Masteroppgave

NTNU
Norges teknisk-naturvitenskapelige universitet
Fakultet for informasjonsteknologi og elektroteknikk
Institutt for informasjonssikkerhet og kommunikasjonsteknologi

Alva Herdis Kierulf
Nora Vågsdal

Ikke-tekniske cybersikkerhetsbarrierer for OT-systemer i petroleumsindustrien

Masteroppgave i Kommunikasjonsteknologi og digital sikkerhet
Veileder: Maria Bartnes
Medveileder: Lars Bodsberg og Roy Thomas Selbæk Myhre
Juni 2022

NTNU
Norwegian University of
Science and Technology

Alva Herdis Kierulf
Nora Vågsdal

Ikke-tekniske cybersikkerhetsbarrierer for OT-systemer i petroleumsindustrien

Masteroppgave i Kommunikasjonsteknologi og digital sikkerhet
Veileder: Maria Bartnes
Medveileder: Lars Bodsberg og Roy Thomas Selbæk Myhre
Juni 2022

Norges teknisk-naturvitenskapelige universitet
Fakultet for informasjonsteknologi og elektroteknikk
Institutt for informasjonssikkerhet og kommunikasjonsteknologi

NTNU

Kunnskap for en bedre verden

NTNU

Ikke-tekniske cybersikkerhetsbarrierer for OT-systemer i petroleumsindustrien

Alva Herdis Kierulf og
Nora Vågsdal

Innleveringsdato: juni 2022
Veileder: Maria Bartnes, NTNU
Medveiledere: Lars Bodsberg, SINTEF og
Roy Thomas Selbæk Myhre, Sopra Steria

Norges teknisk-naturvitenskapelige universitet
Institutt for informasjonssikkerhet og kommunikasjonsteknologi

Tittel: Ikke-tekniske cybersikkerhetsbarrierer for OT-systemer i petroleumsindustrien

Studenter: Alva Herdis Kierulf og Nora Vågsdal

Problembeskrivelse:

Petroleumsindustrien er en av de viktigste sektorene for norsk økonomi. I likhet med resten av samfunnet, blir også petroleumsindustrien påvirket av den pågående digitaliseringen. Industrielle kontrollsystemer som tidligere har vært fysisk adskilt fra omverdenen, blir koblet sammen med internett. Når informasjonsteknologi (IT) og operasjonsteknologi (OT) konvergerer, fører dette til nye utfordringer for OT-systemene. Angrepsflaten blir større og nye trusler blir introdusert. Dette innebærer at petroleumsindustrien må gå fra å kun vektlegge *safety* og tilfeldige feil, til å også ha fokus på *security* og målrettede angrep.

I fysiske OT-systemer bruker man begrepet barrierer om tiltak som iverksettes for å hindre uønskede hendelser. Barrierebegrepet blir lite brukt innenfor cybersikkerhet. For at det skal bli enklere å ta i bruk cybersikkerhetstiltak i OT-systemer, kan det være en fordel om disse tiltakene også kan beskrives som barrierer. I dette prosjektet ønsker vi å se på utvikling av ikke-tekniske barrierer for å håndtere relevante cybersikkerhetsscenarioer. For å undersøke problemstillingen skal vi bruke metoden teknologivitenskap (Design Science). Dette innebærer arbeid i tre faser, en undersøkelsesfase, en utviklingsfase og en testfase. Fasene vil inkludere en litteraturstudie, utvikling av barrierer og samtaler med ressurspersoner i industrien for å få tilbakemeldinger.

Gjennom prosjektet vil vi bidra til å tette gapet mellom IT og OT ved å undersøke hvordan barrierekonseptet kan anvendes også for cybersikkerhet. Ved å forene sikkerhetstiltak fra IT og OT kan man oppnå en mer helhetlig tilnærming til sikkerhet. Hensikten er at det skal bli enklere for industrien å implementere ikke-tekniske barrierer for å oppdage, avverge og håndtere cybersikkerhetsangrep mot OT-systemer.

Godkjent: 2022-02-14

Veileder: Maria Bartnes, NTNU

Medveiledere: Lars Bodsberg, SINTEF og Roy Thomas Selbæk Myhre, Sopra Steria

Abstract

The petroleum industry is becoming more and more digitalized, which leads to a convergence between IT and OT systems. This results in an expanded threat picture for OT systems as it now also includes cyber security threats. Traditionally, OT systems have focused on safety by securing physical assets and preventing accidents. Because of the convergence, it is necessary to also consider security, by securing data and information.

A barrier is a measure to prevent or reduce the consequence of unwanted events. Barriers are used in safety management for OT systems, but it is less common to use the barrier concept for cyber security. This thesis investigates if the barrier concept can be applied to cyber security. As technical measures alone are not enough to handle cyber attacks, we have considered non-technical barriers in our thesis.

We have used design science as our research design, which includes an analysis phase, an innovation phase and an evaluation phase. To gather information, we performed a literature review and completed several inteviews with representatives from the industry. In the innovation phase we started with a ransomware attack against an OT system in the petroleum industry. We identified non-technical barriers that could prevent or reduce the consequence of the attack. One part of the thesis included investigating what requirements from ISA/IEC 62443-2-1 that should be covered by the non-technical barriers. Then, we generalized the method we used to identify the barriers so that the method could be used for other attack scenarios. The result became MICS, a method for identifying non-technical cyber security barriers.

MICS is intended to be used for analyzing new attack scenarios before or after they have happened. The method involves that the scenario shall be detailed according to the MITRE framework to get an overview over the different steps an attacker performs during an attack. By including requirements from ISA/IEC 62443-2-1 in MICS, it will contribute to make it easier for the industry to apply the standard.

