasjonen slik at vi kan benytte den i vår praksis? Sett i relasjon med informasjonsflyt og samhandling vil dette perspektivet gi at det dannes en ny sannhet i organisasjonen, knyttet til lover, regler, normer og praksis, som blir informert om og samhandlet rundt. Dette blir den nye normalen i organisasjonen. Og man vil ikke komme tilbake til utgangspunktet og

opprinnelig praksis før det skjer en hendelse. Informasjonsprosesseringsperspektivet til Turner (1976) er delt inn i seks faser.

| The Sequence of Events Associated with a Failure of Foresight | |
|--|--|
| Stage I | Notionally normal starting point: (a) Initial culturally accepted beliefs about the world and its hazards (b) Associated precautionary norms set out in laws, codes of practice, mores, and folkways. |
| Stage II | Incubation period: the accumulation of an unnoticed set of events which are at odds with the accepted beliefs about hazards and the norms for their avoidance. |
| Stage III | Precipitating event: forces itself to the attention and transforms general perceptions of Stage II. |
| Stage IV | Onset: the immediate consequences of the collapse of cultural precautions become apparent. |
| Stage V | Rescue and salvage — first stage adjustment: the immediate postcollapse situation is recognized in ad hoc adjustments which permit the work of rescue and salvage to be started. |
| Stage VI | Full cultural readjustment: an inquiry or assessment is carried out, and beliefs and precautionary norms are adjusted to fit the newly gained understanding of the world. |

Figur 11: The sequence of events associated with a failure of foresight (Turner, 1976)

Steg en **I** modellen er utgangspunktet og det som da er normalen. Perimetersikringen virker fordi ingen på utsiden er interessert i det som foregår på innsiden, det er bare et industriområde med mye forskjellig produksjon.

I steg **II**, inkubasjonsperioden, tillegger organisasjonen seg uvaner og danner seg egne lover og regler som sakte blir innlemmet i tankegang og kultur, som nye sannheter. Ansatte lar personer komme inn gjennom perimetersikringen fordi de sier de har kort, men har gemt det. Personell i biler lar også andre biler og personer følge etter seg inn porter i stedet for å stoppe innenfor porten slik at neste bil også må registrere seg inn.

Steg **III** viser en hendelse knyttet til svakheter i perimetersikringen. Man lar en person slippe inn gjennomperimetersikringen og denne utfører et tyveri inne på Industriområdet.

Steg **IV** i modellen viser at tyveriet kunne skje fordi perimetersikringen ikke var så sikker som man trodde. Samtidig var andre enn ansatte blitt interessert i hva som ble produsert inne på Industriområdet og så nok verdi i dette til at det var ønskelig å stjele noe.

I steg **V** innser Industriområdet at de nå har blitt et mål for tyverier og må iverksette strakstiltak for å hindre at dette skal kunne skje igjen. Personellet som opererer perimetersikringen, blir gjort kjent med nytt trusselbilde knyttet til tyverier. Samtidig jobber man med mer permanente tiltak.

I steg **VI** blir nye permanente tiltak mot tyverier satt inn, og man iverksetter nye rutiner, regler og retningslinjer tilpasset ny kunnskap om at man har blitt et mål for tyverier. Dette medfører nytt fokus for hele perimetersikringen og de som jobber med denne.

Turners perspektiv viser hvordan informasjon og informasjonsprosessering kan være medvirkende til at barrierer opprettes, men også at disse med tiden, selv kan falle bort dersom man ikke har riktig fokus og ved at man lar uvaner og dårlig sikkerhetsfokus slå rot, inkuberes, i organisasjonen som latente forhold.

Det er syn på og teorier rundt barrierer som bruker andre definisjoner.

Stranden (2019) kaller barrierene for tiltak. Han deler det inn etter sikringstrekanten i Teknologiske tiltak, Organisatoriske tiltak og menneskelige tiltak. Stranden refererer til Standard Norge 2012 og definerer teknologisk sikringstiltak slik: «fysisk, elektronisk eller logisk sikringstiltak» (Stranden, 2019, s. 133).

De tekniske tiltakene er «dumme» sier Stranden (2019). De er avhengige av mennesker og organisasjon for å fungere. Eksempler på slike teknologiske barrierer kan være innbruddsalarmer, gjerder, murer, kameraovervåking, bygningsstrukturer, porter, adgangskontrollsystemer osv. Smith og Brooks (2013) nevner eksempler på tekniske barrierer og tiltak for å forhindre uautorisert personell inn på sperrede områder. De nevner CCTV² overvåking, tilgangskontroll med adgangskort med forskjellige registreringsmetoder, fra magnetstriper til biometri og de nevner overvåknings og sporingssystemer. De nevner tre hovedpunkter i denne kontrollen, deteksjon, gjenkjennelse og identifikasjon.

Organisatoriske tiltak: «tiltak i form av skriftlige eller muntlige beskrivelser, vurderinger og beslutninger som regulerer ledelse, organisering, prosesser, analyser, rutiner, adferd og/eller anvendelse av andre sikringstiltak» (Stranden, 2019, s. 181). Stranden (2019) deler de organisatoriske tiltakene inn i tre hovedgrupper: administrasjon og ledelse, analyse og verifikasjon. Stranden (2019) sier at disse tre hovedgruppene gir oss flere relevante faktorer som kan gjøres om til organisatoriske tiltak.

Menneskelige tiltak: «et sentralt spørsmål vi forsøker å besvare, er hvordan man kan få ansatte til å velge den løsningen som ganger sikkerheten. Det man søker, er den opplyste og motiverte medarbeideren som i tillegg har evner til å gjøre de riktige tingene» (Stranden, 2019, s. 265).

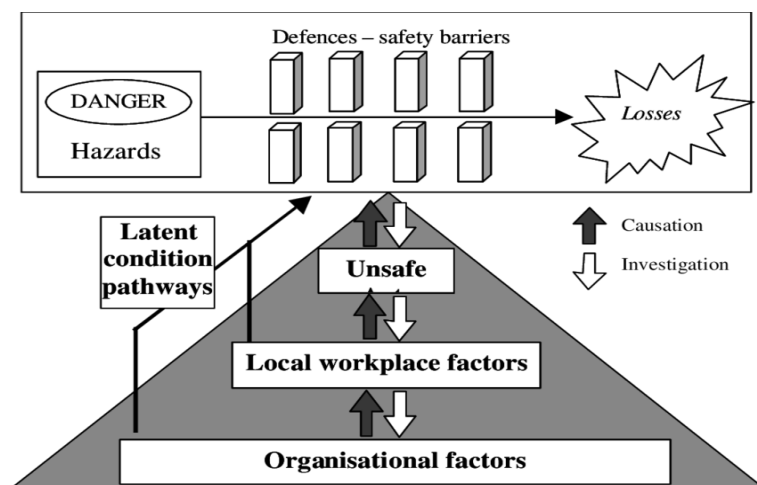
² CCTV - Closed-Circuit TeleVision. Ofte brukt forkortelse for kameraovervåking.

Også menneskelige tiltak deler Stranden (2019) inn i tre hovedgrupper, biologiske, kognitive og sosiale. Denne tredelingen mener Stranden (2019) gjør det forståelig å jobbe med den menneskelige faktor på et hensiktsmessig nivå innenfor sikkerhetsarbeidet.

Innholdet i sikkerhetstrekløveret og beskrivelsen av samspillet mellom det forskjellige delene, med menneskelig og organisatorisk som to av tre hovedfaktorer. Men flere teoretikere hevder at det er forhold som kan rukke ved sikkerheten, selv om man tror man har en sikker arbeidshverdag og organisasjon, de snakker om latente forhold.

2.5.2 Latente forhold

Latente forhold er forhold som ligger i en organisasjon og som er usynlige for de fleste. Barry Turner (1976) omtaler disse latente forholdene. Turner (1976) sier at disse latente forholdene blir inkubert i organisasjonen og blir en del av organisasjonen. På den måten, mener Turner (1976), er de umulige å oppdage, og vil til slutt føre til aktive feil i organisasjoner og arbeidsprosesser. Reason (2016) omtaler også disse latente forholdene som noe man ikke ser, men som har direkte innvirkning på aktive feil eller, som gjøres i organisasjonen. Aktive feil kan gjøres på alle nivåer i en organisasjon. Reason (2016) viser dette denne modellen



Figur 12: Modell for utvikling og gransking av ulykker (Reason, 2016, s. 17)

I modellen er latente forhold vist som de svarte pilene til venstre i modellen som går fra organisatorisk faktorer, via lokale arbeidsforhold til usikker adferd, som leder til en hendelse. De hvite pilene på høyre side viser at man ved en hendelse, jobber seg nedover i modellen for å detektere hvor i organisasjonen årsaken til hendelsen lå. Om det var latente forhold som var årsaken eller om det var en usikker handling.

Reason (2016) peker på dårlig opplæring som et eksempel på slike latente forhold. Hvis man er lært opp til å utføre en oppgave på en spesiell måte, vil man fortsette å løse oppgaven på

slik, til noen forteller deg at det er feil. Dersom ikke praksis før det, leder til at det blir begått en feil. I motsetning til Turner, hevder Reason at man kan eliminere disse latente forholdene ved å bygge en god sikkerhetskultur.

2.5.3 Sikkerhetskultur

Skal man se på sikkerhetskultur isolert vil dette knytte seg opp mot den menneskelige og organisatoriske delen av sikkerhetstrekløveret, men vil gjennom det også ha en direkte innvirkning på de teknologiske tiltakene, siden disse, som Stranden (2019) skrev, er avhengige av de to andre delene.

«Acquiring a safety culture is a process of collective learning, like any other. Nor is it a single entity. It is made up of a number of interacting elements, or ways of doing, thinking and managing that have enhanced safety health as their natural byproduct» (Reason, 2016, s. 192).

Reason (2016) sier en sikkerhetskultur består av fire viktige subkulturer: en rapporterende kultur, en rettferdig kultur, en fleksibel kultur og en informert kultur.

Stranden (2019) gir oss hovedelementene i de fire subkulturene.

I en **rapporterende kultur** blir alt som er av interesse for virksomheten rapportert. Det være seg hendelser som har innvirkning på virksomheten, ulykker, skader eller feil som blir begått. Det er viktig i en slik rapporterende kultur at tilliten til ledelsen er så stor at man rapporterer det som skal rapporteres uten å holde noe tilbake. For dersom noe holdes tilbake kan det på sikt være skadelig for virksomheten. Tanken med å rapportere så grundig er at virksomheten skal kunne lære av de feil og hendelser som blir begått eller skjer.

En **rettferdig kultur** er en kultur der hendelser og reaksjoner står i forhold til hverandre, og det ikke blir handlet vilkårlig ut ifra hvem som begår feil eller hvem som rapporterer inn feil, hendelser eller mangler. Et viktig grunnprinsipp i en rettferdig kultur er at alle skal behandles og straffes likt for like brudd. Dersom dette ikke blir tilfelle og det handles vilkårlig, vil innrapporteringen slutte, og man vil ikke få kjennskap til feil eller hendelser.

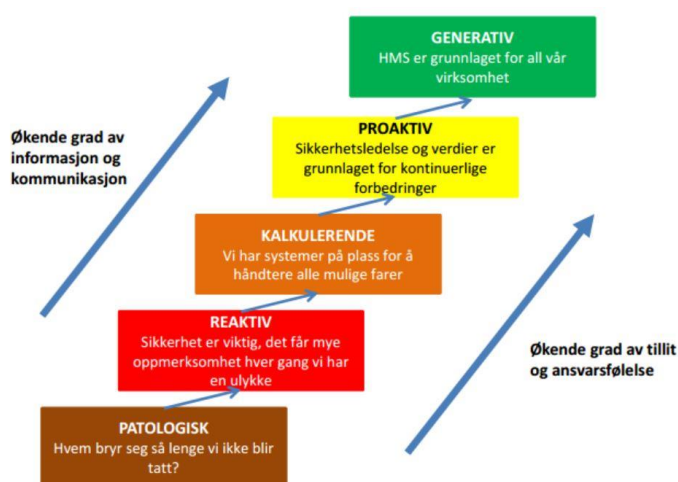
Med **fleksibel kultur** menes en kultur som tilpasser seg ulike situasjoner og krav. Man er fleksibel i forhold til hva som skjer i virksomheten. I en slik fleksibel kultur beveger man seg fra sentralisert til desentralisert styresett ut ifra hvilke hendelser som oppstår. Det er bred kompetanse i organisasjonen og man kjenner godt til prosedyrer og virksomhetens målsetninger. Dette gjør at man sømløst vil kunne bevege seg fra et styresett til et annet.

En *lærende kultur* tilsier at man har en virksomhet som er interessert i og evner å lære av egne feil og hendelser. I en lærende kultur har man evnen til å observere, reflektere, skape og handle og gjennom dette skape en læring for alle i virksomheten. Et tiltak i en virksomhet er å utpeke bestemte medarbeidere som har i oppgave å vurdere og rapportere inn til ledelsen etter hendelser, øvelser og liknende med forslag og tiltak til forbedringer.

«Avslutningsvis er det viktig å påpeke at sikkerhetskultur ikke er tiltaket/virkemidlet for å oppnå ønsket sikkerhet, men et uttrykk for tilstanden historisk, nå eller i fremtiden» (Stranden, 2019, s. 363).

«Finally, it is worth pointing out that if you are convinced that your organization has a good safety culture, you are almost certainly mistaken. Like a state of grace, a safety culture is something that is striven for but rarely attained. As in religion, the process is more important than the product. The virtue – and the reward – lies in the struggle rather than the outcome» (Reason, 2016, s. 220)

Trond Kongsvik (2016) tar også frem sikkerhetskulturbegrepet i sin bok, *Sikkerhet i organisasjoner*. «Kultur «eies» ikke av noen, og forsøk på manipulering av kulturelle forhold, for eksempel i form av sikkerhetskampanjer, kan lett bli gjenstand for motarbeidelse og sabotasje, spesielt hvis slikt forsøk bryter med allerede eksisterende grunnleggende antakelser» (Kongsvik, 2016, s. 111). Kongsvik viser i sin bok til de samme delene av sikkerhetskulturen som Reason (2016) og Stranden (2019) bruker, men han legger til et nytt moment for utvikling av sikkerhetskultur og viser til Hudsons (2007) kulturelle stige.



Figur 13: Hudsons (2007) kulturelle stige (Kongsvik, 2016, s. 118)

Hudson (2007) utviklet sin stige sammen med forskere og praktikere i Shell. «Tankesettet for dette arbeidet kan også sies å ha relativt tydelige funksjonalistiske trekk – kultur betraktes som et verktøy på samme konseptuelle nivå som teknologi og systemer for sikkerhetsledelse, og som virkemiddel for å bedre sikkerheten i ulike kontekster.» (Kongsvik, 2016, s. 117). Modellen er videreutviklet av en modell fra Westrum (1991).

Kongsvik (2016) beskriver arbeidet til Hudson og hans gruppe i vurderingen av stigen som verktøy i bygging av en sikkerhetskultur. Shell gikk her fra en tanke om at en *push-strategi*, hvor ordregiving og ledelseskontroll, ble erstattet med en *pull-strategi*, hvor forbedringsarbeidet skulle skje ved at ansatte fikk en indre motivasjon til å jobbe mot en bedre sikkerhetskultur. På denne måten ønsket man å klatre steg for steg i stigen til man endte på, det man fra et sikkerhetsmessig ståsted anså å være det beste nivået av sikkerhetskultur, «generativ kultur». Denne indre motivasjonen skulle komme gjennom at man jobbet sikkert, uten kontroll og sanksjoner fra ledelsen. «Oppnåelsen av en «generativ kultur» ble ansett å være avhengig av at det var et aktivt ønske om forbedring blant de ansatte heller enn et passivt krav om å møte mål satt av ledelsen» (Kongsvik, 2016, s. 117). I motsetning til modellene til Reason (2016) rundt sikkerhetskultur, ansvarliggjør Hudson (2007) de ansatte i høyere grad enn det Reason (2016) gjør, ved å peke på at kulturen blir bedre dersom man får ansvarliggjort ansatte i den grad at de får et aktivt ønske om forbedring. Dette momentet med ansattes eget ønske, ligger ikke inne i Reason (2016) sin modell.

Når man har sett på vurderingene, truslene, trusselscenariene, sikringen, barrierene og sikkerhetskulturen. Må man se på hvordan dette kan settes i verk ved tilsiktede uønskede hendelser gjennom å se på beredskapen til virksomheten.

2.6 Beredskap

En perimetersikring er avhengig av å bli driftet, kontrollert og vedlikeholdt. Samtidig er det viktig at det blir iverksatt tiltak ved brudd på perimetersikringen. For å kunne imøtekomme dette bør det bygges en beredskap rundt perimetersikringen. Denne beredskapen må være dimensjonert i forhold til de krav som er satt til perimetersikringen og hvordan denne skal driftes, kontrolleres og vedlikeholdes. Denne beredskapen vil anses som en barriere i perimetersikringen og vil være en del av perimetersikringens kvalitet og pålitelighet.

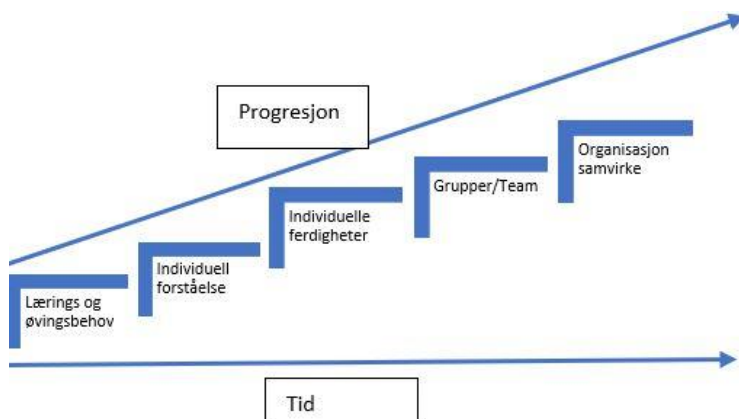
Etablering av beredskap baserer seg på beredskapsanalyser. «En beredskapsanalyse kan forstås og defineres som «en analyse som omfatter etablering av definerte fare- og ulykkessituasjoner, herunder dimensjonerende ulykkessituasjoner, etablering av

funksjonskrav til beredskap og identifikasjon av tiltak for å dimensjonere beredskapen» (Lunde, 2019, s. 60)

Videre referer Lunde (2019) til de fire nasjonale beredskapsprinsippene. **Likhetsprinsippet**, daglig organisering skal også benyttes under uønskede hendelser, slik at beredskapsorganisasjonen er mest mulig lik. **Ansvarsprinsippet**, den som til daglig har ansvar for et fagområde har det samme ansvaret ved en uønsket hendelse. **Nærhetsprinsippet**, uønskede hendelser skal, organisatorisk, løses på lavest mulig nivå. **Samvirkeprinsippet**, man samvirker med relevante aktører og virksomheter i arbeidet med forebygging, beredskap og krisehåndtering. Av disse fire prinsippene er det samvirkeprinsippet som har en innvirkning på perimetersikringen på Industriområdet. hvordan er samvirket mellom de forskjellige operatørene av perimetersikringen, samarbeides det godt, på en måte som gjør at alle i samvirket vet hva som skjer ved en hendelse knyttet til perimetersikringen? Er det slik at alle i samvirket vet hva de skal gjøre? Poenget her er; Vet man hvilke uønskede hendelser man etablerer beredskap for?

Lunde (2019) peker på tre hovedfaktorer i etableringen av beredskap, det er identifisering, etablering og evaluering. I identifiseringen ligger spørsmålene om hva vi skal etablere beredskapen for, hvilke krav den skal oppfylle og hvilke ressurser og tiltak som skal benyttes. For etableringen er spørsmålene hvordan implementere, organisere og dokumentere tiltak og ressurser, samt hvordan man skal gjennomføre opplæring, trening og øving av beredskapsressursene. Evalueringen gjennomføres ved å se på om beredskapen tilfredsstillende eksisterende krav og hvordan etablert beredskap kontinuerlig kan forbedres.

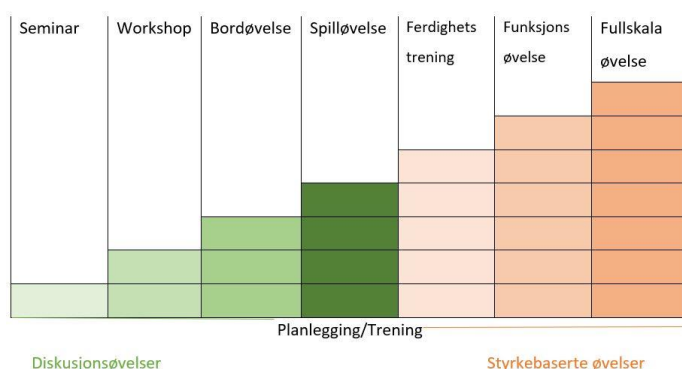
Sommer et al.. (2020) bruker modellen læringstrappa for å vise hvordan man kan øve på forskjellige nivå i en organisasjon. Her vises modellen i en gjengivelse laget til studien:



Figur 14: Gjengivelse av modellen Læringstrappa (Sommer, Pollestad & Steinnes, 2020, s. 128)

I korthet forklarer Sommer et al. (2020) de forskjellige trinnene i modellen på denne måten. Lærings- og øvingsbehov må avdekkes, hva trenger man å lære og hva skal man kunne for å nå de beredskapsmål virksomheten har satt. Individuell forståelse er å forstå hvordan ting skal gjøres. Man må få vite hva som ligger bak og få en grunnleggende teoretisk forståelse og riktige holdninger til det man skal utføre. Individuelle ferdigheter vil være å utvikle praktisk kunnskap i de konkrete arbeidsoppgavene man skal kunne gjennomføre. På grupper/team nivået trener man sammen for å få beredskapsgruppen til å fungere som en samlet enhet, effektivt som et team. Organisasjons og samvirkenivået øver man sammen i hele organisasjonen. Dette blir som en test av de foregående trinnene og at alle i organisasjonen kan sine oppgaver i en uønsket hendelse. Man kan også i disse øvelsene samøve med andre relevante etater eller virksomheter. Sommer et al. (2020) sier at denne måten å øve på, ved fullskalaøvelser, er den beste måte å se om en organisasjon har lært på. Et annet viktig moment i disse øvelsene er at man må øve på de situasjonene man ønsker å løse og ha en beredskap for. Dersom man ønsker å ha en beredskap knyttet til hendelser som omfatter perimetersikringen, må man øve på slike scenarier. Man må øve på inntrengingsforsøk, gisselsituasjon, bombetrusler og andre uønskede hendelser som er reelle trusler mot perimetersikringen. Hvis ikke man gjør det, vil man, som Sommer et al. (2020) sier, ikke lære seg å håndtere disse situasjonene.

For å synliggjøre forskjellige typer øvelser som kan benyttes underveis bruker Sommer et al. (2020) denne modellen, som kan sammenliknes med læringstrappen. Dette er en gjengivelse av modellen laget til denne studien



Figur 15: Gjengivelse av modellen Øvelsestyper (Sommer, Pollestad & Steinnes, 2020, s. 132)

Den grønne delen av trappen er diskusjonsbaserte og teoretiske øvelser man gjør i grupper og på møter. Den røde delen av trappen er fysiske øvelser fra individuell ferdighetstrening til fullskala øvelse.

I tillegg blir dette sagt om dokumentasjon av øvelsene: «Strukturert og systematisk dokumentering av øvingsgjennomføring og oppfølging av evalueringsrapporter, er avgjørende for å kunne oppnå kontinuerlig læring og forbedring av virksomhetens beredskapsevne» (Lunde, 2019, s. 76)

2.7 Oppsummering av teori

Teorien som er brukt i denne studien er valgt for å belyse studiens problemstilling og samtidig kunne danne grunnlag og basis for diskusjon og drøfting opp mot innhentet empiri.

Teoribidragene kan i enkelte tilfeller knyttes både til safety og security problemstillinger, men drøftingen senere i studien vil sette disse inn i security kontekst.

For å kunne besvare problemstillingen og forskningsspørsmålene er teorien satt opp i en rekkefølge som er tenkt fulgt også videre i påfølgende kapitler. Dette for å vise en sammenheng og naturlig rekkefølge på arbeid innen perimetersikring og hvordan arbeidet rundt dette er tenkt.

Kapitlet er derfor bygget fra identifikasjon av uønskede hendelser gjennom risikovurderinger, til hvordan disse skal kunne håndteres med beredskap. Underveis er det synliggjort hvilke trusler, trusselscenarioer man kan stå overfor, hvilke barrierer tiltak man kan sette inn og hvordan man skal kunne etablere og opprettholde en beredskap gjennom læring.

Synligheten av kulturbegrepet gjennom sikkerhetskultur er også en viktig nyanse å ha i denne sammenheng, da dette kan være med på å belyse hvordan synet på safety og security hendelser blir oppfattet og løst på industriområdet.

Funnene i teoriene vil bli ført videre og drøftet i kapittel fem, opp imot funn fra dokumentanalyse, intervjuer, deltakende observasjoner og samtaler fra deltakende observasjoner.

3. Metode

«Metode dreier seg om å etablere prosedyrer og teknikker for å komme fram til mest mulig relevant og pålitelig kunnskap om samfunnet. Dette er teorier om hvordan informanter bør velges ut, hvordan data skal samles inn, og ikke minst hvordan data skal analyseres og tolkes» (Johannesen, Tufte, & Christoffersen, 2016, s. 40).

Metodene valgt i denne studien, er ikke bare valgt for å få fram relevant og pålitelig kunnskap, men også valgt med tanke på forståelse av Industriområdet. For å besvare problemstillingen og forskningsspørsmålene til studien er ikke bare svar, funn og observasjoner viktig, men også forståelsen av i hvilken kontekst spørsmålene blir stilt, svarene blir gitt og observasjonene gjort.

3.1 Forskningsdesign

«Den første fasen i et prosjekt er å foredle den første ideen til en faglig interessant problemstilling» (Ringdal, 2013, s. 20).

Dette er en dekkende setning for denne studien i seg selv. Hvordan få en stor ide til å bli en konkret interessant problemstilling? Dette medfører noen valg, avveininger og ikke minst avgrensinger i oppstartfasen. Hva er det mulig å forske på og hvor stor kan en slik studie være? Det ble tidlig klart at dette kunne gjøres til begge deler, en konkret avgrenset studie, eller en stor og meget omfattende studie. Valget, etter avgrensing, falt på en konkret og avgrenset studie.

«Derfor er det viktig allerede i begynnelsen av et nytt prosjekt å legge vekt på hva prosjektet kan bidra med ut over det andre har gjort» (Ringdal, 2013, s. 21). Som prosjekt vil denne studien, kunne avdekke noe Industriområdet ønsker å sette fokus på, på en annen måte enn de har gjort til nå. På den måten vil også studien kunne sies å være eksplorativ, fordi studien søker svar på noe det ikke er forsket på tidligere og studien vil søke å finne svar på en problemstilling som ikke tidligere er belyst.

Studien vil bygge på kvalitativ metode. «Kvalitativ metode passer også godt til eksplorerende undersøkelser av fenomener og forhold det i liten grad er forsket på» (Ringdal, 2013, s. 24). Videre: «Forskningsspørsmål som kan peke mot kvalitativ metode, begynner gjerne med hva eller hvordan, der formålet er å beskrive ...» (Ringdal, 2013, s. 25). Svar på hva eller hvordan spørsmål, er i utgangspunktet grunnleggende i forhold til å få svar på de spørsmål som studien stiller «Hvordan er påliteligheten ...».

Deltagende observasjon og ulike typer intervjuer vil være de fremtredende metodene for datainnsamling i denne studien, sammen med dokumentanalyse. Det å bruke observasjon som metode og være til stede på Industriområdet, se hvordan oppgaver knyttet til perimetersikringen gjennomføres i sin rette kontekst, i sitt rette element og miljø vil være viktig får å kunne belyse problemstillingen.

Videre vil valgte metoder som er benyttet i studien bli nærmere beskrevet.

3.2 Casestudie

«Casestudier benyttes i dag på en lang rekke forskningsfelt, for eksempel på skoleforskning, evalueringsforskning og organisasjonsforskning» (Ringdal, 2013, s. 169). Denne studien kan hevdes å være en kombinasjon av evalueringsforskning og organisasjonsforskning, da den forsker på Industriområdet som organisasjon, men også på om systemene rundt perimetersikringen er pålitelige, altså en evaluering. «Case som forskningsdesign er en prosess som innebærer utforming av en problemstilling, valg av teoretisk forankring, analyseenheter og datainnsamlingsteknikk samt kriterier for å analysere og tolke data» (Johannesen, Tufte, & Christoffersen, 2016, s. 203). Utvelgelsen av casen til denne studien er basert på ønsker fra industriområdet om et spesifikt tema de ønsket en studie rundt. Allikevel kan det hevdes at rene tilfeldigheter gjorde at nettopp denne casen ble valgt til studien, for det var i dialog med Industriområdet at problemstillingen for casen ble valgt, og ikke motsatt.

Denne studien vil ha en casedesign som beskrives som en unik casestudie. «En unik casestudie bør fange inn kompleksiteten i en case: fokusere på det spesielle, snarere enn på det generelle. Målet for denne typen studier er å tolke og forstå en case, ikke bidra til generelle forklaringer ...» (Ringdal, 2013, s. 171). Her er casen i hovedfokus, målet er å få fram det spesielle med casen, perimetersikring mot uautorisert adgang. I denne studien vil Industriområdet være omgivelsene, mens fenomenet som forskes på er perimetersikringen. «En casestudie er en empirisk undersøkelse av et fenomen i sine naturlige omgivelser, der flere datakilder benyttes» (Ringdal, 2013, s. 108).

Dette kan til sammenlikning være det Johannesen et al. (2016) kaller enkeltcasedesign. Beskrivelsen deres av enkeltcasedesign er enda mer treffende for denne studien enn definisjonen til Ringdal (2013), da Johannesen et al. (2016) sin definisjon av begrepet er mer treffende for problemstillingen i studien. «Enkeltcasedesign er hensiktsmessig hvis casen representerer et kritisk, ekstremt eller unikt tilfelle og der casen kan avdekke viktige fenomener, hendelser eller situasjoner» (Johannesen, Tufte, & Christoffersen, 2016, s. 205).

Denne studien søker å belyse påliteligheten til perimetersikringen av Industriområdet. Et brudd på denne perimetersikringen kommer klart under viktige hendelser eller situasjoner, siden det kan få alvorlige ringvirkninger for sikkerhet, drift og produksjon på Industriområdet.

Johannesen et al. henviser til Yin sin femtrinnsmodell (2016, ss. 207-212). Disse fem trinnene er.

Problemstilling. Problemstillingen som er valgt for oppgaven er valgt i samarbeid med Industriområdet. Etter møter med Industriområdet hvor muligheter for å skrive masteroppgave knyttet dit, ble flere muligheter for problemstilling diskutert. Problemstillingen som til slutt ble valgt var knyttet til et område hvor Industriområdet mente de hadde forbedringspotensial. Samtidig var det en problemstilling hvor jeg kunne benytte meg av erfaringer, kunnskap og kompetanse fra egen arbeidsplass for å forske på å besvare.