With MICS we have identified non-technical barriers for cyber security, and this shows that the barrier concept can be used on cyber security measures.

Sammendrag

Petroleumsindustrien blir stadig mer digitalisert, noe som fører til en sammenkobling av IT- og OT-systemer. Sammenkoblingen fører til at trusselbildet til OT-systemene utvides til å også omfatte cybersikkerhetstrusler. Tradisjonelt har sikkerhet for OT-systemer handlet om *safety*, ved å sikre fysiske verdier og hindre ulykker. Med økt sammenkobling blir det nødvendig å også vurdere *security*, ved å sikre data og informasjon.

En barriere er et tiltak for å hindre eller minske konsekvensene av uønskede hendelser. Barrierer brukes i sikkerhetsstyring for OT-systemer, men det har vært mindre vanlig å se på bruk av barrierekonseptet for cybersikkerhet. Oppgaven ser på hvordan barrierekonseptet kan brukes for cybersikkerhet. Ettersom tekniske tiltak i seg selv ikke er nok til å håndtere cyberangrep, har vi sett på ikke-tekniske barrier.

Vi har brukt teknologivitenskap som undersøkelsesdesign, med en analysefase, en nyskapningsfase og en evalueringsfase. For å samle inn informasjon har vi gjort en litteraturstudie og gjennomført samtaler med representanter fra industrien i flere runder. I nyskapningsfasen tok vi utgangspunkt i et *ransomware*-angrep mot et OT-system i petroleumsindustrien. Videre identifiserte vi ikke-tekniske barrierer som kunne hindre eller minske konsekvensene av angrepet. En del av oppgaven inkluderte også å undersøke hvilke krav fra ISA/IEC 62443-2-1 som bør være dekket av de ikke-tekniske barrierene. Deretter ble metoden vi brukte for å identifisere barrierene generalisert slik at den kunne brukes for andre angrepsscenarioer. Resultatet av arbeidet var MICS, en metode for identifisering av ikke-tekniske cybersikkerhetsbarrierer.

MICS kan brukes til å analysere nye angrepsscenarioer før eller etter de har skjedd. Metoden innebærer at scenarioet skal detaljeres i henhold til MITRE-rammeverket for å få oversikt over de ulike stegene en angriper må gå gjennom for å utføre angrepet. Hensikten er å se hvor man bør sette inn barrierer for å stoppe angrepet. Ved å i tillegg inkludere krav fra ISA/IEC 62443-2-1 i MICS vil det bidra til at industrien lettere kan anvende standarden.

Med MICS har vi identifisert ikke-tekniske barrierer for cybersikkerhet, noe som viser at barrierebegrepet er mulig å anvende på cybersikkerhetstiltak.

Forord

Denne masteroppgaven er skrevet våren 2022 som vår avsluttende del av studiet Kommunikasjonsteknologi og digital sikkerhet ved Institutt for informasjonssikkerhet og kommunikasjonsteknologi (IIK) ved Norges teknisk-naturvitenskapelige universitet (NTNU).

Vi ønsker å takke våre veiledere, Maria Bartnes, Lars Bodsberg og Roy Thomas Selbæk Myhre, for hjelp og gode råd underveis, i tillegg til deling av kunnskap og entusiasme rundt oppgaven. Vi ønsker også å rette en stor takk til alle som lot seg intervjue i forbindelse med oppgaven. Dere ga oss verdifull kunnskap som har økt vår forståelse for temaet, i tillegg til gode innspill som har bidratt til resultatet i denne oppgaven.

Til slutt ønsker vi å takke venner og familie for støtte og råd gjennom våren.

Alva Herdis Kierulf & Nora Vågsdal
Trondheim, 2022

Innhold

Figurer

Tabeller

Akronymer

DMZ Demilitarized Zone.

DoS Denial of Service.

IACS Industrial Automation and Control Systems.

ICS Industrial Control Systems.

IDS Intrusion Detection System.

IIoT Industrial Internet of Things.

IKT Informasjons- og kommunikasjonsteknologi.

IT Informasjonsteknologi.

MICS Metode for identifisering av Ikke-tekniske CyberSikkerhetsbarrierer.

NTNU Norges teknisk-naturvitenskapelige universitet.

OT Operasjonell teknologi.

PST Politiets sikkerhetstjeneste.

SCT Safety Critical Task.

SL Security Levels.

SOC Security Operations Center.

VPN Virtuelt privat nettverk.

YPF Ytelsespåvirkende faktor.

Forklaring av begreper

Begrep	Definisjon/beskrivelse
Barriere	Et tiltak som skal hindre eller minske konsekvensene av uønskede hendelser.
Barriereelement	Tiltak eller løsninger som bidrar til å realisere en barrierefunksjon.
Barrierefunksjon	Hva barrieren skal gjøre eller oppgaven den skal løse.
Cybersikkerhet	Beskyttelse av systemer som utsettes for risiko ved å være koblet til internett.
Ikke-teknisk barriere	De barrierene der barriereelementet er operasjonelt eller organisatorisk.
IT-system	Systemer som har som hovedoppgave å behandle data og informasjon.
Malware	Programvare som kan gjøre endringer på systemer eller informasjon uten eiers godkjennelse.
OT-system	Systemer som har som hovedoppgave å styre eller overvåke industrielle prosesser.
Phishing	En angriper forsøker å lure et offer til å utføre en handling, som oftest via e-post.
Ransomware	En type malware som krypterer filer og gjør de utilgjengelige. Angriperen ber om løsepenger for å åpne tilgang til filene.
Safety	Hindre eller redusere omfanget av ulykker, og sikre fysiske verdier.
Security	Sikring av systemer slik at uvedkommende ikke får tilgang til data og informasjon.
Ytelsespåvirkende faktor	Faktor som er avgjørende for at en barriere skal fungere som tiltenkt.

Tabell 0.1: Forklaring av begreper brukt i oppgaven.

Kapittel 1
Introduksjon

Petroleumsindustrien er svært viktig for det norske samfunnet og den norske økonomien, da den sysselsetter omtrent 200 000 nordmenn [NP21]. I tillegg gir den totale omsetningen fra olje og gass den norske stat flere milliarder kroner årlig. Inntektene fra petroleumsindustrien bidrar med 304 av totalt 1553 milliarder kroner til statsbudsjettet, noe som betyr at sektoren alene står for nærmere 20% av Norges inntekter [SB21].

I tråd med den økende digitaliseringen av samfunnet blir også petroleumsindustrien stadig mer digitalisert. Petroleumsindustrien benytter både operasjonelle teknologisystemer (OT-systemer) og informasjonsteknologi-systemer (IT-systemer). OT-systemer styrer og overvåker industrielle prosesser, mens IT-systemer har som hovedoppgave å behandle data og informasjon [MOL+21]. Tradisjonelt har OT-systemene vært isolert fra de administrative IT-systemene, men økt digitalisering i industrien gjør at systemene i større og større grad kobles sammen. Sammenkoblingen fører til at cybersikkerhetstrusler som tidligere kun har vært knyttet til tradisjonelle IT-systemer, for eksempel *ransomware*[1] som spres gjennom åpne nettverk, nå blir relevante for OT-systemer. For OT-systemer skaper sammenkoblingen et nytt trusselbilde ettersom man her tradisjonelt har fokusert på tilfeldige feil og ikke målrettede angrep [JWBK21].

Dersom systemer i petroleumsindustrien blir skadet, kan det ha store konsekvenser for både økonomi, miljø og fysisk sikkerhet. Økonomiske konsekvenser kan komme i form av stopp i produksjon, tapte ressurser og ødelagt utstyr. Dersom en skade fører til oljesøl, vil det ha negative følger for miljøet og naturen. Skader kan også føre til ulykker som i verste fall kan ha fatale konsekvenser for mennesker som befinner seg i nærheten av systemene når ulykken inntreffer [JWBK21; HØ16; CKL21; ISA22]. Petroleumsindustrien er derfor avhengig av å beskytte systemene sine både fra utilsiktede ulykker og fra målrettede angrep.

[1] Løsepengevirus, utpressingsprogramvare.

I sikkerhetsstyring for OT-systemer anvendes begrepet barriere om tiltak som settes i verk for å hindre eller minske omfanget av en uønsket hendelse. En barriere består av en barrierefunksjon, hva barrierene skal gjøre, og et barriereelement, hvem eller hva som bidrar til å realisere funksjonen. Barrierer oppnår sin funksjon enten ved tekniske, operasjonelle eller organisatoriske elementer [PSA17; ØWFR14; HØST15]. I oppgaven blir operasjonelle- og organisatoriske tiltak sett på sammen med fellesbetegnelsen "ikke-tekniske barrierer". Barrierebegrepet er lite brukt innen cybersikkerhet, men ettersom begrepet allerede er i bruk innen *safety*, kan det være fordelaktig å fortsette å benytte barrierebegrepet og implementere cybersikkerhetstiltak på samme format [KV21].

Tekniske barrierer er ikke tilstrekkelig for å håndtere cyberangrep og dermed kan mennesker være nødvendig for å håndtere hendelsene [GPMH]. Det er viktig å ha fokus på prosesser i virksomheten og sikkerhetskultur blant brukere og ansatte [NSM21a]. Samtidig understrekes det at det er mindre rett frem å identifisere ikke-tekniske barrierer enn tekniske, i tillegg til at det gjerne finnes færre av de ikke-tekniske barrierene [HØ16].

ISA/IEC 62443 er en cybersikkerhetsstandard for OT-systemer [Dav18] som anvendes for cybersikkerhet i petroleumsindustrien. Selv om standarden beskriver overordnede krav for å sikre systemene sine, kan det være vanskelig for industrien å se hvordan den kan anvendes i praksis [HOJ+21]. Barrierebegrepet kan være nyttig for å konkretisere og tydeliggjøre standardens tiltak mot cyberangrep.

1.1 Forskningsspørsmål

I oppgaven undersøkes det hvordan barrierekonseptet kan anvendes også for cybersikkerhet. Målet er å finne ut hvordan man kan identifisere ikke-tekniske cybersikkerhetsbarrierer. Barrierene som identifiseres skal hindre relevante cyberangrep, i tillegg til å bidra med å oppfylle krav fra ISA/IEC 62443. Oppgaven skal besvare følgende forskningsspørsmål (FS) med tilhørende delspørsmål (DS 1 og DS 2):

> ***FS:*** *Hvordan kan ikke-tekniske cybersikkerhetsbarrierer identifiseres ut fra relevante angrepsscenarioer for petroleumsindustrien?*
>
> ***DS 1:*** *Hvilke ikke-tekniske barrierer er relevante for et ransomware-angrep mot et OT-system i petroleumsindustrien?*
>
> ***DS 2:*** *Hvilke krav fra ISA/IEC 62443-2-1 bør være dekket av de ikke-tekniske cybersikkerhetsbarrierene?*

Vi skal utvikle en generell metode for å identifisere ikke-tekniske barrierer. For å utvikle metoden tas det utgangspunkt i et spesifikt angrepsscenario og det identifiseres barrierer til det valgte scenarioet. Dette er formålet med DS 1. Videre kan det være nyttig for industrien om barrierene bidrar til å oppfylle krav i ISA/IEC 62443. Barrierene kan bli en del av å konkretisere standarden slik at den blir mer anvendelig i praksis. DS 2 er altså inkludert for å verifisere at metoden identifiserer nyttige barrierer. Det spesifikke svaret fra DS 1 vil brukes som et utgangspunkt til å finne en generell metode. Svaret fra DS 2 vil bidra til at metoden som utvikles gir ytterligere nytteverdi for industrien. DS 1 og DS 2 vil bidra til å svare på FS.