Teoretiske antakelser. Teoriene som er belyst i studien er teorier som er tatt med fordi de er vurdert som hensiktsmessige for å kunne drøfte og besvare problemstillingen. Tanken bak forskjellige teorier og perspektiver med forskjellige innfallsvinkler mot problemstillingen er nettopp for å kunne ha et bredt drøftingsgrunnlag og dermed et godt grunnlag for en endelig konklusjon.

Analyseenheter. For å belyse problemstillingen og perimetersikringen grundig og gjennomgående valgte jeg gjerdetraséen med Vaktentral og havneport som analyseenheter. For å kunne se perimetersikringen av Industriområdet som helhet og kunne gjøre en helhetlig analyse av denne var vaktentral, havneport og gjerdetraséen selvsagte analyseenheter i dette arbeidet. Vaktentralen fordi den har det overordnede oppsynet av, og kontrollfunksjonen med, hele gjerdetraséen. Havneport fordi denne har en egen definert rolle i perimetersikringen ved forhøyet trusselbilde. Gjerdetraséen som egen analyseenhet for å se på traséen i seg selv som perimetersikring og for å kunne vurdere barrierer som er knyttet til denne.

Rekruttering. Ved rekruttering av intervjuobjekter var det viktig for meg å få et mangfold av informanter som både jobbet med vakthold, drift og beredskap rundt perimetersikringen. Samtidig og i tillegg til dette ønsket jeg å ha med informanter som ikke jobbet med perimetersikringen, men som i kraft av å være personell inne på Industriområdet, faktisk var sikret av perimetersikringen. Det var også viktig at det var en bred gruppe informanter fra forskjellige lag i hierarkiet på Industriområdet, både ledelse og ansatte fagarbeidere. Dette for å se om det er språk mellom ledelsen og fagarbeideres syn på perimetersikringen.

Den logiske sammenhengen mellom data og antakelsene. Denne studien kan best beskrives som en «analyse med utgangspunkt i empiri» (Johannesen, Tufte, & Christoffersen, 2016, s. 211). Johannesen et al. (2016) sier videre «Funnene analyseres mot teorien, som enten vil hjelpe oss å forstå praksis eller danne grunnlag for ny teori. Data og teori har med andre ord en gjensidig påvirkning på hverandre gjennom hele forskningsprosessen». Ny teori i denne studien vil eventuell videreutvikling av barriereperspektivet og sikring.

3.3 Datainnsamling

Datainnsamlingen til denne studien ble gjennomført ved deltagende observasjon, ved tilstedeværelse i arbeidssituasjoner, deltakelse som markør under øvelse, aktiv informantintervjuing og innhenting av og søk etter dokumenter. Disse metodene ble valgt for på best mulig måte belyse problemstillingen og forskningsspørsmålene.

3.3.1 Observasjoner

Tidlig i planleggingen av studien ble det klart at observasjon ville være et godt verktøy for å belyse problemstillingen. Det å være til stede, se hva og hvordan ting blir gjort, diskutert og rapportert gjennom observasjoner var ønskelig. Samtidig ville det i slike situasjoner være mulig å presentere meg, i møte med de medarbeiderne som ville være til stede under studien. Ved å presentere meg og informere om hvorfor jeg var til stede og hva som var misjonen med studien, ville dette også kunne være med på å ufarliggjøre og normalisere prosessen senere, rundt informantintervjuingen. Dette fordi ansatte allerede var kjent med at jeg stilte spørsmål rundt perimetersikringen i andre fora. I slike situasjoner ville det være mulig for meg å være deltaker i diskusjoner og gjennom det skaffe informasjon som ville kunne belyse problemstillingen og forskningsspørsmålene på en bedre måte. Dette i motsetning til kun å passivt observere fra avstand, og ikke få muligheten til å stille relevante oppfølgingsspørsmål i sanntid og i riktig kontekst der informasjonen hadde sitt opphav. En effekt jeg hadde fokus på under observasjonene var det Ringdal (2013) kaller kontrolleffekten. «Valg av observatørrolle har også konsekvenser for kontrolleffekten, det vil si at de som studeres, endrer sin atferd fordi forskeren er til stede» (Ringdal, 2013, s. 230). Ringdal (2013) sier videre at det å oppnå nær kontakt med og tillit hos informanter og de som studeres, kan motvirke denne kontrolleffekten. Allikevel vil dette være noe man må ta med som et moment i denne studien. «Feltarbeid som pågår over kort tid, eller som bærer preg av besøk, sannsynligvis vil være mest utsatt for kontrolleffekten» (Ringdal, 2013, s. 230).

Mine kontakter på Industriområdet mente også at deltakende observasjon ville være en fin form for involvering. De aktuelle informantene, som gjennom å se tilstedeværelse av meg som observatør, ville føle dette som mer naturlig og ikke som en kontroll av arbeidsoppgaver for å finne feil og mangler. Jeg vil i dette tilfellet også kunne benytte meg av to typer observasjon, statisk og dynamisk (Halvorsen, Khawaja, & Storvik, 2019). Halvorsen et.al. (2019) beskriver de to typene observasjon slik. *Statisk observasjon* er observasjon gjort fra avstand hvor syn er den fremtredende sansen for å gjøre observasjonen, *dynamisk observasjon* er observasjon gjort inne i en gruppe mennesker eller inne i lukkede omgivelser. Her er hovedfokus på alle sanser, syn lukt, hørsel og man observerer ved å kombinere alle sansene.

«De logiske empiristene la vekt på at vitenskap begynner med observasjoner av virkeligheten. Vitenskapelig kunnskap er generelle utsagn eller teorier som generaliseres fra observasjoner i empiriske undersøkelser ...» (Ringdal, 2013, s. 38). Ringdal fortsetter, «Bare utsagn som i prinsippet kan verifiseres eller falsifiseres av observasjoner, er meningsfulle.» (Ringdal, 2013, s. 39).

Under observasjon kan jeg innta forskjellige roller. Ringdal (2013) peker på tre forskjellige, den fullstendige observatør, den deltagende observatør og den fullstendige deltaker. I denne studien var det naturlig for meg å innta rollen som deltakende observatør. Gjennom deltakelse på møter, være til stede i vaktentralen under arbeid og delta på øvelser som skal avholdes. Deltakende observatører befinner seg midt imellom to perspektiver for observasjon, beskrevet i Ringdal (2013, s. 230) observatørens outside- og deltakerens innsideperspektiv. Det vises her også til to myter som viser forskjellene mellom de to perspektivene. «Ifølge outsidermyten kan holdbar forskning bare utføres av forskere som har tilstrekkelig avstand, og som kan betrakte en gruppe eller et miljø på en objektiv måte. Insidermyten representerer det motsatte synet. Det er nødvendig å kjenne en gruppe innenfra for å kunne forstå den» (Hammersley og Atkinson, 1996, s. 137-140) i (Ringdal, 2013, s. 230). I denne studien er det viktig å få frem at Industriområdet ga full tilgang til sine områder som var relevante for studien, slik at deltakende observasjon var mulig å gjennomføre. Dette gjør at jeg, som Lysgaard (1975) beskriver i Ringdal (2013, s. 237) kan «forstå adferd ut fra hva som er rasjonelt når man ser det i tilknytning til deres situasjon og de midler de disponerer». Samtidig var det under denne studien umulig ikke å drive med en deltakende observasjon. I hver setting jeg vært, har jeg blitt inkludert og spurt om mine meninger og synspunkter rundt de arbeidsoppgavene, møtene og øvelsene jeg har observert. Selv om jeg har inntatt en nøytral rolle og forsøkt å holde meg i

bakgrunnen, har jeg alltid blitt inkludert i det som har skjedd. Derfor har observasjoner i denne studien blitt gjennomført som deltakende observasjoner.

Johannesen et al. (2016) beskriver observasjon gjennom seks sentrale begreper: Observatøren, Observasjon, Feltet, Feltarbeid, Settingen og Analyseenheten. Ved å knytte disse begrepene direkte til denne studien vil det bli slik. Observatøren er forskeren som gjennomfører forskningen, i dette tilfellet meg selv, som forfatter av masteroppgaven. Observasjoner en systematisk observasjon av de relevante områder og ansatte ved Industriområdet, de ansatte som har jobber knyttet til perimetersikringen. Feltet er Industriområdet og de stedene som er knyttet til arbeid med perimetersikring, for eksempel vaktentral, portvakter og liknende. Feltarbeidet er innsamlingen av data gjennom observasjoner rundt operasjonaliseringen og driften av perimetersikringen, observasjoner gjennom å være markør under en øvelse, deltakelse på sikkerhetskurs og aktiv informantintervjuing. Settingen er vaktentral, havneport, industriområdet utenfor og innenfor perimetersikringen samt andre aktuelle møtestedet som er relevant å besøke for å belyse problemstillingen. Analyseenheten er perimetersikringen, de ansatte som kontrollerer, utfører og opprettholder perimetersikringen samt alle informanter og andre deltagende som er med på å belyse problemstillingen og forskningsspørsmålene. Tabellen under viser aktivitetene under studien.

| Beskrivelse av gjennomførte observasjoner, møter, samtaler og semistrukturerte intervjuer | |
|--|---|
| Oktober 2021 | Innledende møte med HESQ-manager på Industriområdet, med diskusjoner og tanker rundt master og vinkling rundt problemstilling for denne |
| 13. desember | Møte med HESQ-manager for konkretisering av fokusområde for master |
| 13. januar | Møte med HESQ-manager. Innledende innsamling av materiale til grunnlag for masteroppgaven og problemstillingen |
| 10. februar | Observasjon under Påtroppsmøte ved Industriområdet. |
| 16. februar | Veiledning med Kruke |
| Februar | Innhenting av teori til oppgave |
| Mars | Innhenting av dokumenter til dokumentanalyse |
| 14. mars | Veiledning med Kruke |
| Uke 12 | Gjennomføring av 11 semistrukturerte samtaleintervjuer, aktiv informant intervjuing |

| | |
|-----------|---|
| 21. mars | Markør under øvelse |
| 23. mars | Observatør vaktentral ettermiddag (3 timer) |
| 24. mars | Observatør vaktentral formiddag (3 timer) |
| 24. mars | Observatør Havneport formiddag (3 timer) |
| 25. mars | Observatør på Vaktmøte |
| 25. mars | Observatør Påtroppsmøte |
| April | Strukturering av funn fra dokumentanalyse, observasjoner og intervjuer til empiridel. |
| 8. april | Gjennomført 3 digitale sikkerhetskurs |
| 19. april | Gjennomført siste del, del 4, av sikkerhetskurs, klasseromsundervisning |
| 28. april | Observatør på øvelse «Fabrikkalarm» ute på Industriområdet |
| 04. mai | Observatør på øvelse «Fabrikkalarm» inne i KO |
| 06. mai | Veiledning med Kruke |
| 20. mai | Veiledning med Kruke |
| 27. mai | Skriftlig tilbakemelding på innsendt draft |
| 13. juni | Skriftlig tilbakemelding på innsendt draft |
| 19. juni | Skriftlig tilbakemelding på innsendt draft |
| 28. juni | Skriftlig tilbakemelding på innsendt draft |
| 29. juni | Skriftlig tilbakemelding på innsendt draft |
| 30. juni | Innlevering av masteroppgaven |

Tabell 1: Oversikt over aktiviteter i studien

3.3.2 Aktiv informant intervjuing/ samtaleintervju og semistrukturerte intervjuer

Jeg konkluderte tidlig med at informantintervjuing skulle være en del av denne studien. Dette fordi jeg anså det ville gi et godt grunnlag for å besvare problemstillingen sett opp imot valgt teori og dokumentanalyser. Begrunnelsen for dette er at jeg har lang og god kompetanse fra egen yrkespraksis i å innhente informasjon på denne måten. Jeg er vant til å ta notater og få med meg detaljer fra slike settinger og samtidig kunne snakke fritt, og kunne følge opp informasjon som kommer. Samtidig er jeg også klar over at en slik setting kan virke påtrengende og negativ på en informant, dersom man som intervjuer ikke evner å skape tillit i situasjonen. I intervjusituasjonene, er jeg en utenforstående som skal inn å vurdere etablerte arbeidsoperasjoner, rutiner og systemer, informantene kan anse som gode og derfor at studien, i deres syn, ikke er nødvendig. Samtidig vil det i en slik studie være mulig for informantene å ærlig påpeke momenter i egen arbeidshverdag de ikke mener fungerer like godt, og da få

muligheten til å kunne påvirke dette gjennom å delta i studien heller enn å måtte påpeke disse opplevde forbedringspotensialene selv. «Informantenes interesse for å engasjere seg i møter med en forsker kan påvirkes av en rekke forhold. Noen er knyttet til personlighet eller en generell interesse for forskning eller det temaet som bringes på bane» (Andersen, 2006, s. 289) I oppstartsfasen av studien, var jeg opptatt av å presentere meg og informere grundig om studien, intervjuguiden og misjonen med denne, slik at jeg gjennom denne informasjonen opparbeidet meg tillit i organisasjonen. «Hvor vellykket intervjuet blir, har i stor grad å gjøre med hvor motivert informanten er. En forutsetning for et vellykket intervju er at intervjueren makter å skape tillit hos informanten» (Ringdal, 2013, s. 243).

«Forskning kan ses som en betinget kunnskapstilegnelsesprosess, der forutsetninger aktivt utprøves og utvikles underveis. Det er i en slik sammenheng at uttrykket *aktiv* samtalepreget intervju brukes. Aktiv betyr her at forskeren kontinuerlig søker å utnytte intervjusituasjonen til å prøve ut egne forutsetninger så vel som forutsetninger for informantens observasjoner, beskrivelser og vurderinger» (Andersen, 2006, s. 280). «Intervjueren skal være lyttende, men samtidig ta initiativ uten å overstyre eller lede svar i en bestemt retning» (Andersen, 2006, s. 280). Ved informantintervjuing i denne studien ble denne teorien og metoden valgt for gjennomføring av intervjuene. Det å kunne være aktiv i intervjusituasjonen, utforske informantenes observasjoner, beskrivelser og vurderinger var nødvendig for å få relevant informasjon til studien. Informantene i denne studien ble rekruttert fordi de innehar en relevant kunnskap for studien. Følgende informanter er intervjuet underveis i studien.

| Informant | Stilling og erfaring |
|-----------|---|
| 1 | Fagleder industrivern (FLI) over 30 års erfaring |
| 2 | Ansatt hovedresepsjon ca 20 års erfaring |
| 3 | Industrivern |
| 4 | Ansatt i fabrikk på Industriområdet |
| 5 | Operatør vaktentral |
| 6 | Operatør vaktentral |
| 7 | Verneombud Industriområdet |
| 8 | Operatør Havneport |
| 9 | HESQ manager |
| 10 | Ansatt jobber med installasjon og vedlikehold av perimetersikring |
| 11 | ANNA1 stabsleder ved beredskapshendelser |
| 12-29 | Informanter fra samtaler under deltakende observasjoner ikke spesifikt referert til ut ifra sine utsagn |

Tabell 2: Oversikt over informanter

Andersen (2006) beskriver i sin artikkel at informantene som regel er valgt ut fordi de er velinformerte, ressurssterke og har inngående kunnskap om de saker og sammenhenger som intervjuet skal belyse. Noe av denne kunnskapen er taus hos disse informantene, de innehar den, men reflekterer ikke over at de har den, og må derfor utforskes i intervjusituasjonene. Samtidig var det viktig for meg til en viss grad å styre intervjuene inn mot informasjon som var relevant for studien. «Overfor ressurssterke informanter kan og bør intervjuere derfor være mer aktive og i større grad ta initiativ» (Andersen, 2006, s. 282). Allikevel var det viktig for meg, i intervjusituasjonen, å ikke styre samtalen i den grad at intervjuobjektene følte seg ledet av mine spørsmål. Det var viktig å få frem informantenes personlige svar, refleksjoner og tolkninger. «Det er viktig at intervjueren opptrer på en nøytral og ikke-ledende måte» (Ringdal, 2013, s. 243).

Intervjuene ble nedskrevet for hånd og deretter transkribert til PC. I tillegg til disse intervjuene har jeg også fått inn mye informasjon gjennom samtaler med ansatte under deltakende observasjoner. Dette er samtaler som nesten kan sammenliknes med aktiv informantintervjuing, selv om det ikke har vært gjennomført i en intervjusituasjon eller med en satt intervjuguide. I noen tilfeller har disse samtaler gitt informasjon jeg ikke hadde tenkt på å belyse på forhånd, og har på den måten tilført studien enda mer dybde og variasjon enn hva som ville vært tilfellet uten disse samtaler.

Informantene er alle ansatt på Industriområdet. Noen har stillinger direkte knyttet til operasjonaliseringen av perimetersikringen, noen innehar ledende stillinger med ansvar for perimetersikringen, mens andre har stillinger som gjør at de er sikret av perimetersikringen. På denne måten er informantene valgt ut med bakgrunn i relevans for studien og ikke representativitet. Utvelgelsen er gjort med tanke på tema for studien og at de informantene som ble valgt ut skulle kunne tilføre studien faglig begrunnet syn og kvalifiserte meninger for å belyse problemstillingen og forskningsspørsmålene. Dette gjør at de alle er påvirket av perimetersikringen på en eller annen måte. Innsamlet data og informasjon vil være preget av hvor i organisasjonen informantene jobber. Det som er felles for alle informantene er at de stilte velvillige opp og at alle ønsket studien velkommen. For meg og studien gav dette inntrykk av at kontrolleffekten ved denne studien var lav. Informantene har alle vært tydelige på at de synes det er bra at denne studien blir gjennomført.

Ved gjennomgang av datainnhenting, og intervjuene, oppfatter jeg at alle informantene har svart ærlig og konstruktivt ut ifra sine forutsetninger og overbevisninger knyttet til spørsmålene som ble stilt. Dette vil være med på å belyse problemstillingen fra et bredt spekter av erfaringer, syn og oppfatninger. Jeg mener derfor at det grunnlaget i denne studien er valid og vil være med på å belyse problemstillingen kvalitativt og grundig. Materialet jeg har hentet frem, både i datainnsamlingen og i intervjuene vil være tilstrekkelig til å besvare problemstilling og forskningsspørsmål.

3.3.3 Dokumentanalyse

Formålet med dokumentanalysen i denne studien var å se og kartlegge dokumenter som kunne belyse relevante områder for problemstillingen. Siden denne studien forsker på noe som ikke tidligere er forsket på, vil det ikke være dokumenter som er knyttet direkte til problemstillingen. Allikevel søkte jeg etter dokumenter som kunne være med på å belyse problemstillingen, med fokus på forskning og studier knyttet til påliteligheten til perimetersikringer.

Dokumenter som ble gjennomgått i denne delen av studien var utførte risikovurderinger, planverk, instruksjoner og rapporter fra hendelser knyttet til perimetersikring fra andre Industriområder. Det er også tatt med nasjonale trusselvurderinger for å vurdere om disse kan ha en innvirkning på hvordan man må tilpasse seg et generelt trusselnivå i samfunnet, noe som vil spille inn på hvordan problemstillingen vil bli besvart videre i studien.

3.3.4 Internett søk etter relevante dokumenter

I denne studien har jeg gjort søk på søkemotorene Google, Brage, Google Scholar og Web of science, for å finne relevante dokumenter som kunne underbygge studien med tidligere forskning og relevante opplysninger rundt studiens problemstilling. Det ble søkt med både norske og engelske søkeord. Med søkeordet «Perimetersikring» på søkemotoren Brage, kom det opp fire treff. Søket «Sikring av industriområder» ga 85 treff. Søkeordet «Sikring av industri» ga 1447 treff. I studien har jeg benyttet flere søkemotorer tabellen under viser navn på søkemotor, søkeord og antall treff.

| Søkemotor | Søkeord | Antall treff |
|----------------|--|--------------|
| Brage | Perimetersikring | 4 |
| Brage | Sikring av industriområder | 85 |
| Brage | Sikring av industri | 1447 |
| Google | Perimetersikring av norsk industri | 1190 |
| Google | Brudd på perimetersikring i norsk industri | 244 |
| Google Scholar | Perimeter protection of industrial sites | 65900 |
| Google Scholar | Perimeter barriers in industrial sites | 49400 |
| Web of science | Perimeter protection of industrial sites | 65200 |
| Web of science | Perimeter barriers in industrial sites | 48900 |

Tabell 3: Oversikt over funn ved søk på internett

Dokumenter fra disse søkene har vist meg forskning, lovverk og relevante direktiver som har hjulpet meg i studien. Eksempler på dette Statoil sin rapport «The In Amenas attack» fra 2013, trusselvurderingene fra NSM og PST fra 2022, artikkelen til Coaffee & Bosher fra 2018 og artikkelen til Hegde fra 2015. Samtidig har det gitt meg kunnskap om praktisk bruk av flere av de barrierene teorien beskriver. Lovverk og instruksjoner som er benyttet under

observasjoner og ellers i studien, men ikke brukt inn i oppgaven ble jeg også kjent med via disse søkene.

3.3.5 Utfordringer, pålitelighet og reliabilitet ved datainnsamlingen

«Reliabilitet knytter seg til nøyaktigheten av undersøkelsens data, hvilke data som brukes, den måten de samles inn på, og hvordan de bearbeides.» (Johannesen, Tufte, & Christoffersen, 2016, s. 36). Å samle inn data til denne undersøkelsen har vært utfordrende, spennende, lærerikt og interessant. Det at problemstillingen ikke tidligere har vært forsket på i denne utstrekningen, har gitt utfordringer med å finne annen relevant teori som kunne hjelpe meg å belyse problemstillingen fra flere vinklinger. Dette ga studien et virkelig eksplorerende design og alle data som ble samlet, sees på som ny kunnskap i denne sammenheng. Utfordringer med denne måten å samle inn data på vil jo være at dataene heller ikke kan etterprøves med tidligere forskning eller andre studier/undersøkelser. Dette har gitt en ekstra utfordring i at studien og datainnsamlingen måtte gjøres og gjennomføres med stor grad av troverdighet. «Data er ikke selve virkeligheten, men representasjoner av den» (Johannesen, Tufte, & Christoffersen, 2016, s. 66). Er det slik at de dataene som er samlet inn gir et riktig bilde av virkeligheten eller i denne studien, gir de et representativt bilde av perimetersikringens pålitelighet?

3.3.6 Mottakelsen på industriområdet og av informantene

Fra første møte med HESQ-manager har jeg blitt møtt med en utrolig åpenhet, velvilje og raushet på Industriområdet. Alle informanter, ansatte og andre jeg har møtt har virket genuint interessert i studien og at resultatet av denne skal bli så godt som mulig. Jeg har blitt invitert med inn i alle relevante fora og fått mulighet til å delta i møter, i arbeidsoperasjoner, delta på vakter, vært observatør under øvelser og vært markør under øvelser. All denne åpenheten, rausheten og inkluderingen har gitt meg følelsen av å være velkommen og at studien i seg selv er viktig for Industriområdet. Dette fremkommer også fra flere av informantene som sier at dette er en viktig studie for Industriområdet. Til stadighet har jeg blitt møtt med «hei, er det du som skriver masteroppgave om perimetersikringen vår?». Eller «Den oppgaven du skriver, den tror jeg er viktig for oss å se på». Ikke en eneste gang under studien har jeg blitt avvist eller nektet innsyn i dokumenter, arbeidssituasjoner, planverk eller noe annet jeg har sett på som relevant. Det har heller vært motsatt og jeg har blitt tilbudt innsyn i langt mer enn jeg har kunnet tatt inn i oppgaven for å holde denne innenfor avgrensingene jeg har satt. Denne mottakelsen har også gitt meg en slags ærefrykt og har gjort at jeg har lagt et slags press på meg selv til virkelig å ville yte mitt beste. På en måte å belønne eller vise takknemlighet for

måten jeg har blitt behandlet på ved å virkelig jobbe for at studien skal stå til deltakernes forventninger.

3.4 Bias – Forskerens forforståelse og virkelighetsoppfatning

Underveis i studiet da jeg nærmet meg oppstart av masteroppgaven ble jeg kontaktet av en bekjent som er kasserer i skolekorpset jeg er leder i. Han spurte meg om studiet mitt, hva jeg tenkte med det og om jeg hadde bestemt meg for tema for masteroppgaven. Jeg forklarte om studiet og kunne bekrefte at jeg ikke hadde noe tema for masteroppgaven. Kassereren forklarte at han jobbet på hos en av leietakerne på Industriområdet og at de ofte er interesserte i å få masterstudenter til å skrive oppgaver knyttet til Industriområdet. Personlig synes jeg dette hørtes spennende ut. Jeg har familiemedlemmer kamerater og bekjente, som har jobbet inne på Industriområdet i mange tiår. I tillegg har jeg selv også hatt små arbeidsoppdrag der i starten av min yrkeskarriere. På denne måten kjenner jeg ganske godt til Industriområdet og hva som foregår der. Kassereren spurte om jeg kunne være åpen for forslag til tema til masteroppgaven min fra Industriområdet, noe jeg selvfølgelig var.

En uke senere kom han tilbake med kontaktinformasjon til HESQ-manager på Industriområdet og sa vedkommende ville ha en prat med meg om masteren og at jeg skulle ta kontakt. Jeg gjorde det og i løpet av et møte på Industriområdet var vi enige om å gå videre med temaet security. I utgangspunktet noe om sikring av områder. Jeg tok med meg dette tilbake til UiS og diskuterte dette temaet med professor Bjørn Ivar Kruke, for å høre om dette kunne være grunnlag for en master, noe som ble bekreftet. Etter ny samtale med HESQ-manager ble vi enige om at jeg skulle se på ytre perimetersikring av Industriområdet på land og jobbe videre med å finne en problemstilling rundt dette.

Vi har alle en forforståelse av den virkeligheten vi møter. Vi ser fenomener og observerer hendelser basert på vår egen forforståelse og virkelighetsoppfatning. Våre tidligere erfaringer vil kunne sammenlignes med et filter for hvordan vi oppfatter, sanser og ser hendelser. Vår persepsjon er farget av hvordan vi tidligere har møtt, oppfattet, reagert på og taklet disse hendelsene og fenomenene. Johannesen et al. (2016) sier at denne forforståelsen er helt nødvendig for å forstå virkeligheten.

I denne studien har jeg forsket på noe som ikke er forsket på tidligere. Samtidig vet jeg at problemstillingen har kommet til gjennom et samarbeid med Industriområdet og studien er på den måten nesten å anse som et bestillingsverk for å sette lys på og vurdere perimetersikringen og dennes pålitelighet. Dette har jeg gjennom studien følt som et press på

meg selv til å levere et kvalitativt godt resultat som imøtekommer Industriområdets krav til kvalitet.

Man kan si at studien ble til ved en tilfeldighet, ved at jeg i utgangspunktet ved oppstart og planlegging av min masteroppgave ikke hadde planer om å skrive min oppgave knyttet til en studie av Norsk industri. Jeg har aldri jobbet som fast ansatt på et industriområde, eller i denne type industri tidligere. Imidlertid har jeg jobbet mange år i kriminalomsorgen, og da i anstalter med høy til særlig høy sikkerhet, hvor perimetersikring er en viktig del av den daglige driften. Dette er derfor en type sikring jeg har god kompetanse til å kunne forske på. Samtidig var det viktig for meg at denne kompetansen ikke skulle bli førende for studien, men at den skulle være en viktig erfaring å ha som verktøy for å kunne belyse problemstillingen i studien. Begrunnelsen for dette er at utgangspunktet for nivået på og bakgrunnen for perimetersikring av et fengsel med høy sikkerhet og et industriområde er og skal være forskjellig. Dette gjorde igjen at jeg var bevisst på at mine vante krav til perimetersikring ikke var de samme der jeg skulle for å gjennomføre studien. Derfor var det også viktig for meg å ikke se etter hva jeg mente manglet i perimetersikringen, basert på egne erfaringer, men se perimetersikringen i lys av de kravene, reglene og behovene som Industriområdet har. Men allikevel benytte min kunnskap for å kvalitativt kunne besvare problemstillingen i studien, om påliteligheten til perimetersikringen, sett opp imot Industriområdets føringer.

Selv om jeg aldri har jobbet fast på Industriområdet eller i liknende industri, har jeg kunnskap om Industriområdet, hva som produseres der. Jeg har i en årrekke hatt nære familiemedlemmer og gode bekjente som har jobbet inne på Industriområdet. På den måten har jeg hørt mange historier fra, meninger om og blitt tilført kunnskap om Industriområdet. jeg har på mange måter blitt tilført en forkunnskap jeg ikke har kunnet verifisere selv, annet enn ved å stille spørsmål. Derfor har det vært viktig for meg gjennom denne studien å fokusere på hva jeg nå samler inn av data og se virkeligheten gjennom mine egne oppfattelser og innsamlet data. Samtidig er min ikke verifiserte og tilførte sannhet, noe som kan gi meg en bedre forståelse av hverdagen til de informantene jeg møter og derfor også forstå konteksten og miljøet de arbeider i.

Fra min egen arbeidserfaring har jeg også med meg kunnskap og erfaringer som har vært veldig gode å kunne ha med seg i denne studien. Spesielt min kunnskap om opptak av forklaringer etter uønskede hendelser i kriminalomsorgen. Denne kunnskapen gjør at jeg er vant til å sitte i situasjoner hvor jeg er vant til å tilegne meg informasjon fra andre mennesker gjennom samtaler. Teknikker jeg er vant til å bruke her sammenfaller med teknikker fra aktiv

informantintervjuing, som jeg har beskrevet tidligere i dette kapitlet. Det jeg imidlertid har hatt mest nytte av, er min kompetanse rundt det å kunne ta notater under disse samtalene, men allikevel få med meg og kunne følge opp det som blir sagt. Dette har kommet meget godt med i intervjusituasjonene, hvor jeg har kunnet notere, for så å kunne å kunne transkribere intervjuene i etterkant.

Min kjennskap til Industriområdet fra historier og tilført kunnskap var noe jeg aktivt brukte i den innledende fasen av studien. Jeg var tidlig opptatt av å vise at jeg hadde en kunnskap om deres arbeidsplass og deres hverdag. Samtidig var det viktig for meg å vise min kunnskap om og erfaring med perimetersikring. Jeg var derfor opptatt av å presentere meg på møter og på de arbeidsplassene jeg oppsøkte og skulle observere. Jeg var også nøye med å sørge for at det ble informert i forkant av at jeg møtte opp. Alt dette for å imøtekomme og hindre eller minske kontrolleffekten, beskrevet i Ringdal (2013). Samtidig var det viktig å få frem at studien som problemstillingen sier skulle se på om perimetersikringen rundt Industriområdet var pålitelig, ikke om de som drifter eller operasjonaliserer perimetersikringen gjorde jobben sin. Dette igjen for å imøtekomme, hindre eller minske kontrolleffekten.

3.5 Studiens troverdighet eller interne validitet

Med bakgrunn i opphavet til studien og hvordan det ble besluttet at den skulle skrives, er det viktig for meg at studien har troverdighet og validitet. Det å levere noe med kvalitet, men som også er troverdig ut i miljøet på Industriområdet og som besvarer de spørsmålene som stilles i, vil jo være avgjørende for om studien i ettertid vil være anvendelig for Industriområdet.

«Validitet i kvalitative undersøkelser dreier seg om i hvilken grad forskerens fremgangsmåter og funn på en riktig måte reflekterer formålet med studien og representerer virkeligheten» (Johannesen, Tufte, & Christoffersen, 2016, s. 230).

Lincoln og Guba (1985) beskriver troverdighet ved å fremheve det de mener er fire nøkkelbegreper **troverdighet, overførbarhet, bekreftbarhet og pålitelighet**. For meg som forsker og Industriområdet som forskningsobjekt er det avgjørende at denne studien treffer disse fire begrepene, for at studien og funnene fra denne skal kunne være anvendbare i ettertid. Dersom funnene, studiens innhold og konklusjoner ikke oppfyller noen av disse begrepene vil ikke materialet kunne brukes til å være et grunnlag for en vurdering av Industriområdets perimetersikring. Jeg vil i det følgende utdype disse nøkkelbegrepene knyttet til min studie.

3.5.1 Troverdighet

«The basic issue in relation to trustworthiness is simple: How can an inquirer persuade his or her audience (including self) that the findings of an inquiry are worth paying attention to, worth taking account of? What arguments can be mounted, what criteria invoked, what question asked, that would be persuasive on this issue? » (Lincoln & Guba, 1985, s. 290). For at denne studien skal oppfattes som troverdig er det viktig at det er Industriområdet og informantene herfra som sitter igjen med denne opplevelsen. Er de sitert riktig, fremstiller jeg Industriområdet og konteksten i arbeidsmiljøet og operasjonene på en måte som gjør at informantene kan kjenne seg igjen og ikke har blitt feiltolket eller feilsitert? Er dokumentene som er lagt til grunn i dokumentanalysen relevante for de spørsmålene som stilles i studien?

Studien er i utgangspunktet basert på og bygget rundt intern informasjon fra Industriområdet og ansatte der. Samtidig har det vært viktig for studiens troverdighet å knytte relevant teori som omhandler studiens problemstilling til studien. Studiens problemstilling omhandler påliteligheten til perimetersikringen og for at denne skulle kunne vurderes, ble det valgt å hente inn relevante teoribidrag som kan belyse nettopp perimetersikring. I tillegg ble det tatt inn dokumenter som beviser at brudd på perimetersikring av industriområder kan få alvorlige følger. For selv om denne studien er knyttet til Industriområdet lokalt, er det erfaringer fra andre industriområder som kan være med på å belyse problemstillingen og sette denne i perspektiv. Det har vært viktig for meg i denne delen av studien å ikke la meg påvirke eller styre av egen erfaring og kunnskap rundt perimetersikring av områder, men holde meg konsekvent til relevant teori som omhandler dette.

Siden studien har en så sterk lokal forankring og kun interne informanter, har det vært viktig for meg, fra dag en, og skape et tillitsforhold til ansatte ved Industriområdet. Derfor har jeg hele tiden vært nøye med å grundig informere om hvorfor jeg er der og hva jeg gjør. Det å kunne ufarliggjøre og normalisere min tilstedeværelse i arbeidsmiljøet mener jeg vil øke troverdigheten til studien og informantenes opplevelse av deltakelse i denne. Ved å jobbe på denne måten, ønsket jeg å understreke at studien skulle gjennomføres som en vurdering av påliteligheten til perimetersikringen. Informantenes deltakelse ville være med å gjøre nettopp denne vurderingen, med meg som et verktøy for å sette vurderingen i system.

3.5.1.1. Dokumentanalysens troverdighet

I dokumentanalysen er det lagt til grunn nye dokumenter som belyser trusselvurderinger samt interne dokumenter som belyser studiens problemstilling. Eksempler på dette Statoil sin

rapport «The In Amenas attack» fra 2013, trusselvurderingene fra NSM og PST fra 2022 og artikkelen til Coaffee & Boshier fra 2018. Det er gjort vurderinger av hvilke dokumenter som er relevante for studien. Jeg har landet på trusselvurderinger som sier noe om hva som kan forventes å være trusler mot den type industri som Industriområdet representerer. Dette for å kunne drøfte studiens problemstilling og andre funn i datainnsamlingen opp mot disse trusselvurderingene. Dette vil også kunne si noe om troverdigheten til de vurderingene som blir gjort underveis i studien, da de er begrunnet med nye trusselvurderinger og ikke antakelser eller andre uttalelser.

Dokumentene som er samlet internt fra Industriområdet, beskriver dagens perimetersikring, instruksjoner, operasjonalisering, planer og beredskap rundt denne. Siden jeg som forsker ikke er ansatt ved Industriområdet, hadde jeg, ved oppstart av studien, ingen formening om hvilke dokumenter jeg kunne få innsyn i og tilgang til. Dette var et moment jeg tidlig var klar over kunne bli en utfordring for å gjøre en grundig vurdering av perimetersikringen og som også ville kunne påvirke påliteligheten og troverdigheten til studien. Imidlertid ble ikke dette et moment jeg trengte å bekymre meg for. Jeg har under hele studien fått tilgang til alle dokumenter jeg har bedt om og fått tilgang til alt materiale jeg mener har vært relevant for å kunne gjennomføre studien. Materialet er brukt på en måte som gjør at det ikke er sporbart tilbake til Industriområdet og bruken av disse dokumentene blir derfor ikke ansett å være en sikkerhetsrisiko ved gjengivelse i studien.

3.5.1.2 Intervjuenes troverdighet

Intervjuene i denne studien ble gjennomført som semistrukturerte samtaleintervjuer. Informantene ble i god tid informert om tid og sted og fikk informasjon om hva intervjuet skulle omhandle og muligheten til å se intervjuguiden. Informantene ble rekruttert i samarbeid med HESQ-manager på Industriområdet. På den måten at jeg fortalte hvilke intervjuobjekter jeg ønsket og HESQ-manager satte opp dato og klokkeslett for intervjuene. Alle informantene som ble forespurt å delta i studien ønsket å delta, stilte forberedt til intervjuet og hadde satt av god tid. Ved starten av intervjuene ble det understreket at det var deres svar, refleksjoner, meninger og vurderinger som var viktige å få fram, ikke hva de trodde jeg eller Industriområdet, forventet. Alle informantene mente denne studien var nyttig å gjennomføre for Industriområdet og mente det var viktig å belyse temaet som studien tok opp.

Samtidig kan det stilles spørsmål om troverdigheten til informantene i og med at noen av spørsmålene kan dreie seg mot deres arbeidsutførelse. Allikevel opplever jeg at informantene

hadde en tillit til meg som gjorde at de svarte ærlig og oppriktig ut ifra egen erfaring kompetanse og overbevisning på de spørsmålene som ble stilt. Flere av informantene uttrykte også at dette jo var deres mulighet til å kunne være med å påvirke egen arbeidshverdag og kanskje gjøre denne sikrere. «Deres pålitelighet varierer med holdninger og erfaringer, saker, situasjoner, tidsspenn og institusjonelle sammenhenger» (Andersen, 2006, s. 292). Videre sier Andersen «Psykologisk forskning viser at minne er mest pålitelig når vi spør om forhold som vanligvis pleier å skje, som er godt forstått» (Andersen, 2006, s. 292). Dette siste sitatet fra Andersen (2006) er det som, etter min mening, i denne studien kan være størst grunnlag for å stille spørsmål ved informantenes troverdighet. For enkelte av informantene kan det være lenge siden de har opplevd et brudd på perimetersikringen og svar de gir kan være basert på hendelser fra lang tid tilbake. Allikevel vil dette kunne belyse saken og problemstillingen ved at de da i intervjusituasjonen ble utfordret på om de tror slike hendelser kunne ha skjedd i dag og at deres refleksjon da er med på å belyse problemstillingen allikevel.

3.5.2 Studiens overførbarhet

«How can one determine the extent to which the findings of a particular inquiry have applicability in other contexts or with other subjects (respondents) » (Lincoln & Guba, 1985, s. 290). Selv om denne studien og dens problemstilling er knyttet direkte til Industriområdet, er dette en problemstilling og studie hvor funn fra, eller deler av funn fra problemstillingen eller forskningsspørsmålene, kan ha overførbarhet til andre liknende industriområder eller andre områder med perimetersikring. «En undersøkelses overførbarhet dreier seg om hvorvidt det lykkes en å etablere beskrivelser, begreper, fortolkninger og forklaringer som er nyttige på andre områder enn det som studeres» (Johannesen, Tufte, & Christoffersen, 2016, s. 231).

Underveis i studien søkte jeg etter liknende studier som grunnlag og understøtting for denne studien. Jeg klarte imidlertid ikke å finne noen studier med fokus på perimetersikring av industriområder. Jeg fant imidlertid oppgaver som kunne gi meg inspirasjon i skrivingen, selv om de i seg selv ikke er knyttet opp mot perimetersikringer av industriområder er det allikevel mange likhetstrekk. De fleste oppgavene knytter seg til perimetersikring av sikringsverdige bygninger, bykjerner eller knytter seg tettere opp mot securitykultur begrepet knyttet til sikring. «I forbindelse med bygging av nytt regjeringskvartal skal det etableres et ytre perimeter med ca. 75 meters avstand til bygningene i kvartalet som skal huse departementsfunksjoner og Statsministerens kontor. Perimeteret skal ha til hensikt å hindre at kjøretøybårne trusler får tilgang i nærheten av bygningene» (Jore, Kruke, & Olsen, 2020, s. 3) «Denne studien omhandler sikring av det offentlig byrom mot tilsiktede handlinger. De senere

årene har den vestlige verden blitt utsatt for flere terrorangrep med tunge kjøretøy rettet mot sivilbefolkningen» (Hagerup, 2018, s. iii). «Et endret risikobilde i Norge samt en rekke alvorlige hendelser internasjonalt og nasjonalt, har medført til et økt fokus på sikring og risiko for intenderte uønskede hendelser i petroleumssektoren og samfunnet for øvrig» (Larsen & Østensjø, 2015, s. I). «However, perimeter intrusion detection (PID), which is one of the major tasks in visual surveillance, still needs to be formally defined. A perimeter intrusion detection system (PIDS) aims to detect the presence of an unauthorized object in a protected outdoor site during a certain time» (Lohani, et al., 2022, s. 1) «Security countermeasures are the steps taken to strengthen the weak points in a system, either by lessening vulnerabilities or by hardening the facilities. Various security countermeasures are suggested for improving security of CPI» (Gupta & Bajpaj, 2007). Som man ser, er ingen av disse bidragene direkte knyttet til perimetersikring av industriområder, men gir allikevel nyttige og gode innspill til denne oppgavens problemstilling

Min erfaring og kompetanse rundt perimetersikring sier meg at begrepene i denne studien er begreper som enkelt er overførbare til andre. Legger man til grunn at dokumenter og teorier benyttet i undersøkelsen er tilgjengelige for alle og begrepene er vanlige innenfor arbeid med perimetersikring, vil jeg si denne studien er overførbar. Når man i tillegg legger til grunn at det ikke har lyktes meg i å finne tidligere forskning rundt emnet, vil dette kanskje gjøre studien både interessant og anvendbar for liknende industriområder som det denne oppgaven er skrevet rundt. Samtidig er det spesifikke data fra deltagende observasjoner, intervjuer og dokumentstudier som retter seg spesifikt mot dette området. Disse dataene er på mange måter kontekstspesifikke og derfor ikke direkte overførbare.

Det er viktig for andre, som ønsker å bruke denne studien, å ta hensyn til at innsamlet data er spesialisert til Industriområdet. «Det vil være umulig for en annen forsker å duplisere en annen kvalitativ forskers forskning» (Johannesen, Tufte, & Christoffersen, 2016, s. 229). Basert på dette sitatet er det viktig at andre som ønsker å benytte funn, drøftinger eller konklusjoner, knytter dette til egen kontekst, parametere og variabler.

3.5.3 Studiens bekræftbarhet

«Det er viktig at funnene er et resultat av forskningen og ikke et resultat av forskerens subjektive holdninger. Bekræftbarhet skal sikre dette. Begrepet viser til i hvilken grad resultatene fra den kvalitative undersøkelsen kan bekreftes av andre forskere gjennom tilsvarende undersøkelser.» (Johannesen, Tufte, & Christoffersen, 2016, s. 232). Denne

studien har et eksplorativt forskningsdesign, noe som vil si at det ikke er gjort tidligere forskning på studiens problemstilling. Det vil igjen si at studien ikke vil, kunne bekreftes gjennom andre forskeres arbeid. Bekreftelse av denne studien vil derfor måtte gjøres gjennom at Industriområdet og informantene gjenkjenner sine bidrag og kan se disse i sammenheng med innhentet teori, dokumenter, drøftinger og konklusjoner. «The role of the auditor is to make the inspection and verification on behalf of the reader and to attest to having done so» (Lincoln & Guba, 1985, s. 326). Min forståelse av dette, som forsker, er at det er min rolle å sørge for at leseren forstår at studien er bekreftet ved å sette de forskjellige delene opp mot hverandre. I tillegg til at bidrag fra teorien og innsamlet data er tilgjengelige også for lesere som ønsker å verifisere innholdet i disse bidragene.

Basert på at studiens innhold, teorier og dokumenter er søkbare og tilgjengelig for leseren, vil denne studien være bekreftbar.

3.5.4 Studiens pålitelighet (reliabilitet)

«Reliability is typically held to be, in the words of Kerlinger (1973, p. 422) synonymous with “dependability, stability, consistency, predictability, accuracy.” Having described a “reliable man” as one whose behavior is consistent, dependable, and predictable, Kerlinger (1973, p. 443) goes on to say. » (Lincoln & Guba, 1985, s. 292). Siden denne studien har en eksplorativ design, vil påliteligheten til hvordan studien er gjennomført og hvordan data er innhentet og behandlet avgjøre studiens reliabilitet. «Reliabilitet knytter seg til undersøkelsens data: hvilke data som brukes, hvordan de samles inn, og hvordan de bearbeides» (Johannesen, Tufte, & Christoffersen, 2016, s. 229). At informanter og andre ansatte på Industriområdet kjenner seg igjen i det som blir gjengitt, hvordan det er tolket og ser sammenhengen i drøftinger og konklusjonen vil være viktige bidrag til å gi denne studien pålitelighet. «Credibility is a trustworthiness criterion that is satisfied when source respondents agree to honor the reconstructions; that fact should also satisfy the consumer» (Lincoln & Guba, 1985, s. 329).

Jeg vil si at denne studien er gjennomført med høy grad av pålitelighet. Benyttet teori og dokumenter er av nyere dato. Informantene har alle stilt opp etter egen vilje og ønske og innehar alle relevante roller og arbeidsoppgaver knyttet til studiet. Underveis i studiet har jeg som forsker, alltid, blitt inkludert i de settingene jeg har deltatt. Dette være seg øvelser, under observasjoner eller på møter. Selv om jeg har stilt spørsmål og kommet med ytringer under observasjoner, som kan ha virket kontrollerende og intervjuende, har ikke dette ført til at jeg har måttet jobbe for å vedlikeholde påliteligheten underveis i studien. Dette vitner om at

ansatte, informanter og andre deltakere i disse settingene har hatt tiltro til meg som forsker. Informanter har uttalt en opplevelse av at jeg har opptrådt med legitimitet og ærlighet i forhold til studiens innhold og dens problemstilling. Informantene sier alle, de føler de har blitt tatt på alvor og at deres rette meninger og uttalelser har kommet med i studien.

3.6 Etske hensyn knyttet til studien.

«Etske problemstillinger oppstår når forskningen direkte berører mennesker, spesielt ved datainnsamlingen, enten den foregår gjennom deltakende observasjon, intervjuer eller eksperimenter» (Johannesen, Tuft, & Christoffersen, 2016, s. 84). Denne studien berører mennesker på deres arbeidsplass og deres meninger, svar og observasjoner. Det er viktig for meg som forsker at svar, meninger og observasjoner ikke kan spores tilbake til informantene eller andre ansatte. I forkant av studien kontaktet jeg Norsk senter for Forskningsdata (NSD) for å undersøke hvilke retningslinjer som ligger til grunn for å utføre en slik studie som denne.

I dette tilfellet ønsket jeg å gjennomføre en studie hvor ikke personopplysninger kom til å bli lagret. Jeg bestemte meg for at jeg hadde kompetanse til å kunne notere ned intervjuer for hånd og at derved ingen personopplysninger eller lydopptak av informanter, eller andre ansatte, ville ligge lagret elektronisk. Det ble meldt tilbake fra saksbehandler i NSD at min studie ikke var meldepliktig (Norsk senter for Forskningsdata, 2022).

Samtidig er studien av en slik art at det ville vært etisk utfordrende å ikke anonymisere hvilket industriområde det er snakk om, på grunn av at det tas opp en del sikkerhetsmessige utfordringer som kunne ført til uønskede hendelser dersom de kom åpent frem.

3.7 Styrker og svakheter ved studien

Stryker ved denne studien er tilgangen til forskningsmateriale. All dokumentasjon jeg har bedt om har blitt lagt frem, uten unntak. Jeg har fått tilgang til materiale som ikke er direkte knyttet til studien, men som allikevel er med på å belyse problemstillingen. En annen styrke er alle ansatte og informanters ønske om å delta, komme med sine meninger, refleksjoner og diskusjoner rundt studiens problemstilling og forskningsspørsmål. Samtidig er min personlige kunnskap om perimetersikring en styrke. Jeg vet hva som skal til for å ha en tett perimetersikring og vet hvordan en slik perimetersikring må driftes, vedlikeholdes og organiseres.

Samtidig kan min kunnskap om perimetersikring være en svakhet med denne studien, sammen med min mangel av inngående kjennskap til Industriområdet. Det at jeg ikke kjenner

Industriområdet inngående kan innvirke på hva jeg tenker er en god perimetersikring. Min forforståelse av perimetersikring kan her bli en svakhet ved studien, da jeg, basert på mine preferanser om perimetersikring kan sette kravene til Industriområdets perimetersikring for høyt. For å motvirke dette hadde jeg i starten av studien flere samtaler med HESQ-manager for å kartlegge hvilke krav og dimensjonering Industriområdet satte og ønsket og sette til perimetersikringen. Jeg har videre i studien holdt meg til disse kravene og den dimensjoneringen som var føringen fra starten av. Denne tilpasningen vil jeg si har vært en styrke for studien.

Styrker og svakheter ved studien samlet sett vil jeg si at det er flere styrker enn svakheter knyttet til denne studien.

4. Empiri

I dette kapitlet vil funn fra egen forskning i studien presenteres. Kapitlet deles inn i de forskjellige delene av forskningen og systematiseres under hvert punkt med studiens forskningsspørsmål som overskrifter. Del 1 av kapitlet omhandler dokumentanalysen. Her blir funn fra studier av relevante dokumenter presentert. Dette er interne dokumenter fra Industriområdet samt andre dokumenter som ikke er skrevet direkte om Industriområdet men allikevel er relevante for studien. Del to er funn fra intervjuer av ansatte på Industriområdet som har deltatt som informanter i semistrukturerte intervjuer. Del tre er funn fra deltakende observasjoner. Hva jeg som forsker har observert under de settingene jeg har vært deltakende observatør. Del fire er funn fra samtaler under deltakende observasjoner. Ansatte som har uttalt seg i samtaler underveis som også kan sammenliknes med aktiv informantintervjuing. Dette er samtaler som har kommet til ved at jeg har vist interesse for deres arbeid og arbeidsoppgaver. I disse samtaleene har de vist, forklart og diskutert sine arbeidsoppgaver knyttet mot studien. For å strukturere presentasjonen vil det systematiseres ved å knyttes opp til studiens forskningsspørsmål og deles inn i de ulike underkategoriene på hvert punkt. Funnene fra kapitlet, vil sammen med teoriene fra teorikapitlet danne grunnlaget for drøftingen i kapittel 5.

4.1 Dokumentanalysen

4.1.1 Hva slags barrierer etableres for å ivareta perimetersikringen av Industriområdet?

«Et tilstrekkelig sikkerhetsnivå avhenger av at virksomheter oppdaterer sin kunnskap, blir mer sikkerhetsbevisste og tilpasser sikkerhetstiltak etter endringer i trusselbildet» (Sikkerhetsmyndighet, 2022, s. 29). Dokumentasjon fra Industriområdet viser at det ikke er gjort endringer i den ytre perimetersikringen ved nye etableringer inne på Industriområdet, selv om disse er etableringer som kan være av stor interesse for andre aktører.

Industriområdet har tre forskjellige sikkerhetsnivåer knyttet til forskjellige nivåer av trusselbilde. Disse tre nivåene beskriver forskjellige tiltak knyttet til perimetersikringen og systemet rundt denne. Nivå 1 beskriver perimetersikringen ved normal drift, nivå 2 og 3 beskriver begrenset adgang til Industriområdet ved stenging av kjøreporter og slusing av all trafikk via Havneport. Imidlertid er det ingen beskrivelser av andre barrierer som er knyttet til stenging av portene, noe som utføres elektronisk.

Det finnes fra risikovurderinger gode beskrivelser av hendelser som kan skje inne på Industriområdet, men det er ikke beskrevet hvordan disse kan hindres av perimetersikringen. Nevnt som tiltak mot disse hendelsene står «Fabrikkgjerd, overvåking av gjerd og porter og innpasseringskontroll» som de eneste tre punktene knyttet spesifikt til perimetersikringen. Likevel fremkommer det av dokumentene at det er godt risikovurdert knyttet til hendelser og omfanget av disse, men perimetersikringen og tiltak rundt denne tas ikke eksplisitt inn som tiltak for å hindre eller stanse disse hendelsene.

«Sårbarheter kan oppstå når flere virksomheter deler ansvaret for sikkerheten, der man legger andres risikovurderinger til grunn eller der man antar at sikkerheten blir ivaretatt av andre» (Sikkerhetsmyndighet, 2022, s. 33). Det kommer frem av dokumenter at Industriområdet deler opp operasjonaliseringen av perimetersikringen mellom to forskjellige anbudsgivere fra april 2022. Dette er en praksis som er motstridende til hva NSM anbefaler i sin rapport. NSM (2022) sier videre i sin rapport «For det første øker gapet mellom trusselen og sikkerhetsnivået i norske virksomheter og samfunnsfunksjoner. Det skyldes blant annet at bevisstheten og kompetansen om trussel- og risikobildet og hva som utgjør god nok sikkerhet er for svak. Sikkerhetstiltakene er ikke dimensjonert for det reelle trusselbildet, eller innføres ikke raskt nok når nye sårbarheter oppstår» (s. 8).

Det som imidlertid har blitt tatt inn som tiltak, er overfallsalarm i Hovedresepsjon, Havneport og Vaktentral. Da studien ble gjennomført, var begge disse tiltakene på plass som en sikring og dette er derfor ikke tatt med som et behov for forbedring i denne studien.

Risikovurderingen hvor dette er beskrevet er knyttet tilbake til 2019. Dette er risikovurderingen lagt frem for studien som den gjeldende risikovurderingen for disse forholdene.

I beredskapsplanverket, datert 2022, er det klare og tydelige varslingsrutiner for tilsiktede hendelser/sabotasjer/ terror/kriminelle handlinger eller mistanke om dette. Ved slike hendelser gjennomføres varslings direkte til politi, men det beskrives ikke en definert innsats fra industrivernet knyttet til slike hendelser. De hendelsene der det er rutinebeskrivelser for industrivernutrykning er knyttet til safety-hendelser inne på Industriområdet.

4.1.2 Hva truer påliteligheten til dagens perimetersikring?

I nasjonal trusselvurdering 2022 fra PST, står det «Norsk næringsliv og norske kunnskapsmiljøer vil oppleve fordekte anskaffelsesforsøk fra aktører involvert i militær modernisering og opprusting. Aktører knyttet til Russland, Kina, Iran og Pakistan vil

representere en særskilt utfordring» (Nasjonal trusselvurdering, 2022, s. 4). Inne på Industriområdet finnes det teknologi som vil kunne være interessant for slike aktører. Videre sier PST (2022) «Teknologi utviklet for et sivilt formål kan også være viktig for utviklingen og produksjonen av masseødeleggelsesvåpen, deres leveringsmidler og konvensjonelle våpen- og overvåkingssystemer. Det er etter hvert svært mye sivil teknologi som også kan brukes til militære formål» (Nasjonal trusselvurdering, 2022, s. 11). Nasjonal Sikkerhetsmyndighet (2022), viser i sin rapport «Risiko 2022» til eksempelet med forsøket på russisk oppkjøp av Bergen Engines som et eksempel på det NSM beskriver i sin trusselvurdering. Regjeringen stoppet dette oppkjøpet med hjemmel i sikkerhetsloven. «Beslutningen kom blant annet som følge av at teknologien ved Bergen Engines ville styrket Russlands militære kapasitet og gitt Russland viktig militærstrategisk kunnskap og teknologi» (Sikkerhetsmyndighet, 2022, s. 15)

Funn fra interne dokumenter på Industriområdet viser at gjeldende krav til perimetersikringen er adgangskontroll av personell og kjøretøy. Det er også et krav at det skal være et fabrikkgjærde med porter for kjøretøy, gående og syklende. Det skal også være en overvåking av gjerdene, portene og det skal være en innpasseringskontroll i perimetersikringen. Alle ansatte skal også bære adgangskort synlig, slik at identifisering skal kunne gjøres enkelt.

Interne rutiner viser krav til kontrollrunder og kontroll av perimetersikringen. Denne skal gjennomføres hver tredje uke. I tillegg skal det foretas ukentlig sjekk av innpassering og kontroll av adgangskort for personell og kjøretøy. Ved uregelmessigheter bortvises personell og kjøretøy. Disse kontrollene utføres en gang per uke på forskjellige adgangspunkt inn til Industriområdet. Det er industriberedskapen som gjennomfører disse kontrollene.

Analyse av dokumentene viser at kravet til perimetersikringen er å hindre uvedkommende personer og kjøretøy adgang til Industriområdets arealer gjennom et fungerende industrigjærde, adgangskontroll og overvåking av perimeteret. Hendelser som er risikovurdert er lastebiler med sprengstoff som detonerer under rørgater eller lastebiler eller andre store maskiner som kjører inn i rørgater. Det er også risikovurdert anslag mot hovedresepsjonen med gisseltaking. Tiltak til dette er beskrevet i beredskapsplanverket.

Det overordnede kravet til perimetersikringen, som kommer frem gjennom dokumentanalysen, er å hindre uvedkommende adgang til Industriområdets arealer.

4.1.3 Hvordan er informasjonsflyten blant samvirkerne som opprettholder barrierene i perimetersikringen rundt Industriområdet?

Informasjonsflyten på Industriområdet knyttet til hendelser er meget god. Det er klare tydelige rutiner, kanaler og avvikssystemer som er godt innarbeidet i Industriområdet og alle lokasjoner innenfor perimetersikringen. Det som kommer frem fra analysen av dokumenter og dokumentasjon rundt enkelte hendelser, er at det er en grundig og god informasjonsflyt mellom alle relevante parter som knytter seg til opprettholdelse av perimetersikringen.

Det man imidlertid ser er at det ved nyetableringer ikke alltid tas hensyn til perimetersikringen. Lokasjon, bygningsmasse og produksjon plasseres på steder hvor det ikke ville vært normalt med slike plasseringer dersom man hadde tatt hensyn til perimetersikringen. Dersom informasjonsflyten i forkant av slike hendelser hadde vært bedre,

4.1.4 Funn fra annen dokumentasjon rundt perimetersikring

«En godt utformet perimeter- og områdesikring vil derfor kunne bidra til å vinne tid og samtidig skape forutsetninger for egne aktive mottiltak. Det er imidlertid viktig å være oppmerksom på at fysiske sikringstiltak i perimeteret ofte har en svært begrenset tidsforsinkende effekt for en kompetent angriper. Det er derfor viktig med elektroniske tiltak for å detektere og verifisere inntrengning, samt å verifisere hendelsen for det reaksjonsapparatet som finnes.» (Nasjonalt kompetansesenter for sikring av bygg, 2022, s. 103).

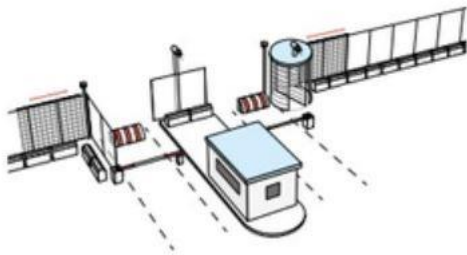
Forsvarsbygg (2022) er mer konkret rettet mot tiltak og barrierer, Sikringshåndboka viser til konkrete barrierer og tiltak knyttet til flere metoder, mål og sikringstiltak. «gjerder holder normalt kun ærlige individer ute og er derfor best egnet til å markere en juridisk grense, med mindre det dimensjoneres mot forsering» (Nasjonalt kompetansesenter for sikring av bygg, 2022, s. 104). Forslag til og eksempler på barrierer som blir trukket frem i boka knyttet til perimetersikring er adgangskontroll, videoovervåkning, bevegelsesdeteksjon og fysiske sperrer.

Et tiltak som nevnes er kjøretøysperrer, aktive eller passive. Passive kjøretøysperrer er for eksempel bokstavene vist fra Emirates stadium i figur 8 tidligere i oppgaven,



Figur 16: Bilde av Emirates stadium II (Coaffee & Bosher, 2008, s. 79)

«Det beste tiltaket mot trusselen fra kjøretøy er passive kjøretøysperrer, for eksempel faste installasjoner forankret i bakken rundt hele objektet, men vanligvis må det etableres inn-/og utpaseringsområde(r) med aktive kjøretøysperrer» (Nasjonalt kompetansesenter for sikring av bygg, 2022, s. 121).



Figur 17: Kjøretøysperrer (Nasjonalt kompetansesenter for sikring av bygg, 2022, s. 109)

Kjøretøysperrer som vist i figuren over er aktive sperrer som kan heves og dermed bli en aktiv barriere i perimetersikringen, ved for eksempel forhøyet trusselnivå. Videre sier Sikringshåndboka at slike barrierer ikke må vurderes isolert, men tas med som en del av en integrert sikkerhetsløsning sammen med andre tiltak.

Et eksempel på en slik integrert sikkerhetsløsning beskrives på følgende måte «Det opprettes et perimetersikringssystem. Det blir programmert inn soner for de ulike områdene rundt perimeteren. Ved alarm på et av deteksjonssystemene, for eksempel på sone 2, vil et kamera snu seg mot sone 2, starte et opptak av hendelsen, og avslutte opptaket 60 sekunder etter at alarmstatus er normal igjen. Dette vil presenteres i vakt på «pop-up»-skjerm med alarm.