For å finne relevante angrepsscenarioer for petroleumsindustrien tar vi utgangspunkt i scenarioer utarbeidet i masteroppgaven "Preparedness Exercises for Cyber Attacks Against Industrial Control Systems in the Petroleum Industry" fra 2021 [SH21]. Et av resultatene fra oppgaven var scenariobeskrivelser av realistiske cyberangrep mot petroleumsbransjen.

1.2 Avgrensninger

Oppgaven er avgrenset til å kun identifisere ikke-tekniske barrierer for cybersikkerhet. For å identifisere barrierene tar vi utgangspunkt i angrepsscenarioer. De mulige angrepsscenarioene er avgrenset til et lite utvalg fordi oppgaven har et begrenset tidsomfang. Ved identifisering av barrierene er det ikke tatt hensyn til enheter som kobles til systemene utenfra (*remote access*[2]). I tillegg er det kun sett på barrierer der barrierefunksjonene skal utføres under et angrep for å hindre konsekvensene av angrepet.

Som en del av å teste resultatmetoden undersøkes det om de identifiserte barrierene bidrar til å oppfylle ulike ikke-tekniske krav i ISA/IEC 62443-2-1. Vi forholdt oss kun til utvalgte deler av én standard. Dette kan være begrensende ettersom man ved å inkludere for eksempel informasjonssikkerhetsstandarder som ISO/IEC 27000-serien kan få andre type verifiseringer av resultatmetoden.

Det er også gjort avgrensninger i hvilke av barriere-begrepene det er lagt vekt på. Hovedfokuset er på barrierefunksjonen og barriereelementer. Ytelsespåvirkende faktorer er lagt til som eksempler på noen av barrierene, men er ikke nødvendigvis fullstendige. I tillegg er oppgaven avgrenset til å ikke se på ytelseskrav, noe som i praksis er en viktig del av barrierestyringen.

[2] Fjerntilgang.

1.3 Disposisjon

Under følger en oversikt over kapitlene oppgaven er delt inn i.

Kapittel 2 inneholder bakgrunnsinformasjon og relatert arbeid som er relevant for oppgaven.

Kapittel 3 beskriver hvilken forskningsmetode som ble anvendt for å svare på forskningspørsmålene. Dette inkluderer gjennomføring av en litteraturstudie, utvikling av barrierer og resultatmetode, og samtaler med representanter fra industrien.

Kapittel 4 presenterer resultatet vi kom frem til. Dette inkluderer relevante krav fra ISA/IEC 62443-2-1, resultatmetoden som ble utviklet for å identifisere ikke-tekniske cybersikkerhetsbarrierer og et detaljert eksempel på barrierer identifisert til et spesifikt angrepsscenario. I tillegg finnes validering av resultatmetoden.

Kapittel 5 diskuterer de identifiserte barrierene, utvelgelsen av krav fra ISA/IEC 62443-2-1, resultatmetoden og resultatene fra intervjuene. Her diskuteres det rundt de to delspørsmålene DS 1 og DS 2, samt forskningsspørsmålet FS.

Kapittel 6 konkluderer oppgaven basert på diskusjonen, i tillegg til å presentere videre arbeid.

Tillegg A inneholder de valgte angrepsscenarioene fra masteroppgaven "Preparedness Exercises for Cyber Attacks Against Industrial Control Systems in the Petroleum Industry", her oversatt til norsk.

Tillegg B inkluderer intervjuspørsmålene som ble stilt til representanter fra industrien.

Tillegg C presenterer ikke-tekniske krav i ISA/IEC 62443-2-1.

Tillegg D presenterer tekniske krav i ISA/IEC 62443-2-1.

Kapittel 2
Bakgrunn og relatert arbeid

Kapittel 2 presenterer relevant bakgrunnsinformasjon for oppgaven, i tillegg til tidligere arbeid relatert til barrierer for cybersikkerhet og ikke-tekniske barrierer. I kapittel 2.1 forklares begrepene IT og OT, før trusselbildet for petroleumsindustrien presenteres i kapittel 2.2. Videre tar kapittel 2.3 og 2.4 for seg barrierer og barrierestyring, mens kapittel 2.5 går inn på tidligere arbeid med cyberbarrierer. Kapittel 2.6 ser på fordeler og ulemper ved menneskelig ytelse. Til slutt presenterer kapittel 2.7 og 2.8 henholdsvis bruken av standarder i bransjen og rammeverket MITRE.

2.1 IT og OT

Operasjonelle teknologi-systemer (OT-systemer) er systemer som har som hovedoppgave å styre eller overvåke industrielle prosesser. Andre begreper som blir brukt om OT-systemer er for eksempel industrielle informasjons- og kommunikasjonsteknologi (IKT)-systemer, industrielle kontrollsystemer[1] og industrielle automasjons- og kontrollsystemer[2]. Slike systemer blir brukt i blant annet petroleumsindustrien. OT-systemer overvåker og styrer fysiske tilstander ved hjelp av for eksempel sensorer, ventiler og pumper [JWBK21]. OT-systemer skiller seg fra informasjonsteknologi-systemer (IT-systemer) som har som oppgave å behandle data og informasjon [MOL+21], ved hjelp av maskin- og programvare som lagrer, prosesserer og overfører data [JWBK21]. I denne oppgaven benyttes forkortelsene IT og OT om de ulike typene systemer.