Hendelser linkes også sammen i databaselogg.» (Nasjonalt kompetansesenter for sikring av bygg, 2022, s. 191)

Sikringshåndboka viser til operatører som viktige «briller» i en perimetersikring. «En operatør som ivaretar et sikkerhetsanlegg er i aller høyeste grad en primærfunksjon, og det må utformes og fasiliteres deretter. Det innebærer at dersom operatøren har andre arbeidsoppgaver, skal ikke synsvinkelen endres nevneverdig under de ulike operasjonene» (Nasjonalt kompetansesenter for sikring av bygg, 2022, s. 187). Det pekes videre på at arbeid i alarmmottak kan være stressende og at det er viktig at personellet der er trent for og blir rekruttert i urohold til de oppgavene som skal løses. «Personellet må også være forberedt på at de vil oppleve situasjoner som ikke har noen klar og forutbestemt rutine. Med tilstrekkelig øvelse og erfaring bør medarbeiderne ha godt nok grunnlag til både å foreslå og iverksette tiltak» (Nasjonalt kompetansesenter for sikring av bygg, 2022, s. 200)

4.1.4.1 Funn fra rapporten «The In Amenas attack»

I rapporten «The In Amenas attack» (Statoil, 2013) som er granskingsrapporten etter terrorangrepet mot Statoils lokasjon i In Amenas Algerie kommer granskingsgruppen frem til noen konklusjoner og anbefalinger basert på sin rapport. Fritt etter rapporten er det de følgende hovedkonklusjoner som ble trukket i rapporten:

Summen av ytre og indre sikringstiltak klarte ikke å hindre skade på personer.

Sikringstiltakene var ikke dimensjonert for et så alvorlig angrep, og var basert på hjelp fra Algerisk militære.

Hverken Statoil eller samvirket rundt sikringen av anlegget kunne hindret angrepet fra å skje, men det er grunn til å stille spørsmål ved tilliten til beskyttelsen fra det Algeriske militære, ingen regnet med en stor terrorstyrke som skulle angripe anlegget.

Statoil har et etablert risikostyringssystem, men organisasjonens totale kapabilitet og kultur må styrkes for å kunne reagere på sikkerhetsrisiko under operasjoner i fiendtlige og komplekse miljøer.

Et annet interessant funn knyttet til risiko og risikostyring er følgende «i de fleste tilfeller er security en liten del av en større og bredere helse, miljø og sikkerhets stilling og få mennesker i slike stillinger har erfaring og ekspertise på security. Som et resultat av dette har Statoil en ineffektiv fulltids ressurs av spesialister på security» (Statoil, 2013, s. 5).

Basert på disse hovedfunnene og rapporten kom granskingsgruppen med totalt 19 anbefalinger knyttet til områdene Organisasjon og kapasitet, risikostyringssystemer, beredskap og respons og samarbeid og nettverk. (Statoil, 2013, s. 76).

4.2. Intervjuer

4.2.1 Hva slags barrierer etableres for å ivareta perimetersikringen av Industriområdet?

Informantene svarer her alle sammen gjerder, kameraer og adgangskontroll. Samtidig nevner de fleste informantene bemanning i vaktentral, havneport og hovedresepsjon som en del av systemet og barrierene i perimetersikringen. Og at de som bemanner disse funksjonene har en viktig rolle for å holde kontroll med og operere perimetersikringen. 8 av 11 informanter sa at inntrengning på Industriområdets arealer oppdages og oppfattes via kameraovervåkning fra vaktentral. Informantene 3, 4 og 5 sier imidlertid at det er helt tilfeldig om slik inntrengning ville ha blitt oppdaget.

Når det gjelder systemer og barrierer som iverksettes viser alle informantene til industriberedskapen, som det systemet eller barrieren som ivaretar perimetersikringen ved hendelser. Det å varsle beredskapen ved hendelser er noe som ligger nært framme i reaksjonsmønsteret til alle informantene da det ble spurt om system og barrierer. Informanter som jobber i og mot beredskapen svarte også at de rykker ut til meldinger om svikt i eller brudd på perimetersikringen. «Ved brudd i perimetersikringen, rykker vi ut for å observere skaden. Dersom vi kan reparere skaden, gjør vi det der og da. Hvis ikke, melder vi inn til Industriområdet og holder eventuelt vakt til noen kommer for å reparere skaden» (Informant 1). Informant 2 sa følgende: «Hvis noen prøver å ta seg ulovlig inn, eller prøver å true seg inn i området, prater vi rolig med vedkommende, utløser stillealarm, og prøver å holde stand til beredskapen kommer og tar over situasjonen».

Informasjonen som kom frem under intervjuene er ganske entydige. Perimetersikringen med barrierene skal sikre at ikke uønsket eller uautorisert personell og eller kjøretøy får adgang til Industriområdets arealer. Samtidig svarer informantene at det er forventet at perimetersikringen er i fungerende stand. Informant 1 sa at det blir kjørt jevnlig kontroll hvor hele perimetersikringen ble kontrollert, hver 3. tirsdag. I tillegg til dette sa informant at det ble gjennomført ukentlige stikkontroller på adgangskort, både til bil og personer. Dersom det blir oppdaget feil ved adgangskortene blir bil og eller person nektet adgang til Industriområdet. Informant 4 sa det ikke tenkes så mye på det i hverdagen, men at «noen

ansatte synes det er vel rigid i porten noen ganger, når man må ut å stemple når man er to i bilen. Synes det er unødvendig å måtte gå ut». Informant 2 sier adgangsreglene inn i Industriområdet oppleves som klare og tydelige. Det er tydelige regler på at uautorisert personell eller andre personer uten avtale vises bort. Informanten sa også at det oppleves at de som opererer perimetersikringen vil reagere ved mistenkelig adferd, da de er blitt ganske trent på dette og se personer som opptrer unormalt.

Informant 11 sa det oppleves et større fokus på perimetersikring nå enn tidligere i forhold til personell inn på Industriområdet. Tidligere kunne man melde opp besøk og de kunne gå inn til rett lokasjon. «Nå må besøkende hentes i vaktentral, havneport eller hovedresepsjon og følges inne på området» (Informant 11).

Informantene 3, 5, 6 og 8 sa at ved forhøyet beredskapsnivå ved Industriområdet blir kjøreporter inn til arealet, bortsett fra havneport, stengt og låst av. All trafikk ledes da ned til bemannet Havneport, som da kontrollerer alle som skal inn på Industriområdet, både adgangskort og kjøretøytillatelse. Informant 5 fulgte opp denne informasjonen med å understreke at avlåsing av kjøreportene var eneste barrieren som ble iverksatt ved forhøyet beredskapsnivå.

4.2.2 Hva truer påliteligheten til dagens perimetersikring?

Når det gjelder om perimetersikringens pålitelighet imøtekommer leietakeres krav er det imidlertid bare en informant som mener det er samsvar mellom disse. En informant svarer «Nei. Tror ikke leietakere vet hvor dårlig det er» (Informant 5). Informant 8 samsvarte med dette og sa: «Overhodet ikke. Det er ikke så sikkert som det ser ut». Andre informanter sa at flere av leietakerne har egne perimetersikringer og adgangskontroller inn i egne installasjoner og lokasjoner inne på Industriområdet. Det kommer tydelig fram at fokuset for hva som er en trussel varierer mellom informantene, allikevel er tankene rundt hva som er de største truslene mot Industriområdet unisone og dreier seg om to ting. Fem informanter hevder at et anslag mot Hovedtanken på området er den største trusselen, samtidig sier de at et slikt angrep ikke vil kunne stoppes med perimetersikringen, da dette angrepet må komme via luften, mens fem informanter hevder at det er anslag mot rørgatene inne på Industriområdet som er den største trusselen. En informant hevder det er et anslag mot Industriområdets vanntårn som er den største trusselen. Funnene varierer veldig på hvilke trusler som kan ramme Industriområdet. Ut ifra svarene ser man også at dette varierer med hvilken rolle og funksjon de forskjellige informantene har.

Informantene peker alle på at de mener det er enkelt å ta seg inn på området gjennom dagens perimetersikring. Alle informantene sier de med en kraftig avbitertang kunne ha klippet seg inn gjennom industrigjerdet og enkelt fått adgang til Industriområdet. Fem av informantene peker også på at det ikke er kameradekning rundt hele perimeteret, men at det er flere steder rundt perimeteret hvor det ikke er kameradekning. Fire informanter sier også at det ikke er bevegelsessensorer på kameraene rundt perimetersikringen, noe som gjør at vaktcentralen ikke får opp alarm ved bevegelse inn mot gjerdet. Informantene 3, 4 og 5 sier helhetlig kameradekning med bevegelsessensorer ville vært et tiltak som ville hevet påliteligheten til perimetersikringen. De begrunner dette med at de da ville ha fått varsel når personer nærmet seg perimetersikringen, mens nå, er man avhengige av å se disse personene på skjermene. «Jeg tror det er enklest på dagtid, for da forsvinner de i mengden. Vi har ikke tid til å følge med» (Informant 5). Dersom fokuset er på en annen arbeidsoppgave, eller de ikke ser på den aktuelle skjermen, vil de ikke få med seg om noen forsøker å ta seg inn gjennom perimetersikringen.

Alle elleve informantene hevder det er enkelt å ta seg inn gjennom dagens perimetersikring hvis man ønsker det. Syv informanter hevder at «tailing», er enkleste måten å ta seg inn på. Det vil si at man kjører inn etter en annen bil, når denne har registrert seg inn på lovlig vis, ved å benytte seg av tregheten i lukkingen av portene. Fire informanter hevder de ville ha gått inn helt normalt, sammen med mange andre. «De som kommer inn her gjør det ved å låne eller ved å ha skaffet seg adgangskort, og slik kommer seg inn på «lovlig» vis» (informant 1). 4 informanter peker på svakheten ved at det ikke er fysiske barrierer som stenger ved kjøreporter under hevet sikkerhetsnivå på Industriområdet. Informantene sier det burde ha kommet fysiske barrierer, roadblockers, som ekstra barrierer i tillegg til portene ved forhøyet sikringsnivå på Industriområdet. De fire informantene peker på at selv om kjøreportene blir låst, er de fortsatt like sårbare for kjøretøy som kjører inn i dem og dermed ville ha kommet gjennom perimetersikringen.

Informant 2 peker på at alle besøkende kan komme tett innpå personell i hovedresepsjonen som en risiko og en trussel mot perimetersikringen. «Ustabile sinna mennesker kan komme helt inntil oss uten noe annet enn skranken som hinder» (Informant 2). Informanten hevder dette i verste fall kan føre til trussel eller gisselsituasjoner hvor ansatte kan utsettes for fare. Informanten sier videre at selv om de har en alarmknapp de kan trykke på og ved det utløse en stillealarm til Industrivernet, er det ikke sikkert at dette er tilstrekkelig til å kunne hindre en alvorlig situasjon. Informant 5 hevder noe som kan sammenliknes med informant 2 sine

oppfatninger knyttet til vaktentral, «Det burde vært mulighet for calling og postkasse for avlevering av kort og annet utstyr, slik at ingen uautoriserte, fysisk, behøver å komme inn i vaktentral etter klokken 16:00». Informant 5 begrunner utsagnet med sårbarheten til vaktentralen dersom noen ønsker å utføre et anslag mot Industriområdet. Informant 5 underbygger forrige utsagn med følgende scenario ved en trusselsituasjon. «En kjedereaksjon, hvor man først angriper vaktentralen, som er operatøren for Industriområdets varslings- og alarmanlegg, for så å jobbe seg videre inn i Industriområdet, med sikkerhet om at ingen hendelser ville ha blitt varslet eller meldt videre, siden vaktentralen var satt ut av spill». Informant 5 peker på at det for en tid tilbake ble fjernet en kjørebom, noe som nå gir besøkende med bil, fri tilgang til området foran både hovedresepsjon og vaktentral. Med henvisninger til tidligere gjennomførte terrorangrep i Norge, mener både informantene 2, 3, 5 og 6 at demonteringen av denne bommen har svekket perimetersikringen, ved å gjøre vaktentral og hovedresepsjon mer tilgjengelige for kjøretøy.

6 informanter peker på adgangskontrollen til Industriområdet som en trussel mot påliteligheten til perimetersikringen. De sier man må bruke adgangskort for å registrere seg inn i området og at dette fungerer tilfredsstillende. Imidlertid peker de på at man ikke må registrere seg ut, som en mulig trussel mot Industriområdet. Det at man kan registrere seg inn og egentlig forbli inne i lang tid uten at dette merkes, mener flere informanter er en trussel mot sikkerheten. Informantene sier uønskede personer kan oppholde seg inne i området og ha god tid til å planlegge, forberede og gjennomføre aksjoner. Samtidig peker 2 informanter på at det i forhold til ulykker inne på området ville vært nyttig med en slik registrering ut av området, da man ville vite hvem som til enhver tid var inne på området og hvem man skulle lete etter ved en eventuell hendelse med evakuering. Informant 11 sier hans firma har egne inn- og utregistreringsrutiner ved hans lokasjon nettopp for å vite hvem som er på lokasjonen ved en ulykke eller hendelse. Informanten sier han er kjent med flere andre lokasjoner som har liknende interne systemer for adgangskontroll. Dette mener informanten er et signal på at kanskje Industriområdet burde hatt en slik ordning. Samtidig peker 3 av informantene på at i Industriområdets sikkerhetskurs, er det lite fokus på perimetersikringen og brudd mot denne. De mener at et større fokus på hva som skjer og hvilke følger eller konsekvenser brudd på perimetersikringen får av følger, ville kanskje ha øket bevisstheten rundt perimetersikringen hos alle som gjennomfører disse kursene.

7 av informantene peker også på at de ikke ser en helhetlig tankegang blant lokasjonene og Industriområdet når det gjelder syn på og viktigheten av perimetersikringen. Noen mener at

det er nok at perimetersikringen er et hinder, mens andre mener at det burde vært en mer sikker barriere mot inntrengning på Industriområdets arealer. I fortsettelse av dette sier 8 av informantene at de ikke opplever at det blir tatt hensyn til perimetersikringen ved nyetableringer inne på Industriområdet, men at det er behov for areal og tilgjengelighet som er styrende. «Nå har det akkurat kommet opp en vaskehall inntil industrigjerdet som hindrer og skygger for kameradekningen i det området. Den etableringen er en svekkelse av mine kontrollmuligheter» (Informant 5). I tillegg, sier informant 5, vil etableringer med høy interesse for vinningskriminelle, med synlig profilering, være en ekstra trussel mot perimetersikringen dersom disse etableringene blir lagt tett inntil gjerdetraséen. Samtidig stiller 2 av informantene spørsmål rundt nyetableringer på området, men utenfor perimetersikringen. Dette er etablering med høyt risikopotensiale, men på grunn av kravet til tilgjengelighet, ligger det på utsiden av perimetersikringen.

4.2.3 Hvordan er informasjonsflyten blant samvirkerne som opprettholder barrierene i perimetersikringen rundt Industriområdet?

Alle informantene er samstemte om at informasjonsflyten rundt perimetersikringen er kjent, tydelig og god. Informasjonen som alle 11 informantene gir på dette punktet vitner om at informasjonsflyt, rapporteringsrutiner og kanaler er godt kjent og at det på Industriområdet er en god rapporteringskultur ved hendelser.

Alle informantene er samstemte rundt til hvem, når og hvordan de skal melde uregelmessigheter eller brudd. Det er tydelige varslingsrutiner med kjente nummer og instanser som skal varsles. 6 av informantene begrunner dette med at gode varslingsrutiner er viktig for sikkerheten inne på industriområdet. Ikke bare til Industriområdet, men også for deres egen personlige sikkerhet. Derfor mener de at disse rutinene er gode og sitter langt fremme i alle ansattes bevissthet. 2 av informantene mener at det burde vært et enklere 4 sifferet nummer som nødnummer, som ville vært enklere å huske, men at nummeret man har i dag fungerer tilfredsstillende.

4.3. Deltakende observasjoner

Underveis i studien har jeg gjennomført mange observasjoner. Jeg har møtt opp presentert meg og forklart hva jeg gjør og hvorfor jeg er der som observatør. Under disse observasjonene har jeg forsøkt å holde meg i bakgrunnen for ikke å bli involvert og dermed kunne observere det som skjer. Dette har under studien vist seg umulig å gjennomføre. Uansett hvilken setting jeg har deltatt ved, har jeg blitt enten spurt om min mening eller om

jeg har synspunkter på det som utføres eller det som skjer. Jeg fant derfor fort ut at i denne studien snakker vi om deltakende observasjoner. Disse deltakende observasjonene ga meg følgende funn i løpet av studien.

4.3.1 Hva slags barrierer etableres for å ivareta perimetersikringen av Industriområdet?

Industrigrunde, adgangskontroll, kontrollrunder, stikkkontroller ved oppmøte og kameraovervåking er systemene og barrierene som blir observert knyttet til perimetersikringen. I tillegg til dette viser operatør i vaktentral, havneport og hovedresepsjon at de har en knapp under skrivebordsplaten som utløser en stille alarm. Denne alarmen utløser en utrykning fra Industriberedskapen.

Observasjoner gjort under studien viser at barrierene i perimetersikringen skal hindre at uønskede eller uautoriserte personer og/eller kjøretøy får tilgang til Industriområdets arealer. Ansvaret for drift, vedlikehold og reparasjoner ligger på Industriområdet selv, med sine underleverandører. I perimetersikringen ligger også driften og operasjonaliseringen av vaktentral, havneport og hovedresepsjon inne som barrierer som skal klare å hindre uønsket eller uautoriserte personer eller kjøretøy denne adgangen. Disse tjenestepostene og da spesielt vaktentralen virker å ha en avgjørende rolle i påliteligheten til perimetersikringen.

Perimetersikringen følger Industriområdets tre nivåer for beredskap, med dertil forhøyede nivåer av sikring. Ved en oppgradering til sikringsnivå 2 vil kjøreporter i perimetersikringen bortsett fra havneporten bli låst. All biltrafikk vil da bli ledet gjennom havneporten.

Havneporten er bemannet og sjekker adgangskort og kjøretillatelse. Denne avlåsningen skjer ved at styringsmodulen til portene deaktiveres dette må gjøres digitalt, denne avstengingen kan ikke gjennomføres fra vaktentral, men må gjennomføres av en underleverandør, som må kontaktes. Det er ingen andre barrierer annet enn deaktivering av styringsenhet som skiller de tre nivåene for sikring av portene. Portene blir ikke låst med fysisk lås, og det er ikke noen form for roadblockers som aktiveres.

I kravet til perimetersikringen ligger også adgangskontrollen til Industriområdet. Kravene til denne kontrollen er at alle som skal inn på området må scanne seg inn med eget adgangskort. Dette adgangskortet får man gjennom å gjennomføre Industriområdets sikkerhetskurs i fire deler. Ved endt sikkerhetskurs må man bestå en godkjenningsprøve. I dette kruset blir det gitt en kort gjennomgang av hva som skjer dersom man forsøker å komme seg inn på Industriområdet uten gyldig adgangskort, låne andres kort for å komme seg inn eller låne bort

eget kort til andre. Man blir opplyst om at dette kan føre til bortvisning fra Industriområdet og inndragelse av adgangsgodkjenning. Man kan på den måten hevde at dette kurset også er en del av kravet til Industriområdets perimetersikring. Kravet til adgangskontroll gjelder kun innpassering til Industriområdet. Det er ingen krav om at ansatte skal registrere seg ut. Dette kravet ligger imidlertid til kjøretøy, hvor disse må registrere seg ut av Industriområdets arealer. Industrieredskaper gjennomfører ukentlige kontroller ved innpassering for å kontrollere adgangskort både for bil og personell. Dersom det oppdages uregelmessigheter, vil personell og eller biler med personell bli bortvist fra industriområdet og godkjenninger kan bli inndratt. Ved kontroll utført under observasjon til denne studien ble det ikke funnet uregelmessigheter ved innpassering.

Enkelte bygninger er bygget inn i gjerde traséen og er på denne måten en del av perimetersikringen. I disse byggene er det egne adgangskontroller og man kan ikke gå igjennom byggene og ut på Industriområdets arealer uten å registrere seg inn gjennom disse adgangskontrollene. I tillegg er enkelte av dem forsterket med kameraovervåking og eller bemannet. Det observeres at disse punktene mest sannsynlig er de sterkeste punktene i hele perimetersikringen og de punktene det er minst sannsynlig at det kommer til å skje brudd.

En av de mest overraskende observasjonene jeg gjorde, var at jeg ikke kunne se noen barrierer i perimetersikringen. Selv om man hever trusselnivået, kommer det ingen nye barrierer inn i perimetersikringen. Det at man låser portene ved hevet trusselnivå er jo ikke i seg selv en barriere, for portene er de samme og det er ingen ekstra sikring rundt disse. Det vil si at det er like enkelt, eller det trengs ikke noe ekstra utstyr for å forsere en port, uansett hvilket trusselnivå Industriområdet er satt i. Det blir ikke satt inn noen form for roadblockers eller annen form for fysisk sperre ved forhøyet trusselnivå. I tillegg til dette er det på en vei fritt å kjøre helt inntil bygningsmassen hvor både hovedresepsjonen og vaktentralen ligger. Her kommer det heller ingen barrierer eller stengsler ved forhøyet trusselnivå. Samtidig observerte jeg også at operatørene i vaktentralen er kun en på jobb av gangen og har mange andre arbeidsoppgaver enn det å observere og operasjonalisere perimetersikringen. I tillegg observerte jeg at det ikke er fullstendig kameradekning rundt hele perimetersikringen og det går ikke an å kjøre en sjekk av perimetersikringen digitalt, man må fysisk kjøre kontroller for å se at alt er intakt. Kameraene er heller ikke utstyrt med bevegelsessensorer, noe som vil si at dersom operatøren er opptatt med andre oppgaver, vil vedkommende ikke kunne oppdage et eventuelt angrep mot eller brudd i perimetersikringen og er på den måten avhengig av at noen

ser og varsler om dette. Det observeres også at deler av perimetersikringen er dårlig opplyst, noe som forverrer operatørens oppgaver på kveld og nattestid.

4.3.2 Hva truer påliteligheten til dagens perimetersikring?

Under studien viser det seg at det bare er delvis kameradekning rundt perimetersikringen. Dette gjør at utsagnene om at forsøk på inntrengning ikke vil kunne bli oppdaget i disse dødsone gir mening. For å kunne observere dette valgte jeg å være til stede i vaktentralen både på formiddag, ettermiddag og kveld. Man kan tydelig observere at arbeidsforholdene til operatøren i vaktentralen og muligheten for å kunne observere via kamera forverres med tiltagende mørke. Etter mørkets frembrudd er det flere plasser av gjerdetraséen man ikke klarer å se med kamera. Dette vil si at kameraovervåking som barriere ikke fungerer etter mørkets frembrudd. Noe som igjen viser at det er industrigjerdet med porter, som er den egentlige perimetersikringen, uten andre barrierer som fanger opp brudd eller inntrengningsforsøk. Samtidig ligger det bygninger inntil perimetersikringen som skygger for kameradekkingen på enkelte områder rundt perimetersikringen. Noe som igjen gjør det vanskelig for operatørene i vaktentralen å holde øye med hele perimetersikringen også på dagtid.

En annen observasjon som gjøres er at spesielt operatørene i vaktentralen har andre oppgaver knyttet til sin tjenestepost, som gjør at de ikke har mulighet til å observere monitorene som dekker kameraovervåkingen av perimetersikringen kontinuerlig. Dette er oppgaver som utstedelse av adgangskort, kjøretøytilatelse, utlån og mottak av verneutstyr og mottak av besøkende. Dette er arbeidsoppgaver som ikke kan gjøres samtidig med at fokus på overvåkingsskjermene opprettholdes. I tillegg har også vaktentralen et stort ansvar ved safety hendelser inne på Industriområdet. Vaktentralen er alarmmottak og videreformidler og sender videre alarmer ved hendelser. Alt dette drives med kun en operatør på vakt av gangen. Noe som igjen betyr at man ikke har mulighet til å holde fokus på overvåking av perimetersikringen og inntrengning kan skje uten at dette blir oppdaget.

Også kjøreportene oppleves under observasjonen som en trussel mot Industriområdets perimetersikring. Her observeres at lukketiden på portene er så lang at det er mulighet for flere kjøretøy og personer å komme seg inn i området etter at et kjøretøy på lovlig vis registrerer seg og kjører inn. Dette omtales som «tailing» av operatører og andre ansatte. Under observasjon i vaktentral ble en bil observert kjørende minst 200 meter inn på Industriområdet før porten var lukket til den grad at ingen andre kunne komme seg inn. Selv

om man ved normal drift vil kunne oppdage «tailing» via kameraovervåking, vil man ikke trenge store distraksjoner eller gjennomføring av andre arbeidsoppgaver hos operatør før noen kunne ha «tailet» denne bilen og kommet seg inn på Industriområdet.

Under intervjuer kom det frem at man anså tilstedeværelsen av ansatte og deres overvåkenhet nesten som en del av perimetersikringen. Det ble sagt at man regnet med at ansatte ville reagere dersom man så personer som tok seg inn, gikk rundt eller gjorde ulovligheter inne på Industriområdet. Under studien, som en del av observasjonen, deltok jeg som markør på en øvelse for nettopp å se om jeg ble konfrontert ved å bevege meg rundt inne på Industriområdet. Øvelsen gikk på at jeg skulle forsøke å ta bilder og forsøke å aksessere områder med fotoforbud og begrenset adgang. Jeg hadde kledd meg i arbeidsklær liknende vanlige ansatte og hadde med meg personlig verneutstyr. Under denne øvelsen gikk jeg rundt inne på Industriområdet og tok bilder med mobilkamera og jeg klarte sammen med øvingsleder å ta meg inn på forbudt område uten påkrevd utstyr. Alt dette uten at jeg ble tilsnakkert eller konfrontert av andre ansatte. For meg viser dette at om noen kommer seg inn på Industriområdet, kan de komme ganske langt og oppholde seg inne på området i lang tid uten å bli oppdaget. Noe som igjen kan gi rette personene god tid til å gjennomføre aksjoner eller annet inne på Industriområdet. Som en ansatt sa i en samtale «en morgen som noen kom på jobb, møtte de en person med fallskjerm som hadde hoppet fra den høyeste bygningen inne på området her. Personen løp fra den ansatte og kom seg ut av området uten å bli identifisert eller stoppet». Dette viser jo at det er mulig å komme seg usett inn og få tilgang til området.

En annen observasjon i så måte er at man i adgangskontrollsystemet har registrering inn, men ikke ut av Industriområdet for personell. Utregistrering er kun for sjåfører av kjøretøy. Under samtale med ansatte mener noen at dette er en mangel i adgangssystemet og burde vært endret. Mest av alt knyttes dette til at man ved hendelser på Industriområdet raskt hadde kunne oppdage hvem som var inne på området og hvor mange som skulle evakueres ved en hendelse. Samtidig ville man kunne ha sett dersom noen hadde kommet seg inn med stjålet kort og ikke forlot området. Flere av lokasjonene inne på Industriområdet har en slik kontroll, altså at personer må registrere seg både inn og ut av lokasjonen. Disse begrunner det nettopp med å ha kontroll på hvem som er inne ved en hendelse, hvem som da må evakueres eller letes etter. Å innføre en slik kontroll også ved utgang fra Industriområdet ville ha gitt muligheten til samme kontroll med personer ved hendelser her, i tillegg til å se om personell forble på området i mistenkelig lang tid. Dette er jo ikke nødvendigvis tegn på at en uønsket

security hendelse var i ferd med å skje, men det kunne jo også være med på å oppdage ulykker eller medisinske illebefinnender hos personell som arbeider alene.

Noe som også observeres er at det ikke er gjort nevneverdige oppgraderinger av perimetersikringen de siste ti år. Selv om det har kommet vesentlig mer industri og vesentlige mer banebrytende teknologi inn på området, noe ev det verdensledende teknologi, er det ikke gjort oppgraderinger av perimetersikringen. For min del er dette oppsiktsvekkende at man ikke oppgraderer og oppjusterer perimetersikringen i takt med mengden teknologi og kvaliteten på denne. Det er soleklart at en del av den produksjonen og teknologien som er inne på Industriområdet i dag både er av stor sivil og militær verdi og interesse. Men hvorfor gjenspeiler ikke dette seg i en satsning på og oppgradering av perimetersikringen?

Industriområdet har kun en stilling som dekker hendelser knytte til både security og safety hendelser. Dette virker som en meget stor arbeidsbyrde for en person. Faren ved dette er at en av områdene blir lidende under det andre. Observasjoner viser at man på Industriområdet har stor kunnskap om og stort fokus på safety-hendelser. Man har et industrivern som er drillet på disse typene hendelser og øvelser som blir avholdt handler i stor grad, nesten utelukkende om safety-hendelser og hvordan håndtere disse. Ved å ha ansatte som var dedikert mot safety og security med klare delte ansvarsområder ville kanskje fokuset på security hendelser også blitt hevet. Kanskje ville dette ført til at øvelser også automatisk fikk innhold av security elementer i tillegg til safety-momentene som ligger der i dag.

4.3.3 Hvordan er informasjonsflyten blant samvirkerne som opprettholder barrierene i perimetersikringen rundt Industriområdet?

Observasjoner under studien og samtaler med ansatte vitner om at informasjonsflyten blant samvirkerne som opprettholder barrierene i perimetersikringen rundt industriområdet er god. Det er klare og tydelige meldingsrutiner og tydelige føringer for hvor, hvem og hva som skal rapporteres.

Industriområdet har egne systemer for avviksrapporing og dette virker tydelig kommunisert, samtidig er det tydelig at systemet blir benyttet. De ansatte jeg snakket med under observasjonene var tydelige på at de kjente til rutiner og hvem som skulle kontaktes, knyttet til forskjellige typer hendelser og avvik. Samtidig kom det også fram i samtaler at de følte innrapporterte saker og hendelser ble tatt tak i den grad det var mulig med de midler og budsjetter som var til rådighet. En ansatt sa følgende: «Viktigste er at vi føler at vi kan si ifra

og at vi får en tilbakemelding som i hvert fall forteller oss at noen har sett det vi melder om, oppleves bra. Hvis ikke, hadde vi jo ikke giddi og meldt om saker».

Opplysninger gitt under observasjonene gikk også på at ved rapporterte hendelser knyttet til perimetersikringen ble disse raskt tatt tak i og fikset. Det var vaktordninger som gjorde at dersom man meldte feil på porter, gjerder eller kameraer, ble dette fikset fort, uten unødvendig vente - og nedetid.

4.4. Samtaler under deltakende observasjoner

Under deltakende observasjoner underveis i studien hadde jeg flere samtaler med ansatte på Industriområdet. Jeg hadde samtaler med 17 ansatte under disse observasjonene. Dette er ansatte som ikke var tiltenkt en rolle som informanter i studien, da det ikke ville vært praktisk mulig å intervju dem alle sammen, allikevel hadde de jeg møtte, kunnskap om hvorfor jeg var der og at jeg skrev en masteroppgave. Derfor er heller ikke disse informantene registrert i oversikten av informanter i tabellen i metodekapittelet. Jeg fikk mye god informasjon ut av disse samtalene. Dette var uformelle samtaler som ble holdt over en kaffekopp eller i forbindelse med at jeg spurte de ansatte om deres arbeidsoppgaver og hvordan de så på egen arbeidshverdag. Andre samtaler kom til ved at jeg bare var til stede i rommet og ansatte begynte å fortelle meg om sine oppgaver knyttet til min oppgave. Samtalene i seg selv kan sammenliknes med aktive informantintervjuer. Det som slo meg var at ansatte var veldig interesserte i å dele sine meninger med meg, og det som gikk igjen var at de håpet oppgaven ville føre til at det ble satt fokus på perimetersikringen. Alle jeg snakket meg under disse samtalene ga meg tillatelse til å bruke informasjonen jeg fikk inn i oppgaven min.

Videre har jeg delt inn informasjonen jeg fikk og knyttet den til oppgavens forskningsspørsmål.

4.4.1 Hva slags barrierer etableres for å ivareta perimetersikringen av Industriområdet?

Informantene hevder barrierene som etableres i perimetersikringen er adgangskontroll, ved innpassering. Samtidig sier flere av dem de opplever denne som strengere enn før fordi de nå, for eksempel, ikke kan sitte på som passasjer i bil gjennom perimetersikringen. De må fysisk ut av bilen og registrere eget adgangskort ved innpassering. Det kommer også frem at alle informantene har opplevd å bli stoppet i kontroll ved innpassering, flere ganger siste år, ved at industriberedskapen har hatt kontroller av adgangskort. En annen barriere to stykker nevner er sikkerhetskursene som må gjennomføres for å få adgang til Industriområdet og at dette i seg

selv er en barriere i perimetersikringen. Det at man får informasjon om hva som skjer dersom man ikke overholder interne lover og regler ved Industriområdet og hva som er sanksjonene ved brudd, mener disse to er en barriere i systemet i seg selv.

Alle informantene jeg snakket med, sa at dagens perimetersikring hovedsakelig er til for å holde uvedkommende ute av Industriområdet. Imidlertid mente alle at det er fullt mulig å ta seg ubemerket inn på området om de ville det. Alle jeg har snakket med har kommet med metoder og steder rundt perimetersikringen de mener ville gjort at de ville ha kommet seg ubemerket inn på området. Samtidig sier flere av informantene at barrierene i perimetersikringen er de samme i dag som de alltid har vært. Det har ikke, som de vet om, kommet flere barrierer eller andre barrierer de seneste årene, selv om det nå er industri og teknologi inne på området som er mye mer verdifullt enn det var tidligere.

Noen informanter stiller også spørsmål hvorfor ikke det er krav til registrering av adgangskontroll på vei ut av området, men bare inn. De begrunner dette med sikkerhet og det å til enhver tid kunne ha oversikt over hvor mange ansatte det befinner seg inne på området. Dette knyttet til uønskede hendelser, både av safety og security art, og vite hvor mange og hvem som må evakueres, eventuelt etterlyses på området ved alvorlige hendelser. Enkelte av informantene hevder det ikke registreres utpasseringer, fordi fagforeningene på Industriområdet mener dette blir en overvåking av ansatte. Dette er et syn informantene ikke deler, fordi de hevder det ville vært sikkerhetsmessig bedre å ha oversikt og at dette sikkerhetsaspektet veier tyngre enn synspunktet rundt overvåking. En registrering av utpassering ville vært til alles beste og informantene mener dette burde ha vært et krav til perimetersikringen.

Alle informantene jeg snakket med nevner også kameraovervåkingen som en viktig del av perimetersikringen. Det at det er kameraer rundt området gir operatørene mulighet til å se uregelmessigheter rundt perimetersikringen, og dermed kan varsle dersom noen prøver å ta seg inn på Industriområdet. En informant sa at en viktig barriere han så ved perimetersikringen, var at utearealene på Industriområdet var så pene og velstelte. Beplantning og gressplener er alltid velholdt. Dette mente informanten i seg selv var en barriere fordi «Når folk ser at det er så velstelt rundt om på området regner de sikkert med at alt annet er på stell også. Det i seg selv gir en avskrekkende effekt i forhold til å skulle forsøke å bryte seg inn her.». Informanten mente imidlertid at dette ikke var tanken rundt uteområdene, men allikevel mente han at dette hadde en virkning.

Noen av informantene jeg snakket med hevdet at selv om sikkerheten på Industriområdet opplevdes som god, kunne de ikke peke på barrierer som kom i tillegg til perimetersikringen ved oppjustert trusselnivå på Industriområdet. Informantene var kjent med at det var tre nivåer for sikring av Industriområdet, men at det ikke kom inn ekstra barrierer ved opphøyd nivå, annet enn at kjøreporter ble låst. Informantene påpekte at det burde være ekstra barrierer ved opphøyde nivåer. Tre av informantene tok frem roadblockers som en mulig barriere de mente burde være et nivå ved kjøreportene ved forhøyet trusselnivå. Med dagens perimetersikring opplevde ikke informantene at det var en forhøyet sikring ved forhøyet trusselbilde, da portene var like sårbare uten tilleggsbarrierer som ved normalt trusselnivå.

4.4.2 Hva truer påliteligheten til dagens perimetersikring?

Informantene kom med flere interessante opplysninger som studien ellers ikke ville ha avdekket. Tre av informantene fortalte at det for en tid tilbake var fjernet en bom i området opp mot vaktentral og hovedresepsjon dette gjør at man nå fritt kan komme helt inntil bygningsmassene hvor både vaktentralen og hovedresepsjonen ligger. Den ene informanten sa følgende om dette «Vi så jo alle, 22. juli i regjeringskvartalet, hva en bil på feil sted full av sprengstoff kan utrette og selv om det her skal være sikkert, så vet jeg vel ikke helt». Informantene hevdet at fjerningen av denne bommen, svekket perimetersikringen, da man nå kunne ta seg helt opp til bygningene med bil uten å legitimere seg først. Samtidig pekte informantene på at det ikke lot seg gjøre å stenge av portene i perimetersikringen fra vaktentralen. Dette måtte gjøres av de som drifter perimetersikringen. Informantene mente at det ved forhøyet trusselnivå eller andre typer hendelser burde være mulig for vaktentralen å stenge av kjøreportene og med det stenge ned perimetersikringen. De sa videre at det burde kunne gjøres ved å taste inn en kode og gjøres digitalt. De anså at denne muligheten ikke fantes som en risiko ved store hendelser i området og anså da muligheten for inntrenging som mulig.

En annen informasjon som kom frem, var at enkelte av informantene ikke syntes det var heldig at besøkende kunne komme inn i bygget ved vaktentralen etter Industriområdets normale åpningstid. Åpningstid definerte de med den tiden dagtidsansatte var på jobb. De forklarte at besøkende og innleid personell kom inn til luka i vaktentralen for å levere utlånt sikkerhetsutstyr eller ved andre henvendelser. Tre av informantene mente at det burde vært en form for calling på utsiden av bygget som gjorde at personell ikke trengte inn i bygget, men kunne snakke med vaktentralen via calling. Utlånt utstyr mente de kunne legges i en kasse eller liknende på utsiden, slik at operatøren kunne sende noen ut for å hente dette når det ikke

var andre til stede. De mente det kunne bli en svekkelse av perimetersikringen når operatør i vaktcentralen ble eksponert for ukjent og uidentifisert personell etter åpningstiden. Samtidig pekte fire av informantene på at ordningen med at det er vaktcentralen som produserer adgangskort. Alle som skal ha adgangskort får dette ved henvendelse i vaktcentralen. Dette er en arbeidsoppgave som tar fokus bort fra operasjonaliseringen av perimetersikringen fordi operatøren, som er alene i vaktcentralen må fokusere på andre arbeidsoppgaver enn å følge med på perimetersikringen. I sammenheng med dette påpekte to av informantene at det heller ikke er bevegelsessensorer på kameraovervåkingen, noe som gjør at hvis de ikke følger med på kameraene hele tiden, vil de heller ikke se om noen forsøker å trenge inn gjennom perimetersikringen. Dette, påpekte to informanter, gjelder også hvis noen prøver å følge etter en bil inn på området gjennom kjøreportene, som er fullt mulig, fordi portene bruker lang tid på å lukke seg etter innkjøring. Fire av informantene mente at ved å ha bevegelsessensorer på kameraene ville de kunne hatt mye bedre kontroll på perimetersikringen enn i dag, fordi de ville blitt varslet når noe eller noen kom inn mot perimetersikringen.

Et siste moment som kom frem var seks av informantene som mente at splittingen av operasjonaliseringen av perimetersikringen ikke var heldig for den helhetlige perimetersikringen og driften av denne. Før var dette samlet under et operatørselskap, men dette skulle 01.04.22 bli operasjonalisert av to selskaper. Informantene uttrykte bekymring for at å samarbeide rundt operasjonaliseringen kunne komme til å skape unødvendige utfordringer og dette kunne komme til å svekke perimetersikringen. De begrunnet dette med at nytt firma ikke hadde kompetanse på vakthold og sikring og at de ikke normalt sett hadde denne typen arbeid i sin portefølje. De var også redd for at den helhetlige oversikten av perimetersikringen ville forsvinne. nå kunne de følge hele perimetersikringen og hadde naturlige møteplasser med alle som jobbet med perimetersikringen, mens etter 01.04.22 visste de ikke hvordan dette samarbeidet skulle foregå. Ville de ha tilgang til hverandres rapporter om brudd eller ville dette tilføre en utfordring med deling av dokumentasjon og annen viktig informasjon de nå naturlig hadde tilgang til siden de var under samme firma.

4.4.3 Hvordan er informasjonsflyten blant samvirkerne som opprettholder barrierene i perimetersikringen rundt Industriområdet?

Samtalene som ble gjennomført under deltakende observasjon avdekte at alle informantene var fornøyde og tilfredse med informasjonsflyten rundt perimetersikringen. Samtidig fremholdt fire av dem bekymringen rundt hvordan dette kom til å bli etter 01.04.22. Hvordan vil informasjonsflyten bli når to forskjellige firmaer skal jobbe med samme perimetersikring?

Rapporterer de samme brudd, har de samme nivå for rapportering og ser og vektlegger de samme typer brudd? Samtidig sa en annen informant at så lenge man klarte å samarbeide nå, ville man vel klare å samarbeide 01.04.22 også. Som informanten påpekte «det er Industriområdet som bestiller en drift og operasjonalisering av perimetersikringen, så da må jo alle som jobber med perimetersikringen ha fokus i forhold til den bestillingen».

Bortsett ifra denne bekymringen om samarbeid, mente alle informantene at informasjonsflyten blant samvirkerne som opprettholder barrierene i perimetersikringen var god. Informantene sa det var tydelige informasjonslinjer og tjenesteveier som informasjonen skulle følge og det var tydelige ansvarsforhold og gjennom dette også klart til hvem og når brudd og eller uønskede hendelser skulle varsles. Informantene opplevde også rask respons og handling ved innmeldt brudd eller hendelser. Tre informanter påpekte imidlertid at de opplevde sen respons på innsendte forslag rundt endringer eller forbedringer i perimetersikringen, uten at de kunne gi noen svar på hvorfor. Alle tre ga imidlertid uttrykk for at dette i noen tilfeller kunne virke demotiverende i forhold til jobben de utførte. Selv om forslagene ikke kunne tas til følge, ønsket de allikevel en bekreftelse på at forslaget var blitt mottatt.

4.5. Oppsummering empiri

Innsamling av data gjennom dokumenter, intervjuer, deltakende observasjoner og samtaler under deltakende observasjoner har gitt meg mye kunnskap og innsikt i Industriområdet og den delen av organisasjonen som operasjonaliserer og drifter jobben rundt perimetersikringen. Bredden av innsamlet materiale har vært meget viktig for å kunne belyse og se problemstillingen i studien i lys av meninger, dokumenter vurderinger og føringer.

Dokumentanalysen ga et innblikk i hvordan Industriområdet anser sikkerheten og hvordan de vurderer denne opp imot perimetersikringen. Samtidig sa det også noe om vektingen og fokuset på security kontra safety hendelser. Hva er det som blir vektlagt i Industriområdets dokumentasjon og hva ligger til grunn i deres risikovurderinger. Ved å sette dette opp mot annen relevant dokumentasjon, fant jeg hvordan andre tenker og ser på perimetersikring, utforming og dimensjonering. Funn rundt hva som nasjonalt blir sett på som trusler mot industri og produksjonsanlegg var også interessante funn satt opp imot interne dokumenter fra Industriområdet.

Intervjuene ga meg et perspektiv på hvordan ansatte anså perimetersikringen i sitt daglige virke. Det å få uttalelser fra ansatte som jobber med, operasjonaliserer, leder og blir sikret av

perimetersikringen ga interessante funn opp imot dokumentanalysen. Det å høre hva de ansatte legger vekt på og om dette samsvarer med vurderingene i og funnene fra dokumentene, både interne og relevante eksterne.

Deltakende observasjoner og samtale underveis i disse ga meg enda flere funn knyttet til den rent praktiske driften og operasjonaliseringen av perimetersikringen. Observasjonene jeg gjorde meg, rundt perimetersikringen, dimensjoneringen, tilhørende barrierer, operasjonaliseringen og arbeidet med drift og vedlikehold ga meg mange interessante funn. Samtidig ble dette utfyllt med gode faglige diskusjoner med ansatte som jobber med perimetersikringen eller har stillinger knyttet til denne. Diskusjoner som belyste funn fra dokumenter, teorier, observasjoner og intervjuer og satte disse i et praktisk perspektiv knyttet direkte til perimetersikringen og dens pålitelighet.

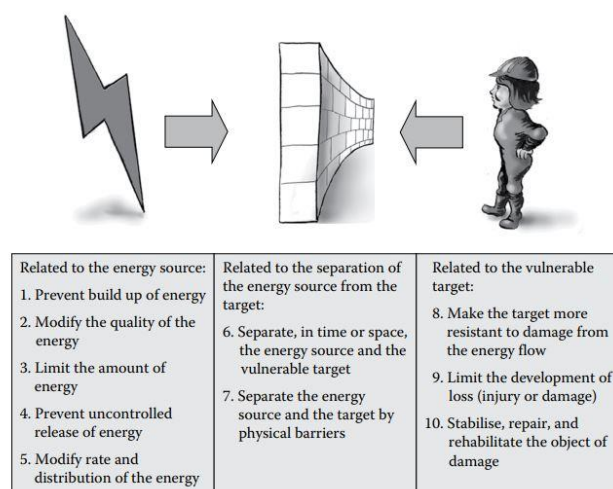
Funnene fra empirien vil nå bli tatt med videre inn i kapittel fem og drøftet opp imot teoriene som ble beskrevet i kapittel to

5. Drøfting

I dette kapitlet vil jeg drøfte funn fra empirikapitlet ved hjelp av det teoretiske rammeverket i kapittel 2, knyttet til studiens problemstilling og forskningsspørsmålene. Jeg vil problematisere noen av funnene og diskutere dette opp imot funn og på den måten belyse studiens problemstilling. I kapitlet vil forskningsspørsmålene utgjøre grunnlaget for de første underkapitlene og oppsummeringen av kapitlet vil gjøres ved å sammenfatte disse fire underkapitlene i et siste femte, med problemstillingen for studien som overskrift. Resultatet av drøftingen vil jeg sammenfatte og de viktigste funnene presenteres i konklusjonen i kapittel seks.

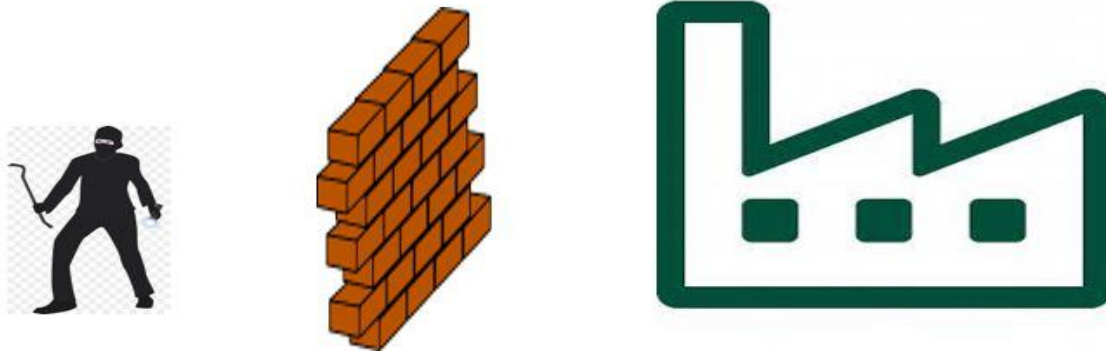
5.1 Hva slags barrierer etableres for å ivareta perimetersikringen?

Haddon (1980) beskriver i sin barrieremodell, barrierer som noe som skiller et sårbart objekt fra en energikilde, som en murvegg mellom energikilden og det sårbare objektet. Modellen er grundigere beskrevet i kapittel 2.5.1, figur 7.



Figur 17: Haddon's 10 accident prevention strategies. (Adapted from Haddon, W., *Hazard Prev.*, 16, 8-12, 1980) (Kjellen & Albrechtsen, 2017, s. 25)

Haddons modell viser overordnede barrierer. «Strategy No. 4, prevention of uncontrolled release of energy, is the primary approach in many cases and includes a large array of measures» (Kjellen & Albrechtsen, 2017, s. 35). Sett i sammenheng med perimetersikring vil Haddons modell si at uautorisert personell og kjøretøy skal hindres adgang til Industriområdet. Uautorisert personell og kjøretøy sees som energien i modellen, murveggen sees som perimetersikringen og målet sees på som verdiene inne på Industriområdet man ønsker å skjerme. Dette kan visualiseres med følgende modell.



Figur 18: Eksemplifisering av barrierenes formål

Industriområdets tre sikringsnivåer kan sees på som en barriere i Haddons modell. Dette ved at de viser til et overordnet sikkerhetsnivå, basert på et trusselbilde som fører til at flere tiltak må settes i verk for å oppnå ønsket sikkerhetsnivå.

Når vi snakker barrierer innenfor sikkerhet snakker vi om security delen av sikkerhetsbegrepet. «Security betyr å sikre seg mot tilsiktede uønskede handlinger» (Stranden, 2019, s. 32). Barrierene som beskrives videre i dette kapittelet vil være knyttet til security og sikring mot uønskede hendelser.

For å kunne si noe om hvilke barrierer som etableres må jeg definere hva barrierer er. Oxford English Dictionary (OED 2005) definerer ordet barriere slik «Fence of material obstruction of any kind erected (or serving) to bar the advance of persons or things, or to prevent access to a place». «Safety barriers are physical and/or non-physical means planned to prevent, control or mitigate undesired events or accidents. » (Sklet, 2006, s. 496). Alle informantene i studien nevner gjerder, kameraer og adgangskontroll som barrierer i perimetersikringen av Industriområdet. Samtidig nevner de fleste også bemanning i vaktentral, havneport og hovedresepsjon som barrierer i perimetersikringen. Reason (2016) deler videre barrierer inn i to hoveddeler. Den første er **Harde**, som i tekniske installasjoner, alarmer, gjerder, låser nøkler osv. Den andre er **Myke**, som Reason (2016) beskriver som en kombinasjon mellom pairer og mennesker. Eksempler på myke barrierer er prosedyrer, regelverk, arbeidstillatelser, operatører osv. Hegde (2015) viser til barrierer i tre deler som del av en sikring; Barriersystem, Barrierefunksjon og Barriereelementer. Disse tre delene sier noe om hvordan barrierene er satt i system, hvordan de skal fungere og hvilke elementer som er satt sammen for at systemet skal fungere som ønsket. Alle tre delene kan inneholde både harde og myke barrierer. Sett i forhold til perimetersikringen av Industriområdet, kan man bruke vaktentralen som et eksempel som inneholder både myke og harde barrierer. Som

barriereelementer har man prosedyrer, lover, regler og operatører som myke barrierer, samtidig som man har kameraovervåking, alarmer, og bygningsmasse som holder uautorisert personell ute, som harde barrierer. Vaktcentralens barriererefunksjon er å overvåke perimetersikringen og varsle og eller utløse alarm ved anslag eller unormaliteter. På denne måten ser man vaktcentralen som et barriereelement, med sin barriererefunksjon inn i barrieresystemet perimetersikringen. «Hvis noen prøver å komme seg inn på området, utløser vi alarm og eller tilkaller beredskapen som rykker ut. Vi forsøker å holde vedkommende person eller kjøretøy under oppsyn med kamera» (Informant 5). Stranden refererer til barrierer som tiltak. Barrierer og tiltak kan også defineres inn under disse tre. Sikringstrekløveret deler sikring inn i tre deler, Menneskelig, Teknologisk og Organisatorisk. Menneskelige barrierer: Handlinger som operatører utfører i forbindelse med perimetersikringen. Operatørens persepsjon, situasjonsoppfattelse og beslutningstaking. Teknologiske barrierer: Gjerder, porter, bygninger og dører. Stranden kaller disse passive eller «dumme» tiltak. Stranden (2019) sier videre at de teknologiske barrierene er avhengige av Menneskelig og Organisatoriske for å ha en effekt. Organisatoriske tiltak: Plan- og instruksverk som beskriver drift, organisering og operasjonalisering av Industriområdets sikkerhet og perimetersikring. Videre i kapittelet vil jeg vise hvilke barrierer jeg avdekte under studien og sette disse i sammenheng med teorier og modeller knyttet til barrierer.

«A barrier system may consist of several barrier elements, and the elements may be of different types (e.g. Technical, operational, human, and software)» (Sklet, 2006, s. 496) Hvilke barriereelementer finnes det i barrieresystemet perimetersikringen av Industriområdet og hvilke barriererefunksjoner har de i dette barrieresystemet? Underveis i studien har jeg avdekket følgende barriereelementer i Industriområdets perimetersikring. **Industrigjerdet med porter, Adgangskontroll, Sikkerhetskurs, Kameraovervåking, Døgnbemannet vaktentral, Hovedresepsjonen og Industriberedskapen.** Videre i dette underkapittelet vil jeg beskrive de forskjellige barrierene opp imot teori og empiri.

5.1.1 Industrigjerdet med porter

«Det finnes mange typer gjerder for ulike formål. Noen ganger er hensikten med et gjerde bare å markere en juridisk grense, mens i andre sammenhenger er hensikten å hindre noen adgang» (Stranden, 2019, s. 142). Informantene i denne studien er ganske entydige om at perimetersikringen rundt Industriområdet skal sikre at ikke uønsket eller uautorisert personell og eller kjøretøy får adgang til Industriområdets arealer. På den måten svarer dette ut hva Stranden (2019) skriver om sikring og barrierer.

«Gjerder holder normalt kun ærlige individer ute» (Nasjonalt kompetansesenter for sikring av bygg, 2022, s. 104). Gjerder og porter er det som per i dag er den synlige delen av perimetersikringen rundt Industriområdet. Men er de der kun for å holde ærlige individer ute? Er det ikke slik at Industriområdet forventer gjerdet skal være en fungerende perimetersikring? Barrierefunksjonen til gjerdene i perimetersikringen, gjør at de vil være betegnet som en hard barriere, hvis man trekker linjene tilbake til Reason (2016). «Safety barriers have been used to protect humans and property from enemies and natural hazards since the origin of human beings» (Sklet, 2006, s. 494). Gjerdet i perimetersikringen er det, man ut ifra Sklet (2006) sin teori, kan kalle et barriereelement i perimetersikringen som barrieresystemet. «En godt utformet perimeter- og områdesikring vil derfor kunne bidra til å vinne tid og samtidig skape forutsetninger for egne tiltak» (Nasjonalt kompetansesenter for sikring av bygg, 2022, s. 103). Forsvarsbygg (2022) viser til en godt utformet perimetersikring som en barriere for inntrenging. Perimetersikringen rundt Industriområdet har tre sikkerhetsnivåer knyttet til sikring. Dette er basert på trusselvurderinger og operasjonaliseres fra vaktentralen etter ordre fra ledelsen på Industriområdet. Samtaler under deltakende observasjon forteller meg hvordan dette virker. Ved forhøyet sikkerhetsnivå stenges kjøreporter ved at vaktentralen ber underleverandøren som drifter kjøreportene om å låse disse. Underleverandøren stenger strømmen til motorene på kjøreportene, som da ikke kan åpnes. All inn og utpassering på Industriområdet ledes på slikt trusselnivå via havneporten. Perimetersikringen som Forsvarsbygg her viser til er sammenlignbart med Sklet (2006) sine tanker om barrieresystem. Informantene sa at å holde uvedkommende ute, er perimetersikringens hovedfunksjon. Men hvordan gjerder og porter skal man ha, hva skal man stille som krav til disse, når de er en av barrierene i perimetersikringen for Industriområdet?

Å hindre uautorisert personell og kjøretøy adgang til Industriområdet er hva alle informantene fremholder er hovedoppgaven til gjerdet og portene. «Ting og tenke på ved valg av gjerde er hvor mye tid man kan kjøpe seg overfor ulike typer av trusselaktører. Momenter som må avklares, er blant annet hvor lett eller vanskelig det skal være å klatre over eller ta seg gjennom gjerdet» (Stranden, 2019, s. 142). Stranden sier videre om porter skal være i gjerdetraséen. «Uansett om det er port som er designet for personell eller for kjøretøyer, er det viktig at porten holder samme kvalitet som resten av gjerdet» (Stranden, 2019).

Som barriereelement i barrieresystemet perimetersikring er det forventet at gjerdet og portene skal være i god stand og operative. Samtidig, som Forsvarsbygg (2022) peker på må det være samsvar mellom kvalitet og robusthet på gjerdet og portene slik at det ikke blir svakheter i

gjerdetraséen. Informant 1 fortalte at gjerdetraséen sjekkes fysisk hver tredje uke. Videre sa informanten at feil eller mangler utbedres på stedet, hvis mulig. Hvis ikke blir det meldt inn og underleverandør blir rekvirert. Informant 1 fortalte at det ble opprettet vakthold, til underleverandør kom, dersom skaden på gjerdetraséen var stor. For at barriereelementene skal danne et barrieresystem må det ha en kobling til hverandre og en samhandling innad i systemet. Et barriereelement som har tett tilknytting til gjerder og porter er adgangskontroll.

5.1.2 Adgangskontroll

Reason (2016) viser til harde og myke barrierer. Eksempler på harde barrierer er; porter, gjerder og kameraer. Eksempler på myke barrierer er; operatører, prosedyrer og rutiner. Adgangskontroll kan, jamfør Reason (2016), ses på som både en hard og en myk barriere. Det er styrt av låser nøkkelkort og porter/rondeller, samtidig som det også er styrt av prosedyrer og tillatelser. Adgangskontrollen på industriområdet styres gjennom digitale nøkkelkortlesere med tilhørende kode. Alle ansatte må registrere seg inn med kort og kode for å få tilgang til Industriområdets arealer. Kjøretøy registreres inn med egen kjøretøytillatelse knyttet til registreringsnummer. Reason (2016) ville kalt dette harde barrierer. Men er denne adgangskontrollen tilstrekkelig, hindrer den som Forsvarsbygg (2022) sier; Holder bare ærlige individer ute og er best egnet til å markere en juridisk grense? Eller er den robust nok til å hindre det NSM (2022) kaller; «Spionasje, målrettet informasjonstyveri ved bruk av fordekte metoder. Tyveriet kan skje ved fysisk eller menneskebasert innhenting, ved å utnytte IKT-systemer, eller en kombinasjon av disse» (Sikkerhetsmyndighet, 2022, s. 4). Informant 2 sa at adgangsreglene inn i Industriområdet oppleves som klare og tydelige. Samtidig er ukentlige stikkontroller av adgangskort lagt inn som en barrierekontroll av barriereelementet adgangskontroll. Informant 1 sa dette ble gjennomført på forskjellige steder fra gang til gang, og både personlige adgangskort og kjøretøytillatelser ble sjekket.

Adgangstillatelser, personlige adgangskort og kjøretøytillatelser produseres og deles ut i vaktcentralen. For å få en slik tillatelse må man ha en rekvirent fra eget firma, godkjent rekvirent fra Industriområdet og bestått sikkerhetskurs. Dersom dette ikke er på plass, gis det ikke adgangstillatelse til Industriområdet. Reason (2016) ville kalt denne delen av adgangskontrollen en myk barriere, da dette er et menneske-, instruks- og regelstyrt barriereelement. For å skaffe seg adgangstillatelse må man gjennom et annet barriereelement, sikkerhetskurs.

5.1.3 Sikkerhetskurs

Sikkerhetskursen er obligatorisk for alle som skal jobbe inne på Industriområdets områder. Som barriereelement har sikkerhetskursen barrierefunksjonen å tilføre ansatte nødvendig sikkerhetskompentanse. I sikkerhetskursen ligger kunnskap om adgangskontroll og hvilke sanksjoner som trer i kraft ved overtredelse mot denne, for eksempel ved å låne bort adgangskort eller kjøretillatelse til andre. Man må avlegge en godkjenningsprøve ved endt kurs, som må bestås. Tre av informantene sier det i sikkerhetskursen er lite fokus på perimetersikringen og brudd mot denne. De mener et større fokus på hva som skjer og hvilke følger eller konsekvenser brudd på perimetersikringen får av følger, kanskje ville ha økt bevisstheten rundt perimetersikringen på sikkerhetskursen. En informant sa «Sikkerhetskursen skal jo dekke alle sider ved sikkerheten, men per i dag er det vel 98 prosent safety og resten security. Det sier litt om hvor fokuset ligger i forhold sikkerhet og sikkerhetsfokus». Observasjoner under sikkerhetskursen, viser svært lite fokus på security i sikkerhetskursen. Samtaler under observasjoner har avdekket at det er mangel på ressurser som styrer fokuset i kursene. Samtidig kommer det frem at security problematikk blir nedprioritert fordi det har vært få uønskede hendelser knyttet til dette i forhold til safety hendelser. Man ser det derfor som unødvendig med mer fokus på security i kursen enn det det er i dag. Som barriere vil dette sikkerhetskursen, ifølge Reason (2016), være en myk barriere, knyttet opp mot instruksjoner lover og regler.

5.1.4 Kameraovervåking

Kameraovervåking inngår som et barriereelement i barrieresystemet perimetersikringen av Industriområdet. Forsvarsbygg (2022) har videoovervåking som forslag til barriere i en perimetersikring. Forsvarsbygg (2022) skriver videre at det bør opprettes et perimetersystem, hvor kameraer med deteksjonssystem inngår i systemet. På den måten vil systemet varsle operatøren når noe kommer innenfor deteksjonsområdet. I tillegg nevnes det også at det i kameraovervåkingssystemet også burde ligge muligheter for opptak, når det oppdages bevegelser på deteksjonsområdet. Denne måten å bygge barrieresystem på er gjenkjennelig i både harde og myke barrierer fra Reason (2016), hvor kameraene i seg selv er harde barrierer, mens operatørene, den menneskelige faktor er myke barrierer. «Safety barriers are physical and/or non-physical means planned to prevent, control, or mitigate undesired events or accidents» (Sklet, 2006, s. 496). I tillegg til kameraovervåkingen er det skiltet langs gjerdetraséen at det er kameraovervåking på Industriområdet. Slik blir personer som oppholder seg på eller inntil gjerdetraséen gjort oppmerksomme på dette.