Et tydelig skille mellom IT og OT, er at OT-systemer ofte er utviklet til spesifikke formål. IT-systemer er på sin side ofte hyllevare som utvikles til generelle formål og som enkelt kan erstattes [CO22]. Det er også tradisjonelt stor forskjell på hvordan man håndterer feil i IT- og OT-systemer. IT-systemer kan startes på nytt og oppdateres ofte, mens for OT-systemer forsøker man å unngå at systemene må startes på nytt.

[1] Engelsk: Industrial Control Systems (ICS).
[2] Engelsk: Industrial Automation and Control Systems (IACS).

Dette er fordi OT-systemer ofte styrer prosesser med høyt skadepotensiale slik at nedetid og tap av kontroll kan være kritisk [JWBK21].

IT og OT tilnærmer seg arbeid med cybersikkerhet på ulike måter. Fordi IT-systemer behandler data og informasjon, ligger hovedfokuset på å forhindre at angripere får tak i denne informasjonen [MOL+21]. For IT-systemer har man dermed vektlagt *security*, som handler om hvorvidt omgivelsene har mulighet til å utføre skade på systemet og informasjonen i systemet [LRNT06]. OT-systemer har på sin side fokusert på å beskytte ressurser, sikre kontinuerlig drift og hindre ulykker [JWBK21]. Hovedfokuset har dermed vært på *safety*, altså hvorvidt systemet har mulighet til å utføre skade på omgivelsene [LRNT06]. Hovedfokuset for sikkerhet i IT-systemer ligger altså på å beskytte digitale verdier, mens i OT-systemer har det å sikre fysiske verdier og hindre ulykker vært prioritert. Tabell 2.1 viser noen forskjeller mellom IT- og OT-systemer.

	IT	**OT**
Brukes til	Å ha kontroll over informasjon [JWBK21], samt å overvåke, administrere og sikre kjernefunksjoner, som epost, i en bedrift [CO22].	Å ha kontroll over fysiske prosesser [JWBK21], derunder å koble til, overvåke, administrere og sikre industrielle operasjoner [CO22].
Fokuserer på	Å beskytte informasjon [JWBK21].	Å opprettholde kontroll og kontinuerlig drift [JWBK21].
Generaliserbarhet	IT-systemer er vanligvis hyllevare og de er som regel ikke uerstattelige [CO22].	OT-systemer spesialtilpasses den bruken de er tiltenkt [JWBK21].
Ytelse	Mål: raske systemer [Zur21].	Mål: sanntidssystemer [Zur21].
Levetid	$<$ 3-5 år [Zur21].	$>$ 20 år [Zur21].
Oppdatering av systemene	Ofte, gjerne automatisk [Zur21].	Sjeldent [Zur21].

Tabell 2.1: Oversikt over forskjeller mellom IT- og OT-systemer.

2.1.1 IT og OT konvergerer

Det pågår en utvikling der industrien blir digitalisert og automatisert. Utviklingen kan kalles for "industri 4.0" [NSM21a] eller "den fjerde industrielle revolusjonen" [TN21]. En del av utviklingen for OT-systemer, er at systemene i større og større grad blir kombinert med tradisjonelt IT-utstyr [NSM21a]. Opprinnelig har OT-systemene vært isolert fra de administrative IT-systemene, men med økt fokus på digitalisering og automatisering i industrien blir disse systemene koblet sammen [JWBK21]. Ved

å koble IT sammen med OT oppnår man bedre ytelse, produktivitet og energieffektivitet i kontrolleringen av fysiske prosesser [CWKL20; CKL21]. For å kunne eksportere sanntidsdata og informasjon fra OT-systemene, og dermed bidra til økt effektivisering, ser man økt bruk av sensorteknologi, 5G og *Industrial Internet of Things (IIoT)*[3] [NSM21a; TN21].

Sammenkoblingen av IT og OT gjør at cybersikkerhetstrusler som tidligere har vært knyttet til tradisjonelle IT-systemer nå blir relevante for OT-systemer. Disse nye truslene må petroleumsindustrien håndtere for å sikre sine systemer. Økt tilkobling øker angrepsflaten, og gjør at de tilkoblede IT-systemene blir en mulig angrepsvektor mot OT-systemer. Et eksempel på en ny type trussel i OT-systemer er *malware*[4] som kan infisere systemene via internett [Dra19]. For OT-systemer har fokuset primært vært på tilfeldige feil og ikke på målrettede angrep, så denne sammenkoblingen skaper et nytt trusselbilde [JWBK21].

Anlegg i petroleumsindustrien er avhengige av at OT-systemene sikrer trygg drift. Driften blir sikret ved at programvare kombineres med sensorer, ventiler eller pumper for å regulere fysiske tilstander og variabler, for eksempel trykk eller varme. Dersom variablene i systemene avviker for mye fra ønskede verdier kan det føre til store ødeleggelser [JWBK21]. Feil i programvare, som kan bli forårsaket av cybersikkerhetshendelser, kan få fysiske konsekvenser og det blir dermed viktig å ha kontroll på informasjonsflyten for å hindre skade på mennesker og omgivelser [CKL21].

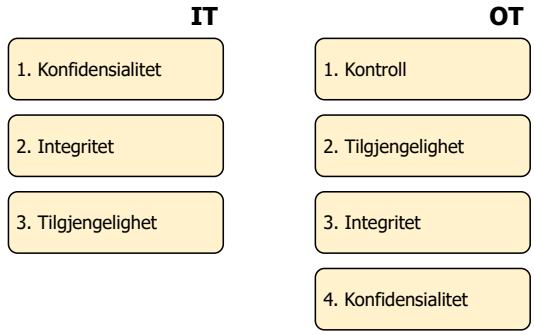
2.1.2 Cybersikkerhet i IT og OT

IT og OT har ulike prioriteringer for hvilke sikkerhetsattributter som anses som viktigst. Innenfor IT vektlegges, i prioritert rekkefølge, konfidensialitet, integritet og tilgjengelighet. Konfidensialitet handler om at data kun skal være tilgjengelig for de som er autorisert til å ha tilgang. Integritet handler om at man skal kunne stole på at data og informasjon er det de utgir seg for å være og ikke kan utsettes for uautorisert endring. Tilgjengelighet handler om at tjenester og data alltid er tilgjengelig for autoriserte brukere når det er nødvendig. For IT-systemer regnes tilgjengelighet som mindre kritisk, og en viss mengde nedetid blir gjerne godtatt [LRNT06; JWBK21].

For OT-systemer er vektleggingen annerledes, og prioriteringsrekkefølgen blir kontroll, tilgjengelighet, integritet og konfidensialitet. Kontroll er et hovedmål for OT-systemene, og har dermed høyest prioritet. Videre regnes tilgjengelighet som avgjørende, da nedetid fører til tap av kontroll, og kan få fatale konsekvenser. Integritet er også viktig, mens konfidensialitet blir prioritert nederst [JWBK21]. Konfidensialitet regnes som mindre viktig, blant annet fordi det er snakk om rådata som uansett må

[3] Det industrielle Tingenes internett.
[4] Skadevare.

analyseres i en gitt kontekst for å ha verdi [Gro]. De ulike prioriteringene for IT og OT er illustrert i figur 2.1.



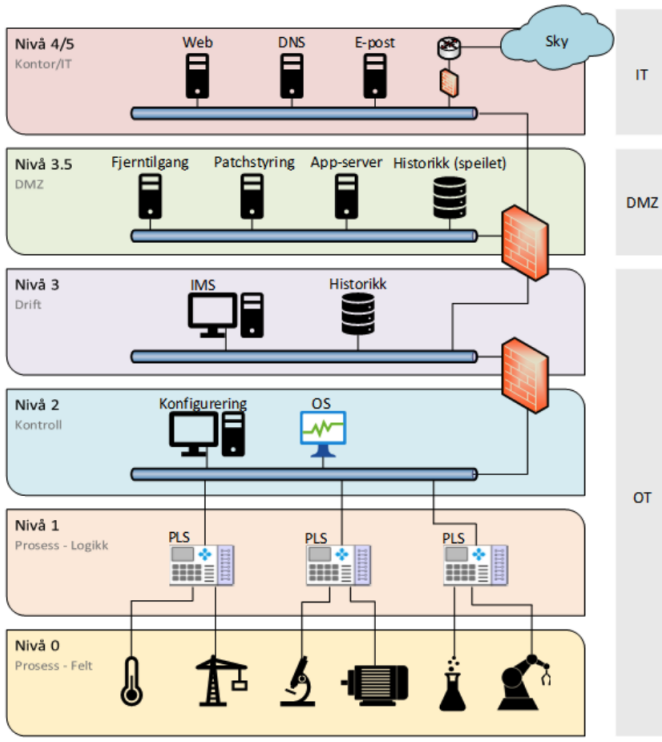
Figur 2.1: Prioritering av sikkerhetsattributter i IT og OT. Figuren er adaptert fra [JWBK21].

Ulik prioritering av sikkerhetsattributter påvirker hvordan cybersikkerhetshendelser blir håndtert i henholdsvis IT- og OT-systemer. Hvis et IT-system blir angrepet, vil man stenge ned den delen av systemet som er angrepet i sin helhet. Siden oppetid er kritisk for OT-systemer, vil svaret på et angrep være å fortsette driften, men prøve å isolere trusselen [ISA20]. Når cybersikkerhetstiltak implementeres for OT er det viktig at tiltakene ikke kan føre til at essensielle tjenester og funksjoner slutter å fungere. Det er derfor viktig at det defineres hvilke tjenester og funksjoner som er kritiske for driften. Av og til kan det godtas at et cybersikkerhetstiltak medfører at en ikke-kritisk funksjon er midlertidig nede, mens en kritisk funksjon aldri skal påvirkes negativt [ISA22].

Oppdatering av systemer er et viktig tiltak for å være best mulig beskyttet mot angrep, men der IT-systemer kan sikkerhetsoppdateres ofte, er OT-systemer mye mindre fleksible. OT-systemer kan bestå av komponenter som ikke kan, eller ikke bør, oppdateres. Dette kan være komponenter som styrer kritiske prosesser og dermed ikke bør forstyrres av oppdateringer, eller komponenter som kjører med spesialtilpasset programvare der det ikke eksisterer oppdateringer. Hvis det likevel er mulig å oppdatere, må oppdateringen verifiseres før installering for å sikre at den ikke innfører problemer for systemene [JWBK21]. Sikkerhetshendelser oppstår ofte på grunn av svakheter i systemene som det allerede finnes oppdateringer for. Derfor er det gunstig å oppdatere systemene så ofte som mulig. Utfordringene knyttet til oppdatering, fører derfor til et dilemma for de som drifter OT-systemene [KO20].