Kameraovervåkingen inngår i den helhetlige perimetersikringen som et barriereelement i barrieresystemet. Men for at dette skal ha en barrierefunksjon i perimetersikringen kreves det operatører som opererer denne kameraovervåkingen. Disse operatørene bemanner den døgnbemannede vaktentralen.

5.1.5 Hovedresepsjonen, døgnbemannet vaktentral og havneport

Hovedresepsjonen, døgnbemannet vaktentral og havneporten er viktige barriereelementer i barrieresystemet perimetersikringen. I tillegg er Havneporten eneste inn- og utgang ved forhøyet trusselnivå på Industriområdet. Gjennom oppbygging, drift og operasjonalisering er disse barrierer, med operatørene, å anse som myke barrierer, selv om Vaktentralen og Havneporten, med en del av sine vakt og overvåkingssystemer, også vil være en hard barriere i barrieresystemet, jamfør Reason (2016) sin definisjon. «En operatør som ivaretar et sikkerhetsanlegg er i aller høyeste grad en primærfunksjon, og det må utformes og fasiliteres deretter» (Nasjonalt kompetansesenter for sikring av bygg, 2022, s. 187). Operatørene i vaktentralen har ansvaret for daglig operasjonalisering av perimetersikringen, dette gjelder ved alle sikkerhetsnivåer. Disse operatørene har ansvaret for kameraovervåking av perimetersikringen og ansvaret for å melde fra eller utløse alarm dersom noen forsøker å trenge inn på Industriområdet gjennom perimetersikringen. Operatørene i Havneporten har også denne funksjonen, men har ikke kontroll med hele perimetersikringen, kun Havneporten. Operatører sier at de ser forsøk på inntrenging på området, som oftest er dette «tailing³». Ofte er dette ansatte på Industriområdet som har dårlig tid og derfor prøver å ta en snarvei inn uten å måtte registrere seg. «Dersom vi oppdager «tailing», blir dette rapportert til nærmeste overordnede til den som kjørte inn og vedkommende sjåfør får en advarsel. Dersom det skjer igjen, risikerer sjåføren å miste adgangskortet og kjøretillatelsen sin» (Informant 5). Dette utsagnet viser at operatørene på Industriområdet har fokus i sitt arbeid og er en reell barriere i perimetersikringen. James Reason (2016) sier at det kan være en fare for at operatører av vaktsystemer kan bli for automatiserte og kun følge systemets innebygde alarmfunksjoner for å detektere inntrengninger eller andre unormaliteter ved overvåkingssystemene, men utsagnet fra informant 2, viser at operatørene i vaktentralen på Industriområdet har rett fokus for å operasjonalisere og inneha en slik oppgave og kan dermed sies å ha en primærfunksjon i perimetersikringen slik som beskrevet av Forsvarsbygg (2022).

³ Tailing: Bil som kjører inn kjøreport etter en annen bil, som lovlig registrerer seg, uten å registrere seg inn med kjørekort og kjøretøytillatelse. Dette kan gjøres på grunn av lang åpningstid på kjøreporter.

Operatørene på vaktcentralen, hovedresepsjonen og havneporten er Industriområdets daglige ansikt utad mot besøkende, sjåførere og innleid personale som skal inn på Industriområdets arealer. På den måten har disse tjenestepostene flere av hva Sklet (2006) ville kalt barrierefunksjoner. I tillegg til å ta imot besøkende og registrere dem inn i området har også vaktcentralen ansvaret for produksjon av adgangskort og kjøretøytillatelse. Samtidig er det på disse tjenestepostene man har mulighet til å oppdage dersom noen prøver å ta seg inn på Industriområdet og operatørene har opplevd ubehagelige situasjoner med sinte besøkende. «Hvis noen prøver å ta seg ulovlig inn, eller prøver å true seg inn på området, prater vi rolig med vedkommende, utløser stillealarm, og prøver å holde stand til beredskapen kommer og tar over situasjonen» (Informant 2). Hovedresepsjonen, havneporten og vaktcentralen har denne form for stille alarm. Den utløses via en knapp under skrivebordet, slik at en uønsket inntrenger ikke ser alarmen blir utløst. Ved slike alarmer eller innmeldinger av unormale forhold, tilkalles industriberedskapen, for å bistå i situasjonene.

Ansatte i hovedresepsjonen har en litt annen rolle i perimetersikringen enn Vaktcentralen og Havneporten. I Hovedresepsjonen kommer besøkende til Industriområdet. Tidligere kunne besøkende melde seg i Hovedresepsjonen og gå inn på Industriområdet dit man skulle. Nå er ikke dette lenger tillatt og de som skal ha besøk, må selv møte de besøkende i Hovedresepsjonen og følge de ut igjen ved endt besøk. Informant 11 sa følgende: «Tidligere kunne man melde opp besøk og de kunne gå inn til rett lokasjon. Nå må besøkende hentes i Hovedresepsjonen, Vaktcentralen eller Havneporten og følges inn.» Informanten mente at dette ga inntrykk av at perimetersikringen og kontroll med innpassering av personell var blitt strengere og med det bedre.

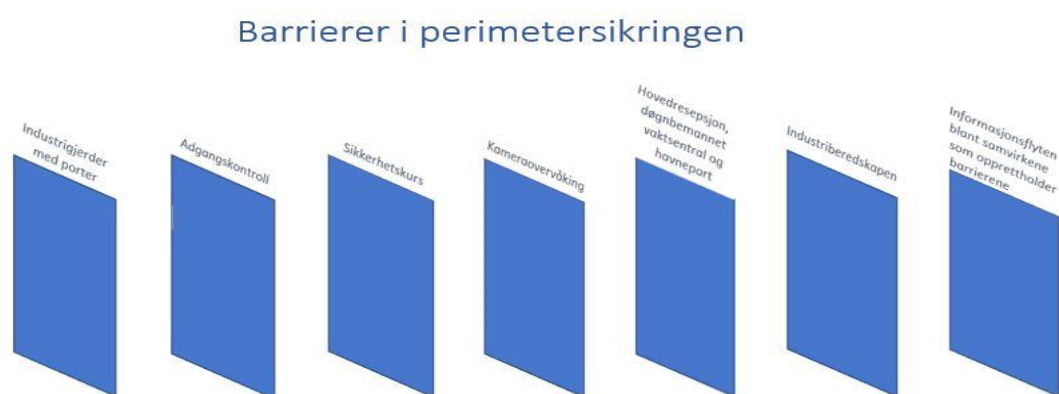
5.1.6 Industriberedskapen

Industriberedskapen rykker ut ved alarmer eller andre meldinger om unormaliteter eller defekter på perimetersikringen. Ved slike utrykninger er beredskapen styrt av de personene som leder den aktuelle utrykningen og det er deres persepsjon av hendelsen og dens risikobilde som avgjør hvordan de handler i den gitte situasjonen. På denne måten ville Reason (2016) ha definert Industriberedskapen som en myk barriere i barrieresystemet. «Ved brudd i perimetersikringen, rykker vi ut for å observere skaden. Dersom vi kan reparere skaden, gjør vi det der og da. Hvis ikke, melder vi inn til Industriområdet og holder eventuelt vakt til noen kommer og reparerer skaden» (Informant 1). Samtidig sier informanten at Industriberedskapen ikke er trent til på eller har utstyr til å pågripe eller konfrontere inntrengere som skulle forsøke å komme seg inn på området allikevel, sa informanten,

konfronterer Industrieredskaben inntrengerne, dersom de anser det som forsvarlig. Det vil si hvis ikke de observerer våpen eller anser det utrygt på annen måte. I tillegg vil politiet bli varslet i slike hendelser og komme til stedet. Industrieredskaben har, ifølge informant 1, hjemmel for å anholde inntrengere og bruke nødvendig makt for å stoppe eventuelle sabotasjeforsøk inne på Industriområdets arealer. Hvis man ser industrieredskaben opp imot Sklet (2006) sin teori om barrierer vil man kunne si, at som barriere, har Industrieredskaben en tydelig barriererefunksjon ved at de rykker ut til brudd på og unormaliteter rundt perimetersikringen. På den måten er Industrieredskaben et viktig barriereelement i barrieresystemet perimetersikringen av Industriområdet.

5.1.7 Oppsummering av barrierene som etableres for å ivareta perimetersikringen

Etter å ha gjennomgått hvilke barrierer som etableres for å ivareta perimetersikringen har jeg kommet frem til følgende barrierer. Tidligere i studien har jeg vist til Reason (2016) sin Swiss-cheese-modell for fremstilling og synliggjøring av barrierer. Modellen viser barrierer og hull eller latente forhold i disse. I dette underkapittelet har jeg beskrevet barrierene jeg har funnet i barrieresystemet perimetersikringen av Industriområdet. Sikringshåndboka (2022) er samsvarende med Reason (2016), Haddon (1980) og Stranden (2019), når det blir vist til at det er samhandlingen mellom flere tiltak og barrierer som i størst grad gir sikring i dybden. Stranden (2019) synliggjør dette ved å se barrierer og tiltak i et tredelt perspektiv, teknologi, organisasjon og menneske, MTO omtalt i kapittel 5.1.1. Jeg har derimot ikke synliggjort hull eller latente forhold i disse barrierene, det blir gjort i underkapittel 5.3. For å vise barrierene har jeg laget en forenklet versjon av Reason sin modell.



Figur 20: Forenklet versjon av Reason sin Swiss-Cheese modell som viser barrierene i perimetersikringen

Funn knyttet til dette underkapittelet viser at Industriområdet har en perimetersikring som svarer til Sklet (2006) sin fremstilling av et barrieresystem med tilhørende barrierer og barriererefunksjoner. Det er i dette underkapittelet ikke tatt hensyn til påliteligheten av

barrieresystemet, men kun synliggjort hvilke barrierer som er til stede og deres barrierefunksjon. Reason (2016) snakker om latente forhold i organisasjoner som kan true barrierenes robusthet og gi hull som kan føre til uønskede hendelser dette kommer jeg tilbake til i underkapittel 5.3.

5.2. Hvordan er informasjonsflyten blant samvirkerne som opprettholder barrierene?

For å kunne si noe om informasjonsflyten på Industriområdet skal jeg se på hva informasjon er, hva informasjonsprosessering er, hva informasjonsflyt er og hvordan dette påvirker samhandlingen. Informasjon kan være mye og omfattende. For å knytte dette til barrierene og jobben rundt perimetersikringen, vil et viktig begrep være informasjonsprosessering.

Informasjonsprosessering finner vi i Turner (1976) sin modell,

Informasjonsprosesseringsperspektivet, nevnt tidligere som figur 11 i oppgaven i kapittel 2.5.1.

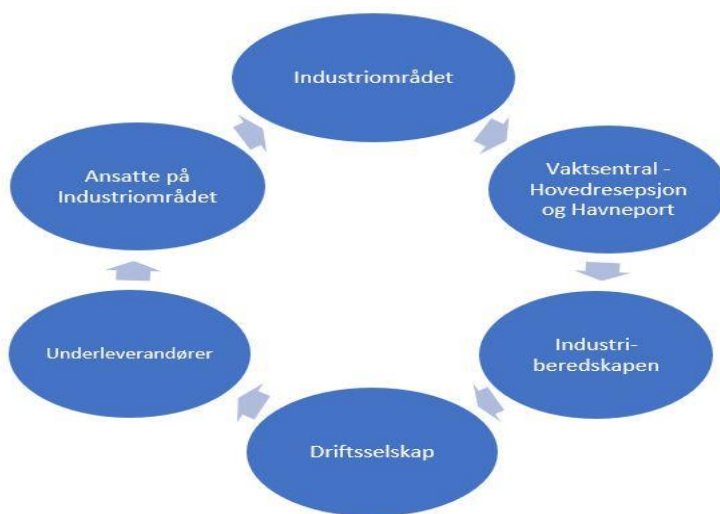
| The Sequence of Events Associated with a Failure of Foresight | |
|--|--|
| Stage I | Notionally normal starting point: (a) Initial culturally accepted beliefs about the world and its hazards (b) Associated precautionary norms set out in laws, codes of practice, mores, and folkways. |
| Stage II | Incubation period: the accumulation of an unnoticed set of events which are at odds with the accepted beliefs about hazards and the norms for their avoidance. |
| Stage III | Precipitating event: forces itself to the attention and transforms general perceptions of Stage II. |
| Stage IV | Onset: the immediate consequences of the collapse of cultural precautions become apparent. |
| Stage V | Rescue and salvage — first stage adjustment: the immediate postcollapse situation is recognized in ad hoc adjustments which permit the work of rescue and salvage to be started. |
| Stage VI | Full cultural readjustment: an inquiry or assessment is carried out, and beliefs and precautionary norms are adjusted to fit the newly gained understanding of the world. |

Figur 219: The sequence of events associated with a failure of foresight (Turner, 1976)

Turner sier noe om hvordan informasjon oppfattes, behandles, tolkes og videresendes. Turners modell er delt inn i seks trinn. Basert på denne prosesseringen, sier Turner, kan det i trinn to, danne seg nye sannheter, oppfatninger og kulturer knyttet til hvilken informasjon som blir formidlet. Dette blir da den nye sannheten i organisasjonen og man lever videre i denne sannheten til det skjer en hendelse som gjør at man igjen må endre praksis. Det er Industriområdet som har ansvaret for informasjonen som blir gitt rundt perimetersikringen og med det også hva som blir informert om. Hvordan Industriområdet prosesserer denne informasjonen vil være avgjørende for hva som blir informert om og informasjonsflyten rundt perimetersikringen. Selv om alle informantene sier at informasjonen og informasjonsflyten rundt perimetersikringen er god, er de ikke klar over hva de ikke blir informert om rundt perimetersikringen. Jamfør uttalelsene fra en informant «Det ser så fint, velholdt og flott ut, så

folk tror at når det er så fint, har de sikkert alt annet på stell også. De tror det er mye mer sikkert enn det er». Kan dette ha noe å gjøre med informasjonsprosesseringen til Industriområdet og hva de velger å gå ut med i informasjonsflyten rundt perimetersikringen?

Det er flere enheter på Industriområdet som drifter og operasjonaliserer perimetersikringen. I teoribidragene fra Stranden (2019), Reason (2016) og Haddon (1980) pekes det på at det er samhandling mellom flere tiltak som i størst grad gir sikring i dybden. For å få til en samhandling er det viktig med informasjon og informasjonsflyt. Samtidig er det viktig at det i samhandlingen rundt perimeteret ikke bare er kommunikasjon fra Industriområdet og ut, men også fra de andre samvirkerne og inn til Industriområdet. 3 av informantene uttaler at ansatte ved Industriområdet vil si ifra dersom de ser eller opplever anslag mot perimetersikringen og da må jo denne informasjonen også flyte tilbake til Industriområdet. Modellen nedenfor viser, baser på informasjon fra studien, hvilke samvirker som er med i informasjonsflyten rundt perimetersikringen. På denne måten vil samvirket, dersom det fungerer, være med på å sikre påliteligheten til barrierene.



Figur 20: Samvirkerne som opprettholder informasjonsflyten rundt perimetersikringen

Industriområdet har hovedansvaret for perimetersikringen. Det gjelder da også informasjon som skal gis om perimetersikringen til alle samvirkerne og ansatte på Industriområdet. I utgangspunktet skjer denne informasjonen gjennom at alle som skal jobbe inne på Industriområdet må gjennomgå sikkerhetskurs med avsluttende godkjenningsprøve. På denne måte har Industriområdet gitt hva de mener er nødvendig sikkerhetsinformasjon og kunnskap man må inneha for å kunne jobbe inne på Industriområdet. Informantene i studien er samstemte om at informasjonsflyten fra Industriområdet rundt perimetersikringen er tydelig

og god. Alle informantene sier at informasjonsflyt, rapporteringsrutiner og kanaler er godt kjent og at det på Industriområdet er en god rapporteringskultur. Reason (2016) beskriver rapporteringskultur som en av fire deler av en sikkerhetskultur. De tre andre delene er rettferdig kultur, lærende kultur og fleksibel kultur. For at man skal kunne opprettholde og videreutvikle informasjonsflyten, kan man si at det er viktig at man opprettholder en god sikkerhetskultur der man rapporterer om hendelser knyttet til perimetersikringen. At man opplever at Industriområdet tar til seg rapporteringen og lærer av det, at brudd blir behandlet rettferdig og at man utvikler perimetersikringen i takt med informasjonen som kommer, og gjennom det er fleksibel. En ansatt sa følgende «Det viktigste er at vi føler at vi kan si ifra og at vi får en tilbakemelding som i hvert fall forteller oss at noen har sett det vi melder om, oppleves bra. Hvis ikke hadde vi jo ikke giddi og meldt om saker».

Informasjonskanalene som brukes i det daglige utover sikkerhetskursene er mail til ansatte og oppslag rundt om på industriområdet. En annen informasjonskanal som benyttes er skilting av gjerdetraséen. Denne informasjonen retter seg til allmennheten utenfor industriområdet og gir informasjon om at området er overvåket og at uvedkommende ikke har adgang til Industriområdets arealer.

Hovedresepsjonen og døgnbemannet vaktentral opplever også at informasjonsflyten blant de som opprettholder barrierene i perimetersikringen er god, med kjent og vel etablerte rapporteringskanaler og en god rapporteringskultur. På lik linje med Industriområdet opplever de rapporteringskulturen som god på området. I tillegg til informasjonsflyt rundt daglig informasjon opplever også operatørene i vaktentralen at det er veldig tydelige og gode rutiner og kommunikasjonskanaler for alarmgiving og varsling av uønskede hendelser. De opplever å bli tatt på alvor og at responsen på denne typen informasjon og kommunikasjon er god. Også her knytter man denne informasjonsflyten til god sikkerhetskultur, hvor man ser nytten av og gevinsten i å rapportere. Operatørene i vaktentralen fremhever sin gode kommunikasjon med industribedriften som avgjørende ved uønskede hendelser og alarmsituasjoner. Her ser man virkelig hvordan rapporteringskulturen virker direkte inn på sikkerhetskulturen, slik som Reason (2016) hevder. Dersom man ikke hadde hatt kultur for å rapportere ville man mest sannsynlig hatt flere uønskede hendelser enn det man har i dag.

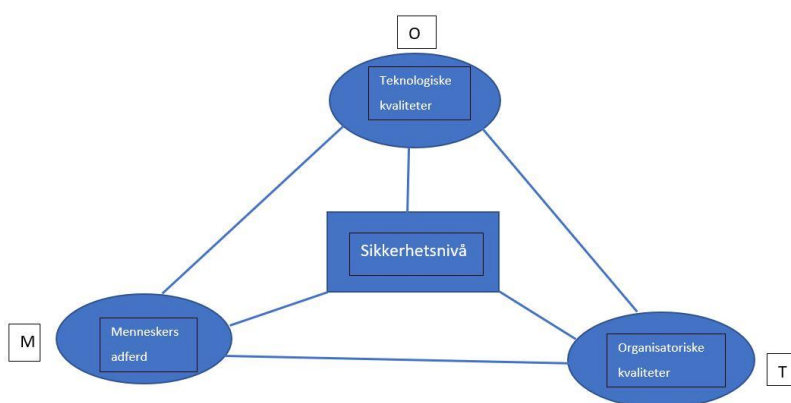
Alle informanter som har uttalt seg gjennom denne studien sier at informasjonsflyten mellom samvirkerne som opprettholder barrierene er god. Informantene er bredt sammensatt fra alle samvirkerne og gir samme svar uansett stilling eller funksjon. Man kan stille seg spørsmålet om de får all informasjon som er nødvendig, eller om de kun får det de trenger av informasjon

til å utføre sine daglige arbeidsoppgaver. Hvordan prosesserer Industriområdet informasjonen før den sendes ut? Blir relevante ansatte tatt med på informasjonsrunder i forkant av avgjørelser rundt perimetersikringen, og får de mulighet til å uttale seg dersom de mener noe bør utbedres eller utvikles rundt perimetersikringen? Dette skal jeg komme tilbake til under underkapittel 5.3.7.

5.3. Hva truer påliteligheten til dagens perimetersikring?

«Med påliteligheten til en enhet forstås dens evne til å utføre en tiltenkt funksjon» (Aven, Boyesen, Njå, Olsen, & Sandve, 2019, s. 122). I denne studien vil det altså si, evnen perimetersikringen har til å hindre uautorisert personell og kjøretøy adgang til Industriområdets arealer. For å kunne avgjøre om perimetersikringen er pålitelig må man gjøre en pålitelighetsanalyse, eller en risikoanalyse av barrieren. «I en driftssituasjon måles denne evnen ved å se på om barrieren virker eller ikke virker ved behov eller ved tester» (Aven, Boyesen, Njå, Olsen, & Sandve, 2019, s. 122). Videre sier Aven et al. (2019 s. 122) «Ved vurdering av pålitelighet antar en at barrieren ikke er ødelagt som følge av en ulykkesituasjon». Denne tankegangen kan sammenliknes med Haddon (1980) sin barrieremodell som jobber med tanke på at barrierer er tette. Barrieren er tett, fordi vi antar at den virker. Men dette står i kontrast til uttalelser fra informanter, som sier at det ikke er så sikkert som man tror «det er ikke så sikkert som det ser ut» (Informant 8).

Samtidig kan man i denne fasen av studien se til Antonsen et al. (2017) sin MTO modell beskrevet tidligere og laget til denne oppgaven som figur 6 i kapittel 2.5.



Figur 21: Gjengivelse av modellen Sikringstrekløveret - 2 (Antonsen, Heldal & Kvalheim, 2017, s. 283)

Og drøfte om de Organisatoriske og Teknologiske barrierene har de nødvendige kvalitetene som skal til for å gjøre perimetersikringen pålitelig. Og samtidig spørre seg om Menneskene har en atferd som er med på å gjøre perimetersikringen pålitelig. Antonsen et al. (2017)

snakker om sikkerhetsnivå i sin modell. Altså, er sikkerhetsnivået tilstrekkelig til at man har en pålitelig perimetersikring?

Sklet (2006) snakker om barriereelementer, barriererefunksjoner og barrieresystem. Han sier et barrieresystem inneholder barriereelementer som har barriererefunksjoner. For at barrieresystemet skal være pålitelig må barrierene med sine barriererefunksjoner virke som tiltenkt. Sklet (2006) nevner tre kriterier for å avgjøre påliteligheten til et barrieresystem ved gransking av barrierer ved ulykker: «- Barrierer som var installert og hvordan de virket, - barrierer som var installert men ikke ble brukt og – barrierer som ikke var installert men som var nødvendige» (Sklet, 2006, s. 502). I denne studien, i lys av Sklet sine teorier vil perimetersikringen være barrieresystemet. Barriereelementene vil være vaktsentral, kameraovervåking, gjerder og porter, havneport osv. Barriererefunksjonene vil være den oppgaven hvert barriereelement er satt til å løse, vaktsentral med overvåking, gjerder og porter skal hindre adgang osv. Sklet (2006) sin modell og tre kriterier leder oss til Reason (2016) sin Swiss-cheese-modell.

Reason sier i sin Swiss-cheese-modell at det kan forekomme hull eller latente forhold i forskjellige barrierer. Hull er direkte mangler, forhold som ikke er på plass, eller det Sklet (2006 s. 502) nevner som «barrierer som ikke var installert, men var nødvendige». Latente forhold, sier Reason (2016) er ikke så enkle å oppdage, det er forhold som ligger i organisasjonen og som får utslag i direkte feil ved senere tidspunkt. Eksempler på latente feil kan være dårlig opplæring. I denne studien kan latent forhold være at opplæringen gitt i sikkerhetskurset ikke er tilstrekkelig for å kunne møte Industriområdets krav til opplæring. Er det huller eller latente forhold i barrieresystemet perimetersikringen? Videre i dette kapittelet skal påliteligheten til de forskjellige barrierene i barrieresystemet perimetersikringen drøftes og i slutten av hvert delkapittel vil det synliggjøres hull eller latente forhold i hver enkelt barriere.

Kapittelet avsluttes med en oppsummering av funnene.

5.3.1 Industriegjerdet med diverse porter

Industriegjerdet, med diverse porter, er uten tvil en stor og viktig barriere i perimetersikringen. Men er dette en sikker barriere som holder uønsket personale ute eller er det mulig å komme seg inn gjennom denne barrieren. Holder gjerdet og portene, som Forsvarsbygg (2022) sier, bare ærlige folk ute, eller er det dimensjonert mot forsering? Hva kan man måle dette mot? Arbeidet med denne studien avdekker at det ikke har vært hendelser eller ulykker inne på

Industriområdet som skyldes inntrenging via gjerdetraséen. En informant beskrev at de hadde observert en person med fallskjerm som hadde hoppet fra det høyeste bygget inne på Industriområdet, men de hadde ikke klart å få tak i ham før han hadde kommet seg ut igjen. Det kommer også i samtaler fram at det har vært tyverier av verktøy og biler, men dette har ikke vært forbundet med skader i gjerdetraséen. og man antar derfor at tyvene har kommet seg inn og ut igjen gjennom portene ved å bruke stjalne adgangskort. Kan man da si at gjerdet og portene fungerer som en barriere, eller tror man bare at det er slik? Kan man si, med tanke på hva Forsvarsbygg (2022) uttaler, at man har klart å holde ærlige folk ute, men noen uærlige har sluppet inn? Hva kan være årsaken til dette og er dette hva Reason (2016) ville ha kalt hull i barrierene eller er det latente forhold? Og er perimetersikringen da god nok?

Informant 5 sa «Jeg tror ikke leietakerne vet hvor dårlig det er» informant 8 fulgte opp og sa «Overhodet ikke. Det er ikke så sikkert som det ser ut». En annen informant sa «utearealene her er så fine, velstelte og velholdt at folk tror nok at her har de det meste på stell. Men de vet ikke hvor enkelt det er å ta seg inn på området». Alle informantene i studien fortalte hvor og hvordan de ville ha kommet seg inn gjennom gjerdetraséen og ingen av dem trodde de ville ha problemer med å komme inn. «Man trenger bare en vanlig avbitertang» sa en informant i en samtale.

Et annet funn er at det ikke er knyttet andre barrierer til gjerdet og portene i perimetersikringen. «Det beste tiltaket mot trusselen fra kjøretøy er passive kjøretøysperrer rundt hele objektet, men vanligvis må det etableres inn-/ og utpasseringområde(r) med aktive kjøretøysperrer» (Nasjonalt kompetansesenter for sikring av bygg, 2022, s. 121).

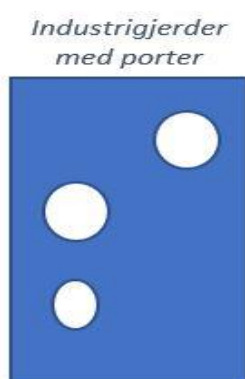
Observasjoner samtaler og intervjuer i studien viser at det ikke finnes slike sperrer, hverken aktive eller passive. «Portene og gjerdene er de samme, og det er ingen tillegg ved forhøyet trusselnivå ved industriområdet, det kommer ingen roadblockers eller annet utstyr, vi bare låser portene, de forsterkes ikke» (Informant 5). Flere informanter pekte på at det i senere tid var tatt ned en bom, som gjorde at biler nå kan kjøre helt inntil byggene der hovedresepsjonen og vaktentralen er. Med henvisning til tidligere terrorangrep i Norge, mente informantene dette var en forringelse av perimetersikringen.

I tillegg kom det frem at en enkel måte å komme seg inn på Industriområdet på, var gjennom det ansatte kaller for «tailing». Dette lar seg gjøre fordi lukketiden på portene er så stor. Under en deltakende observasjon så jeg en bil registrere seg inn, og kjørte inn porten. Det tok ca 35 sekunder fra bilen var kjørt til porten var helt lukket. Sjøføren så ikke ut til å observere om andre fulgte inn etter og var ute av syne fra porten før den var lukket. «det burde vært

sensorer i portene slik at de lukket seg når bakerste aksel på bilen passerte.» (Informant 5). Fra egen arbeidsplass, Kriminalomsorgen, er det en innarbeidet del av sikkerhetskulturen, at dersom man kjører inn en port, venter man på innsiden til det er umulig for noen andre å komme inn porten, før man kjører videre. Ville dette vært en mulighet å få inn i sikkerhetskulturen også på Industriområdet? Forsvarsbygg (2022 s.110) stiller følgende spørsmål «Kan man omgå sikringstiltakene eller utnytte mangel i sikringen? Kan man for eksempel passere inn sammen med autorisert person/kjøretøy?» James Reason (2016) ville ha kalt dette for et latent forhold. Lukketiden på portene er beregnet på at tunge vogntog skal ha nok tid til å komme seg inn, personbiler bruker mye kortere tid og porten vil derfor stå ubevoktet åpen. Det latente forholdet slår inn når en personbil passerer og det blir til et hull i barrieren.

Er da gjerdetraséen en barriere som oppfyller sin barrierefunksjon i barrieresystemet? Eller vil informasjonen som kommer frem, si at dette er en barriere som er/har et hull eller et latent forhold i det samme barrieresystemet? Spørsmålet som også må stilles er om ikke ledelsen ved Industriområdet er klar over forfatningen til gjerdet og portene? Eller kan man si med informasjonsprossesseringsperspektivet til Barry Turner (1976) at ledelsen, på grunn av få hendelser har vært gjennom en inkubasjonsfase og tror at gjerdet fungerer som det skal siden inntrenging via gjerdet ikke har ført til hendelser? Derfor tenker de heller ikke på å utbedre eller forsterke de svake punktene før det kommer en hendelse som kan knyttes til latente forhold i eller direkte hull i barriereelementet, gjerder med diverse porter.

Barrieren «Industriegjerdet med diverse porter» med hull og latente forhold, kunne vises på denne måten hvis vi skulle se på modellen til Reason (2016).



Figur 22: Hull og latente forhold i barrieren Industriegjerdet med porter.

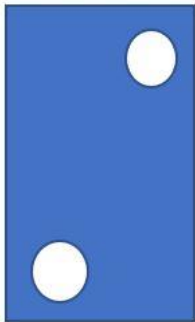
5.3.2 Adgangskontroll

Adgangskontrollen er også et barriereelement i barrieresystemet perimetersikringen. alle informantene og observasjoner under studien peker på at adgangskontrollen inn på Industriområdet fungerer. Alle som skal inn på Industriområdet registrerer seg inn med eget adgangskort, med personlig kode. I tillegg må de som kjører bil ha egen kjøretillatelse til bilen. Denne delen av barrieren fungerer, mener alle som har deltatt i studien. Men samtidig mener 6 av informantene at det er en stor mangel i adgangskontrollen. Man trenger ikke registrere seg ut. Forsvarsbygg (2022) snakker om inn- og utpasseringsområder. «For å heve sikkerhetsnivået kan man benytte kortlesere begge veier, slik at vedkommende blir registrert både inn og ut.» (Nasjonalt kompetansesenter for sikring av bygg, 2022, s. 173). Inne på Industriområdet fremkommer det at det er lokasjoner som allerede har registrering både inn og ut av sine lokasjoner, hvis disse ser behovet for dette, hvorfor har ikke hele Industriområdet dette sikkerhetsnivået? Informant 11 sa at hans firma har egne inn- og utpasseringsrutiner ved hans lokasjon, nettopp for å vite hvem som er på lokasjonen ved en ulykke eller hendelse. Informanten sa videre at han kjente til flere andre lokasjoner som også har slike egne ekstra adgangssystemer.