2.1.3 Nettverkstopologi for et OT-system

Et eksempel på hvordan et OT-system kan være delt opp er vist i figur 2.2. Figuren viser hvordan IT-nettverket er separert fra OT-nettverket med en *Demilitarized Zone (DMZ)*[5]. Det er regnet som god praksis å ha en slik sone [Woo] for å beskytte OT-systemet på et overordnet nivå ved å tvinge all kommunikasjon inn og ut av systemet til å gå gjennom DMZ. DMZ er isolert fra OT- og IT-nettverk ved hjelp av brannmurer. Videre viser figur 2.2 de ulike nivåene nettverket er delt inn i. Sone 4/5 er kontornettverket, som vil være koblet til eksterne systemer via en brannmur. Nivå 3.5 er DMZ som inneholder brannmurer som kontrollerer trafikk mellom nivå 4 (IT) og nivå 3 (OT). På nivå 3 inngår ekspert- og vedlikeholdssystemer, samt servere for lagring av data. Nivå 2 er et nettverk av operatørstasjoner og servere for datautveksling og -presentasjon, mens nivå 1 er et nettverk av kontrollere for prosess- og sikkerhetssystemer med tilhørende servere for utveksling av data. På nivå 0 befinner de fysiske prosessene og utstyr som brukes til styring og overvåkning seg [JWBK21].



Figur 2.2: Nettverkstopologi for OT-system. Figuren er hentet fra [JWBK21].

[5]Demilitarisert sone.

2.2 Trusselbildet i petroleumsindustrien

Det digitale risikobildet i Norge er komplekst og i stadig endring [NSM21a]. De siste årene er det observert en tredobling av cyberangrep mot norske offentlige og private virksomheter, og Politiets sikkerhetstjeneste (PST) understreker at nettverksoperasjoner utgjør en alvorlig og vedvarende trussel mot Norge [PST22a]. Trusselaktørene omfatter blant annet kriminelle og statlige aktører, der særlig trusselen fra statlige aktører anses som mer og mer alvorlig [NSM21a; PST22a]. PST vurderer at etterretningstrusselen fra særlig Russland har økt som følge av krigen i Ukraina [PST22b]. Mer spesifikt er norsk petroleumsindustri utsatt for etterretningsaktivitet som kan resultere i et stort og langsiktig skadeomfang for Norge [PST20].

På verdensbasis er det et økende antall angripere som retter seg mot petroleumsindustrien [Dra22]. Sammenkoblingen av IT- og OT-nettverk fører til at OT-systemer blir mer eksponert mot digitale trusler [TN21], noe som er med på å øke sårbarhetsflaten til OT-systemene. Angrep på OT-systemer i petroleumsindustrien kan få alvorlige konsekvenser og kan resultere i bortfall av kritiske samfunnsfunksjoner [NSM21a]. Petroleumsindustrien forvalter store verdier og angripere forsøker å utnytte OT-miljøene blant annet for å tilegne seg disse. Alle deler av olje- og gassproduksjonen er utsatt for trusler, men raffinering av olje og distribusjon til kunder anses som de viktigste målene for angripere [Dra22].

Angripere som retter seg mot petroleumsindustrien kan utnytte informasjon og systemer som er eksponert mot internett, samt skaffe seg *remote access* eller utnytte usikre leverandør eller tredjepartstilganger. Dette vil kunne introdusere betydelig risiko for systemene og driften [Dra22]. En av truslene som øker risikoen for OT-systemene er *ransomware*. Undersøkelser Dragos har gjennomført viser at antallet *ransomware*-angrep mot OT-systemer økte med 500% mellom 2018 og 2022. 5% av disse var rettet mot systemer innen olje og gass. Man ser også at angripere i større grad utvikler *ransomware* som er spesifikt rettet mot å stanse industrielle prosesser i OT-systemer [Dra22].

I desember 2020 ga Waterfall Security Solutions ut en liste med "The Top 20 Cyber Attacks On Industrial Control Systems"[6]. Listen presenterer de 20 angrepene som vurderes som mest aktuelle for industrielle kontrollsystemer [Gin20]. To angrepstyper som går igjen på listen er *ransomware*-angrep og innsideangrep. Samtidig initieres mange av angrepene av *phishing*[7].

Våren 2021 skrev Guro Hotvedt og Andrea Neverdal Skytterholm masteroppgaven "Preparedness Exercises for Cyber Attacks Against Industrial Control Systems in the Petroleum Industry" [SH21] som avsluttende del av sin studie Kommunikasjons-

[6] "Topp 20 cybersikkerhetsangrep mot industrielle kontrollsystemer".
[7] Nettfisking.

teknologi og Digital sikkerhet ved NTNU. I oppgaven så de på beredskapstrening for cyberangrep mot OT-systemer i petroleumsindustrien. Oppgaven undersøkte hva som karakteriserer realistiske scenarioer for petroleumsindustrien for så å utvikle eksempelscenarioer som det kan være hensiktsmessig å trene på å håndtere. Resultatet av oppgaven var, blant annet, at *ransomware*- og ulike innside-angrep var realistiske for petroleumsindustrien. Scenarioene som ble utviklet er en del av å eksemplifisere trusselbildet og å kartlegge relevante trusler.