De seks informantene mener mangel på utregistrering er en trussel mot Industriområdet og et latent forhold i adgangskontrollen. Informantene peker på at man kan registrere seg inn og forbli inne i området i lang tid uten at dette registreres og dette mener informantene er en trussel mot sikkerheten i området. Informantene sa at man kan havne i en situasjon der en uønsket person kan komme seg inn på området med et stjålet kort og oppholde seg der over lang tid og planlegge, forberede og utføre sabotasjer eller andre aksjoner. Hadde man skulle ha registrert seg ut, ville det ha kommet varsel hvis registrerte personer ikke forlot området til normal tid. To av informantene peker også på at det sikkerhetsmessig, også i forhold til safety hendelser, ville vært trygt å vite hvem som var inne på området til enhver tid. For eksempel ved ulykker som krever evakuering av området. «Da vet man hvem man skal lete etter ved en ulykke, per i dag vet vi ikke hvem som er inne på området til enhver tid» Informant 6.

Barrieren «Adgangskontroll» med hull og latente forhold, kunne vises på denne måten hvis vi skulle se på modellen til Reason (2016).

Adgangskontroll

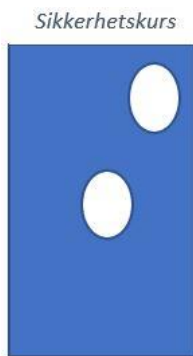


Figur 23: Hull og latente forhold i barrieren Adgangskontroll.

5.3.3 Sikkerhetskurs

Som nevnt tidligere er sikkerhetskurs en myk barriere i barrieresystemet. Sikkerhetskurset bygger på lover, regler, forskrifter og rutiner. Samtidig er eksemplene man bruker for å få frem poengene i sikkerhetskurset basert på tidligere erfaringer. Observasjoner underveis i studien viser at det er lite fokus på security hendelser i kurset. Det gis informasjon om adgangskontroll og hva som gjelder for adgangskontroll og at man ikke må låne bort sine personlige adgangskort til andre, men dette er en meget liten del av det totale sikkerhetskurset. Hvorfor er det slik? Det er Industriområdet som bestiller disse kursene av en underleverandør og det er Industriområdet som da også bestiller innholdet, hvorfor er det da så lite fokus på adgangskontroll? Barry Turners (1976) informasjonsprosesseringsmodell sier noe som kanskje kan være et svar på dette. Modellen går på at dersom man, over tid, opplever noe som en sannhet så inkuberes dette i organisasjonen og blir en sannhet. Er det slik at det gjennom tiden har vært så få hendelser knyttet til hendelser mot perimetersikringen at man ikke ser behov for å vektlegge dette mer i sikkerhetskurset? Reason (2016) sier at en organisasjon ikke er sikker, men at kontinuerlig arbeid mot å bli sikker, egentlig er sikkerheten. Kan dette fraværet av security fokus i sikkerhetskursene bli et latent forhold, som kan svekke dette barriereelementet og svekke ansattes fokus på security og i verste fall føre til hendelser og anslag mot Industriområdet? Hvis man ser på Reason (2016), Stranden 2019 og Haddon (1980) som beskriver at det er samhandlingen mellom flere tiltak som og barrierer som i størst grad gir sikring i dybden, vil man, i forhold til perimetersikringen, ha den sikringen når fokuset på perimetersikringen er så lite i sikkerhetskurset? Ville det for eksempel ikke her vært naturlig å ansvarliggjøre alle med adgangskort og kjøretøytillatelse til at de ikke skulle slippe noen inn sammen med seg når portene står så lenge åpne etter innpassering?

Barrieren «Sikkerhetskurs» med hull og latente forhold, kunne vises på denne måten hvis vi skulle se på modellen til Reason (2016).



Figur 24: Hull og latente forhold i barrieren Sikkerhetskurs

5.3.4 Kameraovervåking

Kameraovervåking beskrives av Forsvarsbygg (2022) som deteksjonssystem.

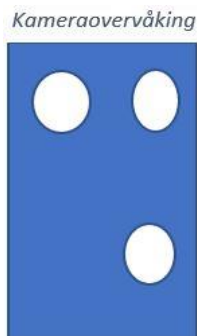
Deteksjonssystemet er en del av en perimetersikring. «Det opprettes et perimetersikringssystem. Det blir programmert inn soner for de ulike områdene rundt perimeteren. Ved alarm på et av deteksjonssystemene, for eksempel på sone 2, vil et kamera snu seg mot sonen, starte et opptak av hendelsen, og avslutte opptaket 60 sekunder etter at alarmstatus er normal igjen. Dette vil presenteres på «pop-up»-skjerm med alarm. Hendelser linkes også sammen i databaselogg.» (Nasjonalt kompetansesenter for sikring av bygg, 2022, s. 191).

Arbeid med studien avdekker at Industriområdet ikke har et helhetlig deteksjonssystem eller kameraovervåkingssystem. Fem av informantene peker på at det ikke er kameradekning rundt hele perimeteren. Fire informanter sier at det heller ikke finnes noen bevegelsessensorer på noen av kameraene i perimetersikringen. Under deltakende observasjoner, sa ansatte at slik kameraovervåking er per i dag, er det bare flaks om de klarer å få med seg det som skjer. Siden det ikke er bevegelsessensorer på kameraene, er operatørene avhengige av å kontinuerlig se på skjermene for å oppdage anslag mot perimetersikringen. Med alle oppgavene de har i dag, i tillegg til å følge med på kameraovervåkingen, er ikke dette mulig og man har flaks når man ser noe. Andre informanter i disse samtaler pekte også på dårlig lysforhold om kvelden som et hinder for å oppdage hendelser på kamera. To av informantene etterlyste også bedre kameradekning rundt portene i perimetersikringen, slik at de kunne se og snakke med ansatte som ønsket inn, men gikk til feil port, og å kunne informere ansatte dersom det var feil ved portene.

Informantene fra vaktentral og Industrieredskaben etterlyste alle en bedre og mer helhetlig kameraovervåking med bevegelsessensorer inn i perimetersikringen. De beskrev alle, kameradekningen per i dag, som en falsk trygghet, som kun virket når man kontinuerlig så på skjermene, men ikke ellers. I tillegg så man heller ikke da hele perimetersikringen, siden det ikke var dekning rundt hele. En informant sa, «Nå har det akkurat kommet opp en vaskehall inntil industrigjerdet, som hindrer og skygger for kameradekningen i det området. Den etableringen er en svekkelse av mine kontrollmuligheter.» (informant 5).

Informasjonen som har kommet fram gjennom studien, i forhold til kameradekningen i perimetersikringen, avdekker man flere hull og latente forhold i dette barriereelementet. Følger man Sklet (2006) sin teori, vil man kunne hevde at kameraovervåkingen ikke oppfyller sin barrierefunksjon, i og med det er mangler og den ikke er helhetlig rundt området og at det ikke er bevegelsessensorer tilknyttet.

Barrieren «Kameraovervåking» med hull og latente forhold, kunne vises på denne måten hvis vi skulle se på modellen til Reason (2016).



Figur 25: Hull og latente forhold i barrieren Kameraovervåking.

5.3.5 Hovedresepsjonen, døgnbemannet vaktentral og havneport

Hovedresepsjonen, Vaktentralen og Havneporten er alle barriereelementer i barrieresystemet, men de har forskjellige barrierefunksjoner, selv om noen av funksjonene er like.

Barrierefunksjonen til disse tre er arbeidsoppgavene de er satt til å løse knyttet til perimetersikringen og å opprettholde perimetersikringens pålitelighet. Ansatte i Hovedresepsjonen, Vaktentralen og Havneporten tar imot besøkende til Industriområdet. Deres oppgave er å sjekke om den besøkende har en avtale og om nødvendig varsle ansatte som mottar besøk, at besøket har kommet. De ansatte i Hovedresepsjonen og Havneporten sitter bak en skranke ubeskyttet mot de besøkende, mens Vaktentralen sitter inne i Vaktentralen og betjener besøkende gjennom en luke. Informant 2 sa følgende «Ustabile sinna mennesker kan komme helt inn til oss uten noe annet enn skranken som hinder». Informanten hevder dette kan føre til trussel- og i verste fall gisselsituasjoner. Informanten hevdet at de hadde opplevd situasjoner som hadde krevd at de måtte tilkalle Industriberedskaper for hjelp. Men selv om de kunne tilkalle Industriberedskaper, var ikke informanten sikker på om dette var tilstrekkelig til å kunne hindre alvorlige situasjoner. «Utformingen av vaktlokalet bør generelt være dimensjonert for å tåle en forhøyet trusselsituasjon. Dette kan innebære – resepsjonsløsninger som beskytter mot personangrep og/eller beskytning, - systemer for registrering av besøkende, - sluser som forhindrer inntrenging» (Nasjonalt kompetansesenter for sikring av bygg, 2022, s. 196). Direkte adgang til personell er mulig både i Hovedresepsjonen og i Havneporten. I Vaktentralen betjenes besøkende gjennom en luke, allikevel sier informant 2 følgende «Det burde vært mulighet for calling og postkasse for levering av kort og annet utstyr, slik at ingen uautoriserte, fysisk, behøver å komme inn til luka i vaktentralen etter klokken 16:00». Informanten begrunner

utsagnet med sårbarheten til vaktcentralen dersom noen ønsker å utføre et anslag mot industriområdet, gjennom først å angripe vaktcentralen og ved det sette Industriområdets varslings- og alarmanlegg ut av spill. Informanten sa at selv om man ikke kom seg inn i vaktcentralen normalt sett, kunne man jo tenke seg at en gjerningsperson kunne true seg inn i vaktcentralen, så lenge man var kommet inn i bygget. Siden Havneporten er valgt som inn- og utkjøringspunkt ved forhøyet trusselbilde på Industriområdet, vil man kunne stille seg spørsmålet om det er tilstrekkelig sikkerhetsnivå knyttet til Havneportens barrierefunksjon? Burde egentlig Havneporten hatt samme utforming og sikkerhetsnivå som Vaktcentralen, siden barrierefunksjonen til Havneporten faktisk endrer seg ved forhøyet trusselbilde mot Industriområdet? Ville det vært riktig å ha samme kravene til bygningsmassen og bemanningen på og av Havneporten, som man har til Vaktcentralen? Det er hevet over enhver tvil at i daglig normal drift, er vektingen av sikkerheten mellom de barriereelementene riktig vektet, ved at det er vaktcentralen som er best sikret. Vaktcentralen har i det daglige en helt annen funksjon som barriere enn Hovedresepsjonen og Havneporten, gjennom at vaktcentralen også drifter resten av Industriområdets sikkerhetssystemer, ikke bare perimetersikringen. Forsvarsbygg (2022) definerer dette som alarmmottak. «Alarmmottaket skal være bemannet døgkontinuerlig av spesielt utdannet personell. Det skal alltid være minst to personer på vakt, og lokalene skal minst være sikret tilsvarende kravet til sikring av de objektene som alarmmottaket mottar alarmer fra» (Nasjonalt kompetansesenter for sikring av bygg, 2022, s. 171). Observasjoner gjennom studien og samtaler med informanter viser at det kun er en operatør på vakt i vaktcentralen til enhver tid. Ved observasjoner av øvelser viser det seg at det heller ikke ved krisesituasjoner og uønskede hendelser hvor arbeidsmengden og stressnivået til operatøren øker, er det rutiner for å forsterke med ytterligere operatører.

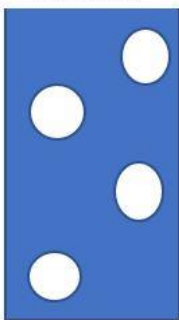
Et annet moment som stiller spørsmålsteget ved barrierefunksjonen til Vaktcentralen opp imot perimetersikringen, er operatørens arbeidsoppgaver i tillegg til overvåking av perimetersikringen. Informantene 5 og 6 sa at med dagens oppgaver i Vaktcentralen har de ikke mulighet til å ha det fokuset de trenger for å kunne ha tilstrekkelig overvåking av perimetersikringen. I tillegg påpekte de at det ikke var bevegelsessensorer på kameraene, som igjen gjorde at de ikke ble varslet dersom noen nærmet seg eller gjorde anslag mot perimetersikringen. Hvis de da var opptatt med andre oppgaver, som å produsere adgangskort, sjekke rekvisiter for adgangsklarering, bistå KO ved hendelser eller ta imot utlånt utstyr, vil de ikke få med seg hendelsen som viser seg på skjermen og da heller ikke kunne varsle eller

utløse alarm. «En operatør som ivaretar et sikkerhetsanlegg er i aller høyeste grad en primærfunksjon, og det må fasiliteres deretter. Det innebærer at dersom operatøren har andre arbeidsoppgaver, skal ikke synsvinkelen endres nevneverdig under de ulike operasjonene» (Nasjonalt kompetansesenter for sikring av bygg, 2022, s. 187). Når det ikke er bevegelsessensorer på kameraene gjør dette at operatørene i Vaktentralen ikke har mulighet til å holde det fokuset som kreves for å kunne si at de overvåker perimetersikringen annet enn sporadisk.

Et annet moment flere informanter tok opp var at Vaktentralen ikke har mulighet til å sperre portene, ved forhøyet trusselnivå ved Industriområdet. For å sperre portene må operatøren ringe til selskapet som drifter perimetersikringen for at de så sperrer portene ved å kutte strømmen til portstyringene slik at portene ikke kan åpnes med adgangskort. I slike tilfeller ønsket informant fem at de hadde kameraer og callinger ute på portene slik at besøkende eller ansatte som ville eller måtte inn på Industriområdet kunne fått informasjon om å kjøre til Havneport via calling. Når man ser på perimetersikringen basert på informasjon fra informanter og observasjoner kan man stille seg spørsmålet om perimetersikringen rundt Industriområdet er det Forsvarsbygg (2022) kaller «en godt utformet perimeter- og områdesikring»?

Barrieren «Hovedresepsjonen, døgnbemannet vaktentral og havneport» med hull og latente forhold, kunne vises på denne måten hvis vi skulle se på modellen til Reason (2016).

*Hovedresepsjon,
døgnbemannet
vaktentral og
havneport*



Figur 26: Hull og latente forhold i barrieren Hovedresepsjonen, døgnbemannet vaktentral og havneport.

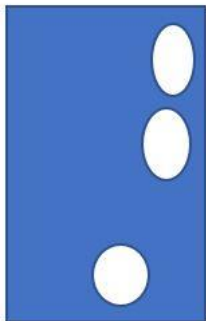
5.3.6 Industrieredskapsen

Industrieredskapsen er tidligere nevnt, hva Reason (2016), ville karakterisert som en myk barriere det vil si en prosedyrer, lover, regler og personell. Barrierefunksjonen til industrieredskapsen er å rykke ut på alarmer eller uønskede hendelser rundt

Videre, i henhold til interne rutiner, kontrollerer Industrieredskaben hele perimeteret hver tredje uke og de gjennomfører ukentlige kontroller av adgangskort og kjøretillatelser. Dersom de finner uregelmessigheter, blir personene og eller kjøretøyene bortvist. Men, informant 1 sa at dersom man finner et brudd på perimetersikringen ved sjekk av denne, forsøker de å reparere bruddet. Dersom de ikke kan gjøre dette med utstyret de har, melder de fra om bruddet og holder vakt, om de anser det nødvendig, frem til bruddet er reparert. Det som også kommer frem er at selv om man finner hull i perimetersikringen, gjør man ikke noe for å finne ut av hvordan hullet oppsto. Man melder ikke inn at det kan være uønskede personer på området, man melder kun om hullet. En informant sa i en samtale «Vi vet jo ikke om huller er nytt eller gammelt, derfor sørger vi for å få det tettet, men vi gjør ikke noe mer ut av det». Hva om det er uønskede personer som har kommet seg inn gjennom dette hullet og vandrer rundt på Industriområdet, hvor lang tid vil de kunne ha på å planlegge og gjennomføre en aksjon, dersom de virkelig har kommet seg inn på området? Oppfyller Industrieredskaben sin barrierefunksjon på denne måten?

Barrieren «Industrieredskaben» med hull og latente forhold, kunne vises på denne måten hvis vi skulle se på modellen til Reason (2016).

Industrieredskaben



Figur 30: Hull og latente forhold i barrieren Industrieredskap

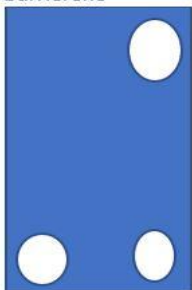
5.3.7 Hvordan er informasjonsflyten blant samvirkerne som opprettholder barrierene
Alle informantene hevder at informasjonsflyten blant samvirkerne som opprettholder barrierene er god. Men er den egentlig det når ansatte melder inn om forhold de mener svekker perimetersikringen og dette ikke blir besvart eller rettet opp i? På tross av at informantene hevder informasjonsflyten er god, kommer uttalelser som at «det har kommet opp en vaskehall helt inntil perimetersikringen som skygger for kameradekningen» (Informant 5). Når 7 av informantene peker på at de ikke ser en helhetlig tankegang blant lokasjonene og Industriområdet når det gjelder syn på og viktigheten av perimetersikringen.

Når det blir påpekt at å fjerne en bom i perimetersikringen svekker perimetersikringen og bommen likevel blir fjernet. Informantene hevder unisont at informasjonsflyten rundt drift vedlikehold og operasjonalisering av perimetersikringen er god. Men tre informanter hevder at informasjon som blir levert om ønsker om utbedringer eller oppgraderinger av perimetersikringen tar lang tid å få svar på, om de i det hele tatt får svar. Kan man med denne informasjonen si at informasjonsflyten blant samvirkerne er god?

Hvis vi går tilbake til Barry Turner (1976) sitt informasjonsprossesseringsperspektiv, og tenker på hans seks trinn fra normal tilstand i steg en til full revisjon og omlegging av kulturen i steg seks. Er det slik at på grunn av få hendelser og lite anslag mot perimetersikringen, så ser ikke Industriområdet på oppgraderinger og utbedringer av perimetersikringen som nødvendig? Har oppfattelsen av at perimetersikringen er så god at den ikke trenger å utbedres eller oppgraderes inkubert seg i Industriområdet og slike investeringer blir derfor sett på som unødvendige? Er det derfor kommunikasjon som går på forslag rundt oppgraderinger og utbedringer ikke besvares? Man lever rett og slett i en verden som sier at det vi har og hvordan vi opererer det er godt nok. Kanskje må man videre inn i stegene til Turner (1976) og få en hendelse, som direkte kan knyttes tilbake til for dårlig eller utdatert perimetersikring eller for høyt arbeidspress og for mange oppgaver i Vaksentralen som gjør at de ikke har fokus på perimetersikringen, for at dette skal komme på dagsorden og utbedres.

Barrieren «Hvordan er informasjonsflyten blant samvirkerne som opprettholder barrierene» med hull og latente forhold, kunne vises på denne måten hvis vi skulle se på modellen til Reason (2016).

*Informasjonsflyten
blant samvirkerne
som opprettholder
barrierene*



Figur 28: Hull og latente forhold i barrieren Hvordan er informasjonsflyten blant samvirkerne som opprettholder barrierene

5.3.8 Oppsummering av barrierenes pålitelighet

Hvis jeg bruker Reason sin Swiss-cheese-modell for å analysere de barrierene jeg nå har gått igjennom, tenker jeg at det kan synliggjøres i følgende tabell. Hullene i figurene i bunnen av

foregående underkapitler viser til hull og latente forhold i barrierene. Disse er listet opp i høyre kolonne i tabellen under. Venstre kolonne i tabellen viser hvilke barrierer hullene eller de latente forholdene hører til.

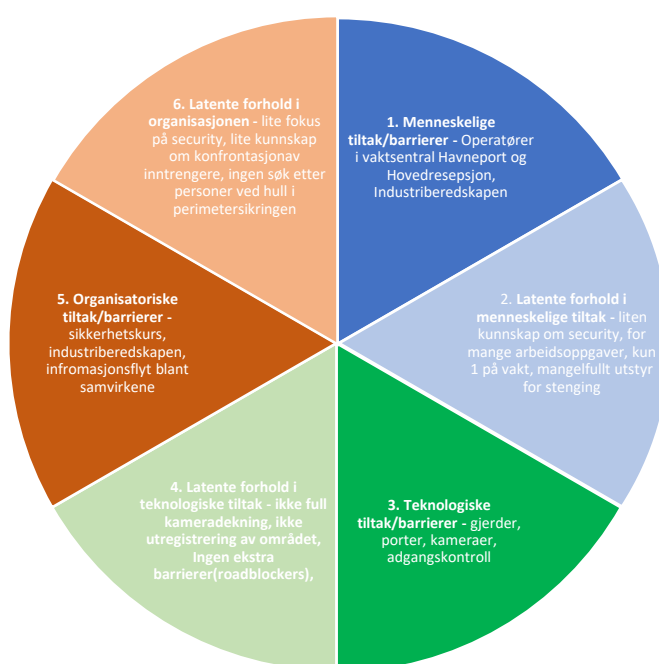
| Barrierer | Hull/Latente forhold |
|---|---|
| Industrigjerdet med porter | Ingen ytterligere barrierer eller hindringer ved forhøyet trusselnivå (roadblockers), fjernet port gir adgang til bygningene med vaktentral og hovedresepsjon, tailing mulig grunnet lang lukketid på kjøreporter |
| Adgangskontroll | Ingen registrering ut av området annet enn for biler, adgangskort kan stjeles eller lånes bort, |
| Sikkerhetskurs | Lite fokus på security og hva som er ansvaret rundt perimetersikring, burde ansvarliggjort ansatte rundt perimetersikring. |
| Kameraovervåking | Dekker ikke hele perimetersikringen, ikke bevegelsessensorer, hindres av enkelte bygg langs gjerdetraséen |
| Hovedresepsjon, døgnbemannet vaktentral og havneport | Har andre oppgaver enn kjerneoppgavene rundt vakthold av perimetersikringen, arbeidsforhold gir ikke mulighet for kontinuerlig kontroll med perimetersikringen, kan ikke stenge porter ved forhøyet trusselnivå, kun en på vakt |
| Industriberedskapsen | Iverksetter ikke søk etter personer ved oppdagelse av brudd på perimetersikringen, lite fokus på security hendelser. Ingen trening eller øving på hendelser med uønskede personer. |
| Informasjonsflyten blant samvirkerne som opprettholder barrierene | forskjellig virkelighetsoppfatning av perimetersikringen, vanskelig å bli hørt om oppgraderinger og utbedringer, man mener |

| | |
|--|---|
| | det er god informasjonsflyt men ser mangler når man hører hva og hvordan det blir informert |
|--|---|

Tabell 4: Tabellvis fremstilling av Swiss-cheese av funn fra oppgaven

Denne fremstillingen viser at det finnes hull og latente forhold i de forskjellige barrierene. Hvis man følger Reason sin modell, vil dette være grunnlag for at alvorlige hendelser kan skje. Jeg vil komme tilbake til dette i underkapittel 5.4.

For å visualisere barrierene og hullene eller de latente forholdene tydeligere, kan vi vise de i en modifisert modell, laget til dette studiet, bygget på Strandens (2019) sikringstrekløver, hvor de mørke feltene (1, 3 og 5) er barrierene og de lyse (2, 4 og 6) er hull eller latente forhold.



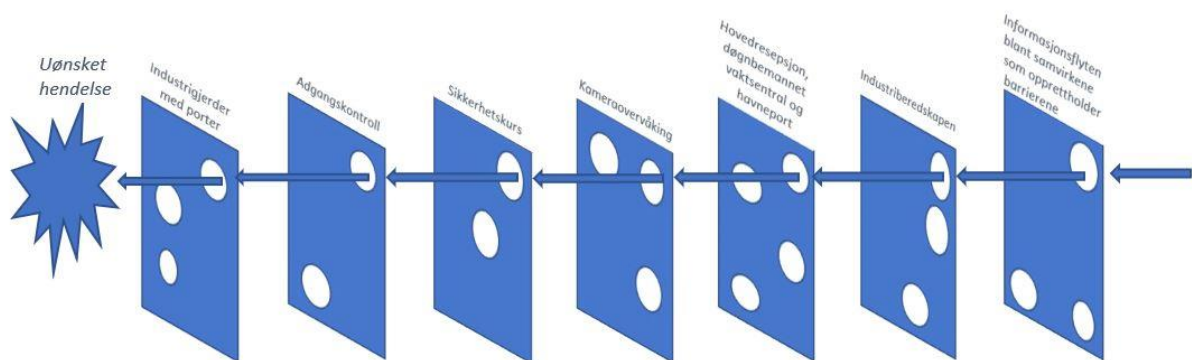
Figur 29: Barrierer i en modell av Strandens (2019) sikringstrekløver

Med de hullene som avdekkes i alle barrierer blir det fristende å gå til Sklet (2006) gjengitt i Hegde (2015) og se på hvordan det ser ut i hans tre nivåer. Barriereelement, barriererefunksjon og barrieresystem og igjen se om de forskjellige barriereelementene opprettholder eller oppfyller sin barriererefunksjon i barrieresystemet. Hvis man bruker Strandens (2019) sin inndeling, Menneskelig, Teknologisk og Organisatorisk, vil man kunne si at det i alle

barriereelementene er oppdaget hull, eller det Reason (2016) kaller latente forhold, som kan føre til at perimetersikringen blir brutt og at uvedkommende kan ta seg inn på Industriområdet umerket.

5.4. Hva er påliteligheten til perimetersikringen rundt Industriområdet?

Hva er så påliteligheten til perimetersikringen av Industriområdet? Hvis vi går tilbake til Reason (2016) sin Swiss-cheese-modell og lager en tilpasset modell bygget på funnene fra studien, med de barrierene som er beskrevet og de hull eller latente forholdene som ligger i disse barrierene. Vil det da være tette barrierer mot uønskede hendelser, slik som Haddon (1980) viser i sin modell, eller vil vi finne sammenhengene eller møtende hull eller latente forhold i barrierene slik som Reason (2016) beskriver? Funnene i studien gir oss følgende tilpassede utgave av en Swiss-cheese-modell



Figur 33: Swiss-cheese-modell tilpasset spesifikt for denne studien

Ja, studien viser at det er hull i barrierene. Funn fra studien, som beskrevet i kapittel 5.3, viser også at det er hull i barrierene som er sammenfallende i den grad at de kan skape en uønsket hendelse som i dette tilfellet vil være uoppdaget inntrenging på Industriområdet via perimetersikringen. Spørsmålet blir videre hvor sikkert ønsker man at det skal være på Industriområdet? Hva er det man anser å være tilstrekkelig eller hensiktsmessig sikkerhet? Dette vil jo være en diskusjon som ofte ender med en kost-nytte-analyse. Hvor sikkert må det være for å verne de verdiene som er inne på Industriområdet og hva er kravet til dette basert på historie, altså hvor ofte har det skjedd brudd på perimetersikringen slik den er i dag?

Samtidig ser man, spesielt gjennom funn fra annen teori, at man ofte kan vurdere risiko som lavere enn den egentlig er. Samtidig viser de samme funnene at det også er vanlig å vurdere trusselbildet til lavere enn det faktisk er. Betyr det at man på Industriområdet lever i Turners inkubasjonsfase, hvor man ikke klarer å se hvor alvorlig trusselbildet mot Industriområdet,

med nye verdensledende teknologi, interessant for både sivile og militære interesser, faktisk er? Når man igjen ser dette i et historisk perspektiv og forsøker å telle antall inntrenginger på Industriområdet som har ledet til alvorlige hendelser, er det ikke rart at man stoler på dagens perimetersikring og ikke ser behovet for å bruke midler på å oppdatere denne. Samtidig sier James Reason (2016) at sikkerhet ikke er noe man har eller innehar, men det er den kontinuerlige jobben mot og den pågående innsatsen for å være sikre som er sikkerheten i seg selv, det å hele tiden jobbe mot å bli sikrere. Samtidig bør man se på utviklingen av produksjon og teknologi inne på industriområdet og ta inn over seg at det per i dag er både produksjon og teknologi som PST (2022) anser å være interessant for både sivile og militære formål. Er man der, som NSM (2022) beskriver at; Bevisstheten og kompetansen om trussel- og risikobildet og hva som utgjør god nok sikkerheter for svak?

Og spørsmålet blir egentlig da; Er man i forkant av en eventuell hendelse, klarer man å forutse hva som kan skje og er man forberedt nok til å takle dette med den perimetersikringen man har? Er man oppe på proaktiv eller generativ i Hudsons (2007) kulturelle stige?

Det å jobbe med denne formen for sikkerhet er egentlig å gå fra Reason sin Swiss-cheese-modell til en Norsk-brunost-modell. Man ønsker å jobbe med å gå fra hullete til tette skiver, for å hindre nye hendelser fra å skje, og for å få til det, må man kanskje bruke en del midler på sikkerhet man aldri vil kunne måle om var nødvendig eller ikke. Selv om man kan si det er vellykket, dersom ikke hendelser skjer i fremtiden, men man vil da kunne hevde at det er ikke sikkert det ville skjedd med det gamle systemet heller. Spørsmålet blir om man er villig til å ta den sjansen og leve med gammel perimetersikring, når man vet hvor fort utviklingen skjer, også blant de som planlegger og gjennomfører intenderte angrep.

Eller kanskje problemstillingen er, som et av funnene i Statoils rapport fra In Amenas (2013) at ansvaret for security i organisasjonen er lagt inn under en Helse- miljø- og sikkerhetsstilling der hovedfokus er HMS og safety hendelser og kunnskapen og fokuset på Security blir nedprioritert og underkommunisert?

6. Konklusjon

Denne studien har hatt som formål å besvare følgende problemstilling:

«Hva er påliteligheten til perimetersikringen rundt Industriområdet?»

Hva er så påliteligheten til perimetersikringen? For å kunne belyse problemstillingen grundig har jeg hatt følgende tre forskningsspørsmål knyttet til problemstillingen.

«Hva slags barrierer etableres for å ivareta perimetersikringen?»

«Hvordan er informasjonsflyten blant samvirkerne som opprettholder barrierene?»

«Hva truer påliteligheten til dagens perimetersikring?»

Disse forskningsspørsmålene har hjulpet meg med å synliggjøre de forhold jeg mener har innvirkning på påliteligheten til perimetersikringen av Industriområdet.

Studien har vist at det er hull i perimetersikringen. Det er hull som viser seg åpenbare og det er andre som ikke vil komme frem før man opplever et anslag, som da vil være latente forhold knyttet til perimetersikringen.

6.1 Viktige funn fra studien

Jeg vil peke på syv viktige funn fra studien som har innvirkning, til dels alvorlig, på perimetersikringens pålitelighet.

Ingen egne barrierer knyttet til forhøyet trusselnivå på Industriområdet. Det er per i dag ikke knyttet ekstra barrierer til perimetersikringen ved forhøyet trusselnivå mot Industriområdet. Selv om man har prosedyrer som sier at porter stenges og at all trafikk skal sluses gjennomhavneporten, er det fortsatt de samme gjerdene og portene som skal stanse forsøk på inntrenging på Industriområdet. Det er ikke tiltak som forsterker disse portene ved forhøyet trusselnivå.

Ikke helhetlig kameradekning rundt perimeteret og ikke bevegelsessensorer på kameraene. Selv om det er skiltet rundt Industriområdet at det er kameradekning er ikke denne helhetlig. Det er områder rundt perimetersikringen som ikke er dekket av kamera. Disse blindsonene er områder hvor personer kan ta seg usett inn på området uten av vaktentralen har mulighet til å oppdage disse via kamera. Det er heller ikke bevegelsessensorer på kameraene som per i dag inngår i denne overvåkingen. Dette gjør at dersom ikke operatørene på vaktentralen oppdager et forsøk på inntrenging, vil det heller ikke bli oppdaget via kamera.

Bom fjernet fra perimetersikringen gir direkte tilgang med kjøretøy til hovedresepsjon og vaktentral. Fjerning av kjøreport fra perimetersikringen ved hovedinngang, gir direkte adgang foran byggene hvor vaktentral og hovedresepsjon er lokalisert. Dette gjør disse to postene utsatt for anslag med kjøretøyer.

Ikke registrering av ansatte ved utgang fra Industriområdet. Ansatte registrerer seg inn på området, men ikke ut. Dette gir mulighet for at ansatte eller uønsket personell som har skaffet seg adgang kan oppholde seg inne på Industriområdet over lang tid. De vil da kunne ha god tid til å planlegge, forberede og gjennomføre aksjoner. Ved registrering også av utganger, vil dette ikke være mulig på samme måte, da man vil kunne få varsler om personell som oppholder seg inne på Industriområdet over lang tid. Et annet moment er at man ved ulykker eller hendelser raskt vil få oversikt over hvem som er inne på Industriområdet og gjennom det vite størrelsesorden på en eventuell evakuering.

Det letes ikke etter inntrengere ved oppdagelser av hull i perimetersikringen. Når man på kontrollrunder, eller tilfeldig, oppdager hull i perimetersikringen settes det ikke i verk en rutine for å forsikre seg om at det ikke er uautorisert personell inne på Industriområdet. Dette betyr at personer kan oppholde seg inne på området til de tilfeldig blir oppdaget. Det burde ha vært en varslingsrutine i samvirket som informerte om mulig inntrengere på Industriområdet i tillegg til at man burde foreta et søk etter uautorisert personell.

Det er nivåforskjell på sikringsgrad mellom Industriområdet og enkelte leietakeres lokasjoner. Flere lokasjoner inne på Industriområdet har høyere sikringsnivå enn Industriområdet selv. Er dette naturlig, eller burde sikringsnivået til Industriområdet gjenspeile sikringsnivået til alle leietakerne? Her kan man ta hensyn til hva som er hensiktsmessig sikkerhet for flertallet av lokasjonene inne på Industriområdet og godta at noen lokasjoner velger å ha egne sikringstiltak. Samtidig vil dette gi signaler om sikkerheten til nyetableringer på Industriområdet.

Hvordan prosesseres informasjon til aktører som trenger oppdateringer når endringer skjer på Industriområdet? Hvilken informasjon, om hva og på hvilken måte blir gitt til de aktørene som trenger informasjon på Industriområdet. Hvordan er informasjonen prosessert før den når mottaker? Er det slik at all nødvendig informasjon kommer ut fra Industriområdet og er det slik at Industriområdet er mottakelig for informasjon som kommer til den knyttet til påliteligheten av perimetersikringen? For at perimetersikringen skal være pålitelig må også informasjonen og informasjonsflyten i samvirket være pålitelig med klare tydelige informasjonskanaler.

6.2 Forslag til videre forskning

Det bør gjøres en grundig sikkerhets- og risikovurdering knyttet til Industriområdets utvikling de siste 10 år. Det er vesentlig større grad av teknologi og produksjon som kan være av interesse for både sivile og militære aktører enn det var for 10 år siden. Allikevel oppleves det som om perimetersikringen rundt området ikke har utviklet seg i takt med utviklingen av teknologien og produksjonen. Derfor anbefales det å gjøre en vurdering på om dagens perimetersikring gjenspeiler hva man skal verne eller sikre ved hjelp av perimetersikringen. Dette er en omfattende jobb, men bør gjøres. Samtidig er det viktig med tanke på videre utbygginger og etableringer på Industriområdet, hvor man da kan vise til eventuelle nye etableringer hvor sikkerhetsnivået ligger opp imot deres krav til sikring. Samtidig kan man jobbe mot at NSM sin uttalelse fra 2022 om at «bevisstheten og kompetansen om trussel- og risikobildet og hva som utgjør god nok sikkerhet, per i dag er for svak.» ikke skal være gjeldende på Industriområdet.

Funnene i denne studien bør om mulig også deles med andre sammenliknbare industriområder, slik at man kan gjøre seg nytte av funnene fra denne undersøkelsen og dens mulige overførbarhet også på andre industriområder. For øvrig kan funn fra denne undersøkelsen vise viktigheten av å jobbe kontinuerlig med å forske på perimetersikringer for å opprettholde et hensiktsmessig sikkerhetsnivå på et industriområde. Dette sett i sammenheng med hvilken teknologi og produksjon som drives på industriområdet og behovet for sikring av denne. Hvordan samkjøre Industriområdenes og leietakernes krav til og behov for sikring av områdene, slik at det om mulig kan samkjøres under ett sikkerhetsregime.

6.3 Anbefalinger

Opprette egen stilling med fokus på security delen av sikkerhet. Man ser fra flere andre sammenliknbare industrier at stillinger som er knyttet direkte til security-sikkerhet opprettes for å ha dette fokuset som egen rolle opp mot ledelsen. Man begrunner dette med at safety og security er to store forskjellige fagfelt som krever fullt fokus for at jobben kvalitativt skal kunne gjøre godt med riktig fokus. Med dagens organisering vil alltid safety fokus komme foran security.

Oppgradere kameradekning til å bli helhetlig og med bevegelsessensorer. Man bør oppgradere kameradekningen og legge inn bevegelsessensorer på kameraene. Dette for at anslag mot perimetersikringen oppdages og varsles uten at det er avhengig av at operatørene i vaktentralen skal måtte overvåke skjermene kontinuerlig.

Bygge inn aktive kjøretøysperrer ved alle kjøreporter. Det bør bygges inn aktive kjøretøysperrer ved alle kjøreporter, slik at det er et forhøyet nivå for gjennomtrenging ved forhøyet trusselnivå mot Industriområdet. Disse må kunne opereres fra vaktcentralen,

Referanser

- Al-Fedaghi, S. (2017, mars). Securing the Security System. *International journal of security and its applications 11 (3)*, ss. 95-108.
- Andersen, S. S. (2006, Mars). Aktiv informantintervjuing. *Norsk statsvitenskapelig Tidsskrift vol. 22* , ss. 278-298.
- Antonsen, S., Heldal, F., & Kvalheim, S. A. (2017). *Sikkerhet og ledelse*. Oslo: Gyldendal Akademisk.
- Argenti, F., Landucci, G., Cizzani, V., & Reniers, G. (2017, april). A study on the performance assessment of anti-terrorism physical protection systems in chemical plants. *Safety Science, Volume 94*, ss. 181-196.
- Aven, T., & Renn, O. (2009). On risk defined as an event where the outcome is uncertain. *Journal of Risk Research, Vol. 12, No. 1*, 1-11.
- Aven, T., Boyesen, M., Njå, O., Olsen, K. H., & Sandve, K. (2019). *Samfunnssikkerhet*. Oslo: Universitetsforlaget AS.
- Aven, T., Røed, W., & Wiencke, H. S. (2017). *Risikoanalyse*. Oslo: Universitetsforlaget.
- Bakka, Å. A. (2020, februar 03). *Innbrudd på industriområde*. Hentet fra lister24.no: <https://www.lister24.no/nyheter/i/wPaz7G/innbrudd-paa-industriomraade>
- Bakke, L. A. (2015, august 11). *Fysisk terrorsikring i byens uterom: en studie av fysiske terrorsikringstiltak og hvordan slike kan integreres i byens uterom, hvor Oslo Rådhus brukes som en arena for å teste ut, og diskutere ulike tilnærminger*. Hentet fra <https://nmbu.brage.unit.no/>: <http://hdl.handle.net/11250/295993>
- Bhattarai, R., Zhang, Y., & Wood, J. (2021, 01 05). *Evaluation of various perimeter barrier products*. Hentet fra rosap Repository Open Science Access Portal: <https://rosap.nrl.bts.gov/view/dot/56880>
- Bolstad, K. (2014, januar 16). *Elleve innbrudd på Øra i løpet av 14 dager*. Hentet fra f-b.no: <https://www.f-b.no/nyheter/nyheter/elleve-innbrudd-pa-ora-i-lopet-av-14-dager/s/2-2.952-1.8249122>

- Casciano, M., Khakzad, N., (...), & Cozzani, V. (2019, desember). Ranking chemical industrial clusters with respect to safety and security using analytic network process. *Process safety and environmental protection*, ss. 200-213.
- Coaffee, J. P., & Boshier, L. P. (2008, juni). Integrating counter-terrorist resilience into sustainability. *Urban Design and Planning*, volume 161, Issue 2, ss. 75-83.
- Cunha, A., Marcineiro, N., Forcellini, F., & (...). (2018, juni). The impact of strategic planning on institutional integration toward patrimonial and perimeter security planning of the 2016 olympics games. *Brazilian journal of operations & production management* 15 (2), ss. 285-293.
- Dedousis, P., Stergiopoulos, G., (...), & Gritzalis, D. (2021). A security-aware framework for designing industrial engineering processes. *IEEE Access* 9, ss. 163065-163085.
- Dunbobbin, B., Medovich, T., & Murphy, M. (2004, november 5). Security vulnerability assessment in the chemical industry. *Process safety progress an official publication of the American institute of chemical engineers AIChE*, ss. 214-220.
- Egeli, A. (2014, juni 16). *Masteroppgave "Analysemetodikk i forbindelse med terrorisme - bruk eller ikke bruk av sannsynlighet"*, Universitetet i Stavanger. Hentet fra uis.no: <http://hdl.handle.net/11250/221328>
- Endal, E. G. (2022, april 26). *Aksjonister lenket seg fast for å protestere mot gruveprosjekt*. Hentet fra tv2.no: <https://www.tv2.no/a/14747311/>
- Engen, O., Gould, K., Kruke, B., Lindøe, P., Olsen, K., & Olsen, O. (2019). *Perspektiver på Samfunnssikkerhet*. Oslo: Cappelen Damm.
- Georges, P., & Merette, M. (2012, november). Toward a North American Security Perimeter? Assessing the trade, FDI, and welfare impacts of liberalizing 9/11 security measures. *Economic modelling* 29 (6), ss. 2514-2526.
- Gupta, J. P., & Bajpaj, S. (2007). Terror-Proofing Chemical Process Industries. *Science Direct, Volume 85, Issue 6*, ss. 559-565.
- Hagerup, I. C. (2018, juni). *Masteroppgave "Sikring av offentlig byrom. En kvalitativ studie av et tverrsektorielt samarbeid i en samfunnssikkerhets kontekst."* Universitetet i Stavanger. Hentet fra uis.no: <http://hdl.handle.net/11250/2580495>

- Halvorsen, E., Khawaja, N., & Storvik, B. L. (2019). *Rapportlære for Kriminalomsorgen*. Bergen: Vigmostad & Bjørke AS.
- Hegde, J. (2015, Oktober 15). *Origins of energy barrier accident perspective*. Hentet fra Systemsafety.wordpress.com: <https://systemssafety.wordpress.com/2015/10/15/origins-of-energy-barrier-accident-perspective/>
- Johannesen, A., Tufte, P. A., & Christoffersen, L. (2016). *Introduksjon til samfunnsvitenskapelig metode*. Oslo: Abstrakt forlag AS.
- Johannesen, B., Tufte, P. A., & Christoffersen, L. (2016). *Introduksjon til samfunnsvitenskapelig metode*. Oslo: Abstrakt forlag.
- Johansen, P. B. (2020, november 20). *Da mannen hadde klippet seg gjennom gjerdet kom politiet*. Hentet fra TA.NO: <https://www.ta.no/da-mannen-hadde-klippet-seg-gjennom-gjerdet-kom-politiet/s/5-50-1063366>
- Johnsen, L. G. (2019). *Risikovurdering Praktisk risikovurdering i virksomheter*. Oslo: Gyldendal Akademisk.
- Jore, S. H., Kruke, B., & Olsen, O. (2020, 05). *Vurdering av konsekvenser ved etablering av ytre perimeter rundt nytt regjeringskvartal*. Hentet fra <https://uis.brage.unit.no/>: <https://hdl.handle.net/11250/2653567>
- Kalam, A. (2021, mars). Securing SCADA and critical industrial systems: From needs to security mechanisms. *International journal of critical infrastructure protection* 32.
- Kjellen, U., & Albrechtsen, E. (2017). *Prevention of accidents and unwanted occurrences: theory, methods, and tools in safety management (2. utgave)*. Boca Raton: CRC Press.
- Kongsvik, T. (2016). *Sikkerhet i organisasjoner*. Bergen: Fagbokforlaget.
- Kruke, M. E. (2017, Juni). *Masteroppgave i samfunnssikkerhet "Beskyttelse av sensitiv informasjon. En studie av norske nettselskapers beskyttelse av sensitiv informasjon."*, *fordypning i sikkerhet og beredskap i nordområdene*. Hentet fra UiT Munin: <https://hdl.handle.net/10037/11344>
- Larsen, C. I., & Østensjø, C. (2015, juni 15). *Masteroppgave "Operatørselskapene i petroleumssektoren sitt syn på sikringskultur - Bruk eller ikke bruk av begrepet*

- sikringskultur.*" Universitetet i Stavanger. Hentet fra uis.no:
<http://hdl.handle.net/11250/298602>
- Lee, C. (2015, mars). Criminal profiling and industrial security. *Multimedia tools and applications* 74 (5), ss. 1689-1696.
- Lee, S., & Huh, J. (2021). Management of schemes and threat prevention in ICS partner companies security. *CMC-computers material & continua* 69 (3), ss. 3659-3684.
- Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. Newbury Park: SAGE Publications, Inc.
- Lohani, D., Crispin-Junior, C., Barthèlemy, Q., Bertrand, S., Robinault, L., & Rodet, L. T. (2022, mai 9). *MDPI*. Hentet fra mdpi.com: <https://doi.org/10.3390/s22093601>
- Lunde, I. K. (2019). *Praktisk krise- og beredskapsledelse*. Oslo: Universitetsforlaget.
- Løsnæs, E. (2022, april 17). *Kobbertyvene ble tatt på fersken – nå er en kvinne tiltalt*. Hentet fra ta.no: <https://www.ta.no/kobbertyvene-ble-tatt-pa-fersken-na-er-en-kvinne-tiltalt/s/5-50-1349163>
- Merad, M., Rodrigues, N., & Salvi, O. (2008). Urbanisation control around industrial Seveso sites: the French context. *International journal of risk assessment and management* 8 (1), s. 158.
- Miøen, E. (2016, juni 14). *Masteroppgave "Beredskap i norsk industri - En studie av tverrsektorielt samvirke mellom Herøya Industripark og nødetatene."*, Universitetet i Stavanger. Hentet fra Uis.no: <http://hdl.handle.net/11250/2411974>
- Mustaparta, A. J. (2016, januar). *Masteroppgave "Industrivernet- Norges skjulte beredskapsaktør? - En studie om betydningen av samvirke mellom industrivernet og lokale beredskapsaktører."*, Universitetet i Stavanger. Hentet fra uis.no:
<http://hdl.handle.net/11250/2393783>
- Nasjonal sikkerhetsmyndighet, N. (2017). *RISIKO 2017, Risiko og sårbarheter i en ny tid*. Hentet fra NSM.no: https://nsm.no/getfile.php/133726-1592915950/Filer/Dokumenter/Rapporter/nsm_risiko_2017_lr_0404_enkelts_v3.pdf
- Nasjonal trusselvurdering*. (2022). Hentet fra PST.no: <https://www.pst.no/alle-artikler/trusselvurderinger/ntv-2022/>

- Nasjonalsikkerhetsmyndighet. (2016). *Risikovurdering for sikring, Håndbok*. Oslo: NSM.
- Nasjonalt kompetansesenter for sikring av bygg, F. (2022). *Sikringshåndboka (3. utgave)*. Oslo: Forsvarsbygg.
- Njå, O., Sommer, M., Rake, E. L., & Braut, G. (2020). *Samfunnssikkerhet*. Oslo: Universitetsforlaget.
- Norman, B., & Adams, D. (2007, april). Virtual perimeter security (VPS) in a physical protection system. *IEEE aerospace and electronic systems magazine* 22 (4), ss. 30-33.
- Norsk senter for Forskningsdata. (2022, Februar 25). Hentet fra Hvordan gjennomføre et prosjekt uten å behandle personopplysninger?: <https://www.nsd.no/personverntjenester/oppslagsverk-for-personvern-i-forskning/hvordan-gjennomfore-et-prosjekt-uten-a-behandle-personopplysninger/>
- Reason, J. (2016). *Managing the risks of Organizational Accidents*. New York: Routledge.
- Reniers, G. (2011, februar). Terrorism security in the chemical industry: Results of a qualitative investigation. *Security journal*, ss. 69-84.
- Reniers, G., Dullaert, W., & Soudan, K. (2009, april). Shaping av novel security approach in chemical industrial clusters to prevent large-scale domino events. *Security journal*, ss. 119-142.
- Ringdal, K. (2013). *Enhet og mangfold*. Bergen: Fagbokforlaget.
- Samferdselsdepartementet. (2013, mai 31). *Forskrift om sikring av havneanlegg*. Hentet fra Lovdata.no: <https://lovdata.no/dokument/SF/forskrift/2013-05-29-538?q=ISPS>
- Sikkerhetsmyndighet, N. (2022, Januar). *Risiko*. Hentet fra www.nsm.no: [nsm.no/Risiko2022](http://www.nsm.no/Risiko2022)
- Sklet, S. (2006). Safety barriers: Definition, classification, and performance. *Journal of Loss Prevention in the Process Industries* 19, 494-506.
- Smith, C. L., & Brooks, D. J. (2013). *Security science*. Oxford: Elsevier Inc.
- Sommer, M., Pollestad, B., & Steinnes, T. (2020). *Beredskapsøving og -læring*. Bergen: Fagbokforlaget.

- Srivastava, A., & Gupta, J. (2010, november). New methodologies for security risk assessment of oil and gas industry. *Process safety and environmental protection*, ss. 407-412.
- Statoil. (2013). *The In Amenas attack*. Stavanger: Statoil.
- Stenbro, F. (2019, februar 11). *Politiet fant kniv på to menn som tok seg inn på industriområde i Bodø*. Hentet fra an.no: <https://www.an.no/politiet-fant-kniv-pa-to-menn-som-tok-seg-inn-pa-industriomrade-i-bodo/s/5-4-957385>
- Stranden, R. (2019). *Sikring*. Oslo: Gyldendal.
- Sørensen, F. E. (2018, august 5). *Masteroppgave "Metodikkens betydning for beslutningstaker. En studie med fokus på utviklingen av barrierestyring mot tilsiktede uønskede handlinger."*, Universitetet i Stavanger. Hentet fra Uis.no: <http://hdl.handle.net/11250/2508153>
- Tu, P., Yu, T., Nevatia, R., Gao, D., & Lee, S. (2012). A systems level approach to perimeter protection. *2012 IEEE Workshop on the Applications of Computer Vision (WACV)*, ss. 257-262. Hentet fra IEEE Workshop on the Applications of Computer Vision.
- Turner, B. A. (1976, September). The Organizational and Interorganizational Development of Disasters. *Administrative Science Quarterly*, Vol. 21, No. 3, ss. 378-397.
- Vasudevan, A., & Selvakumar, S. (2015, november). Evolution of a hybrid model for an effective perimeter security device. *Defence science journal* 65 (6), ss. 466-471.
- Xie, J., Sun, K., & Lei, X. (2021, desember). Risk assessment method for power plant industrial control information security based on Bayesian attack graph systems. *Journal of electrical systems*, ss. 529-541.
- You, Y., Cho, I., & Lee, K. (2016, september). An advanced approach to security measurement system. *Journal of supercomputing* 72 (9), ss. 3443-3454.
- Yu, H., & Chang, H. (2020, november). A meta-analysis of industrial security research for sustainable organizational growth. *Sustainability* 12, s. 9526.

Vedlegg 1: Informasjon til informanter i forkant av semistrukturert intervju

Vil du delta i forskningsprosjektet

«Hvordan er påliteligheten til perimetersikringen rundt Industriområdet?»

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å se på påliteligheten til perimetersikringen rundt Industriområdet, og om denne perimetersikringen har tilstrekkelige barrierer for å hindre uønsket inntrengning eller adkomst til industriområdets områder. I dette skrevet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål

I denne masteroppgaven vil formålet være å vurdere Industriområdet ytre perimetersikring, nærmere bestemt områdene som er sikret med industrigjerdet på land. Oppgaven vil ikke ta for seg sikring mot kaianleggene.

Formålet med oppgaven vil være å se på perimetersikringen og dens barrierer sett i et lys av ny, relevant sikkerhetsteori og kunnskap om område- og perimetersikring. Oppgaven vil være en vurdering av om dagens perimetersikring med tilhørende barrierer. Eventuelt peke på områder som kan bidra til å øke perimetersikringen og forslag til nye barrierer.

Oppgaven skrives med følgende problemstilling og tilhørende forskningsspørsmål:

Problemstilling:

«Hvordan er påliteligheten til perimetersikringen rundt Industriområdet?»

Forskningsspørsmål:

1. *Hva slags barrierer etableres for å ivareta perimetersikringen?*
2. *Hvordan er informasjonsflyten blant samvirkerne som opprettholder barrierene?*
3. *Hva truer påliteligheten til dagens perimetersikring?*

Problemstillingen og forskningsspørsmålene kan bli justert underveis i prosjektet.

Hvem er ansvarlig for forskningsprosjektet?

Universitetet i Stavanger er ansvarlig for prosjektet.

Hvorfor får du spørsmål om å delta?

Du er valgt ut som informant til denne oppgaven, fordi du i din stilling er vurdert til å inneha kunnskap og kompetanse, som vil være med på å belyse problemstillingen og forskningsspørsmålene i en grad som vil kunne være med på å besvare disse.

Valg av informanter til denne oppgaven er gjort i samsvar med HESQ manager.

Hva innebærer det for deg å delta?

Ved å delta i dette prosjektet innebærer det at du sier deg villig til å være informant i et intervju, med utgangspunkt i oppgavens problemstilling og de fire forskningsspørsmålene, listet over i dette dokumentet.

Varigheten av intervjuene er satt til ca 1 time. Og vil bli gjennomført som en samtale mellom deg og undertegnede.

Opplysningene du gir i intervjuet vil bli anonymisert og du vil ikke i oppgaven nevnes med navn. Industriområdet vil også anonymiseres i oppgaven.

Jeg vil ta notater under intervjuet som jeg vil bruke i drøftingsdelen av masteroppgaven.

Det er frivillig å delta

Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Deltakelse i dette prosjektet vil ikke påvirke ditt forhold til arbeidsplassen eller arbeidsgiver. Disse ønsker problemstillingen og forskningsspørsmålene belyst, som en prosess i en vurdering av om perimetersikringen av industriområdet per i dag er tilstrekkelig.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger

Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

Opplysningene du gir i intervjuet, vil utelukkende bli brukt som grunnlagsmateriale inn i omtalte masteroppgave.

Ved informasjonsinnsamling og i oppgaven vil du siteres som informant [nummer] og ikke ved navn eller stilling.

Ferdig oppgave vil bli levert til HESQ manager for intern distribusjon til interesserte intervjuobjekter, etter oppgaven er vurdert. Oppgaven vil også kunne bli lagt ut på Universitetet i Stavanger sine biblioteker for gjennomførte masteroppgaver.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?

Dataene slettes når prosjektet avsluttes/oppgaven er godkjent, noe som etter planen er juli – august 2022.

Dette vil være generelle funn og konklusjoner fra oppgaven og ikke opplysninger knyttet tilbake til den enkelte informant.

Alle notater fra intervjuene vil destrueres når oppgaven godkjennes.

Hva gir oss rett til å behandle personopplysninger om deg?

Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra Universitet i Stavanger har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Dine rettigheter

Så lenge du kan identifiseres i datamaterialet, har du rett til:

innsyn i hvilke opplysninger vi behandler om deg, og å få utlevert en kopi av opplysningene
å få rettet opplysninger om deg som er feil eller misvisende
å få slettet personopplysninger om deg
å sende klage til Datatilsynet om behandlingen av dine personopplysninger

Hvis du har spørsmål til studien, eller ønsker å vite mer om eller benytte deg av dine rettigheter, ta kontakt med:

Universitetet i Stavanger ved Bjørn Ivar Kruke, Bjorn.i.kruke@uis.no

Vårt personvernombud: Personvernombud@uis.no

Student: Erik Halvorsen, erikvessia4@gmail.com Tlf: 90022160

Hvis du har spørsmål knyttet til NSD sin vurdering av prosjektet, kan du ta kontakt med:

NSD – Norsk senter for forskningsdata AS på epost (personverntjenester@nsd.no) eller på telefon: 53 21 15 00.

Med vennlig hilsen

Erik Halvorsen

Erik Halvorsen

Student

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet «*Hva er påliteligheten til perimetersikringen rundt Industriområdet*», og har fått anledning til å stille spørsmål. Jeg samtykker til:

- å delta i semistrukturert intervju
- at intervjuer kan komme tilbake med oppfølgingsspørsmål i løpet av studien

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet

(Signert av prosjektdeltaker, dato)

Spørreskjema til semistrukturert intervju i forbindelse med masteroppgave

Masteroppgavens problemstilling:

«Hvordan er påliteligheten til perimetersikringen rundt Industriområdet?»

Masteroppgavens forskningsspørsmål

1. *Hva slags barrierer etableres for å ivareta perimetersikringen?*
2. *Hvordan er informasjonsflyten blant samvirkerne som opprettholder barrierene?*
3. *Hva truer påliteligheten til dagens perimetersikring?*

Disse forskningsspørsmålene kan bli justert i løpet av studien.

Spørsmål som vil bli stilt i intervjuet:

Spørsmålene vil bli utdypet gjennom oppfølgingsspørsmål underveis i intervjuet.

1. **Hvem vil forsøke å ta seg inn på industriområdet?**
2. **Hvorfor vil noen ta seg inn på Industriområdet?**
3. **Hvordan vil noen ta seg inn på Industriområdet?**
4. **Hva skal til for å ta seg inn på Industriområdet?**
5. **Hvilke tiltak/barrierer ligger i perimetersikringen i dag? Hva finnes av sikkerhetsinstallasjoner og systemer?**
6. **Hvem opererer perimetersikringen?**
7. **Hvem har ansvaret for perimetersikringen, installasjon, drift og vedlikehold?**
8. **Når vil noen forsøke å ta seg inn på Industriområdet?**
9. **Hvor tror du det er mest sannsynlig at noen ville forsøkt å ta seg inn på Industriområdet og hvorfor?**
10. **Hvordan oppdager man at noen forsøker å ta seg inn på Industriområdet gjennom perimetersikringen?**
11. **Hva skjer når noen forsøker å ta seg inn på området gjennom perimetersikringen (aktivt forsøk)?**

- 12. Hvilke varslingsrutiner trer i kraft ved brudd på perimetersikringen, ved aktivt forsøk?**
- 13. Hva skjer når man oppdager svekkelse i perimetersikringen?**
- 14. Hvilke varslingsrutiner trer i kraft ved oppdagelse av svekkelse i perimetersikringen?**
- 15. Hva ser du som den største trusselen ved brudd på ytre perimetersikringen, hva tenker du er det verste som kan skje?**
- 16. Hvordan vil du vurdere ytre perimetersikring av Industriområdet i dag?**
 - a. Hva er bra med dagens system?**
 - b. Hva mangler i dagens system?**
- 17. Hvordan jobbes det i samvirket rundt ytre perimetersikring av Industriområdet?**
 - a. Hvem har ansvar for opplæring?**
 - b. Hvem har ansvar for trening (individuelle ferdigheter)?**
 - c. Hvem har ansvar for øving (samtrening)?**
- 18. På hvilken måte spiller ytre perimetersikring inn, som faktor ved nyetableringer på Industriområdet?**
- 19. Hvordan vil du si at Industriområdets krav til perimetersikring samsvarer med leietakernes krav til perimetersikring?**

Takk for at du ønsket å stille som informant til min masteroppgave.

Med vennlig hilsen.

Erik Halvorsen

Masterstudent
Universitetet i Stavanger

Vedlegg 3: kopi av mailutveksling med NSB i forhold til meldepliktig oppgave.

Hei.

Jeg skal skrive en masteroppgave ved Universitetet i Stavanger. I denne masteroppgaven skal jeg intervju ansatte på et industriområde. Disse ansatte vil ikke bli navngitt eller identifisert på noen måte under arbeidet med oppgaven. Industriområdet vil også bli anonymisert i oppgaven, slik at det heller ikke vil være mulig å gjenkjenne informanter ut i fra stilling eller tittel, knyttet til arbeidssted. Notater fra intervjuer vil bli skrevet ned for hånd og destrueres etter endt arbeid med oppgaven og vil bli nummerert med informant nummer, ikke navn.

Er denne masteroppgaven meldepliktig til dere i NSD?

Mvh

Erik Halvorsen

Marianne Høgetveit Myhren <marianne.myhren@sikt.no>

fre. 25. feb., 14:50

til meg, personverntjenester@nsd.no

Hei

Det er kun hvis du skal behandle personopplysninger at du skal melde inn prosjektet for en vurdering hos oss.

Les mer her om hvordan gjennomføre det anonymt her:

<https://www.nsd.no/personverntjenester/oppslagsverk-for-personvern-i-forskning/hvordan-gjennomfore-et-prosjekt-uten-a-behandle-personopplysninger>

Og her kan du lære mer om hvorfor melde, dersom du skal samle inn personopplysninger:

<https://app.xtramile.no/nsdekstern/course/f9d46177-ee95-4980-8c5e-1fb97e67e561>

Jeg håper dette var til hjelp!

Vennlig hilsen

Marianne Høgetveit Myhren

Seksjonsleder Seksjon for personverntjenester Divisjon for forskning og kunnskapsressurser

Telefon: 53 21 15 56/ (+47) 907 67 351 Sikt – Kunnskapssektorens tjenesteleverandør