De neste delkapitlene tar for seg de tre overordnede angrepstypene *malware*, innsideangrep og *phishing*. Dette er aktuelle og reelle cyberangrep for petroleumsindustrien som går igjen i angrepene fra "The Top 20 Cyber Attacks On Industrial Control Systems". Samtidig er angrepene sentrale i angrepsscenarioene som brukes i denne oppgaven. I tillegg vurderer vi at ikke-tekniske tiltak kan bidra til å forhindre disse angrepstypene, blant annet fordi angriper her utnytter menneskelige svakheter [DNV16].

2.2.1 Malware

Malware er et begrep som beskriver programkode som kan utføre endringer på systemer eller informasjon uten at eieren av systemet har gitt tillatelse til det [Nät19]. *Malware* kommer vanligvis inn i systemer ved å spre seg via et nettverk, gjennom flyttbare lagringsmedier eller gjennom mennesker. Å utnytte mennesker ved hjelp av *social engineering*[8] blir mer og mer utbredt [DNV16].

Ransomware

Ransomware ses ofte på som en type *malware* som krypterer filer på en datamaskin eller i et nettverk slik at filene blir utilgjengelige. Angriperen krever typisk betaling for å dekryptere filene [Bar22; FBI22]. Et *ransomware*-angrep kan være tilfeldig eller målrettet. I de tilfeldige *ransomware*-angrepene lastes viruset ned ved et uhell og utnytter kjente sårbarheter for å spre seg og kryptere innhold. I de målrettede angrepene retter angriperen seg mot en bestemt person eller bedrift og forsøker å lure de til å laste ned *ransomware*. Angriperen kan eksempelvis lure en ansatt med en *phishing*-e-post med et ondsinnet vedlegg [Gin20].

Tidligere *ransomware*-angrep

Det har vært flere tilfeller av *ransomware*-angrep mot OT-systemer i løpet av de siste årene. To av angrepene, angrepet mot Norsk Hydro i 2019 og angrepet mot Colonial Pipeline i 2021, er presentert i dette kapittelet.

Angrepet på Norsk Hydro. I mars 2019 ble Norsk Hydro rammet av et omfattende cybersikkerhetsangrep mot sine systemer [H20]. Norsk Hydro er en norsk produsent

[8] Sosial manipulasjon.

av aluminium og fornybar energi. Angrepet ble satt i gang ved at en uvitende ansatt åpnet en infisert e-post som gjorde det mulig for angriperne å spre viruset via IT-systemene til Hydro. Viruset var av typen LockerGaga, et *ransomware* som krypterte filer på personlige datamaskiner og servere. Det ble postet en melding fra angriperne på de kompromitterte maskinene om at systemene var kryptert og for å dekryptere krevde angriperne betaling i kryptovalutaen Bitcoin. Angrepet førte til produksjonsstans på flere anlegg, andre anlegg måtte gå over fra automatisk til manuell operasjon [Bri19]. Hydro har anslått at angrepet kostet mellom 550 og 650 millioner norske kroner (NOK) [H20].

Angrepet på Colonial Pipeline. Colonial Pipeline er USA sitt største rørledningssystem for raffinerte produkter [Kum16]. Systemet kan frakte mer enn tre millioner fat bensin og diesel mellom den amerikanske golfkysten og New York og er dermed sentral når det gjelder forsyningen av disse produktene i det nordøstlige USA. I mai 2021 ble Colonial Pipeline Company utsatt for et *ransomware*-angrep som resulterte i at rørledningssystemet ble stengt ned [NSM21a]. Angriperne kom seg inn i selskapets systemer ved å stjele ett enkelt passord [KR21] som var lekket på *the dark web*[9] [TM21]. Passordet var til en virtuelt privat nettverks (VPN)-løsning som var satt opp for at de ansatte skulle kunne logge seg på selskapets systemer hjemmefra. VPN-løsningen manglet multifaktorautentisering og dermed kom angriperne seg inn i selskapets IT-systemer kun med dette ene passordet [NSM21a].

Inne i systemene krypterte og overførte angriperne store datamengder fra selskapet [NSM21a]. Dette medførte at selskapets drivstoffdistribusjon til store deler av østkysten i USA ble stanset i hele fem dager [NSM21a]. Den 7. mai oppdaget Colonial Pipeline Company et løsepengekrav på 4.4 millioner dollar i kryptovaluta som de valgte å betale [TM21]. Senere bekreftet amerikanske myndigheter at den russiske cyberkriminalitetsgruppen DarkSide sto bak angrepet [NSM21a].

Spyware

Spyware[10] er programvare som installeres av en angriper uten av brukeren vet om det. Formålet er å overvåke brukere og datamaskiner. Programvaren kan spres på ulike måter, enten ved målrettede angrep med virus eller som vedlegg til annen programvare. Et *spyware*-angrep kan innebære at angriperen stjeler data som kredittkortinformasjon, innloggingsinformasjon eller annen sensitiv informasjon, som kan utnyttes til ulovlig aktivitet [TWNS07]. *Spyware* kan også installeres på mobiltelefoner for å avlytte samtaler eller spore brukeres lokasjoner [Gil21]. En annen type *spyware* finnes i legitime applikasjoner og samler inn statistikk om brukernes oppførsel på applikasjonen eller datamaskinen [TWNS07].

[9] Det mørke nettet.
[10] Spionvare eller spionprogramvare.

Stuxnet

Stuxnet regnes som det første målrettede, spesialtilpassede cyberangrepet mot et OT-system, og regnes som et vendepunkt for industrien når det gjelder cyberangrep som fikk fysiske konsekvenser [KL15]. Forskere har beskrevet angrepet som verdens første digitale våpen. Angrepet ble oppdaget for første gang i 2010, da det ble brukt for å angripe systemer fra det iranske atomprogrammet [MB]. Stuxnet er et angrep der en sofistikert angriper peker seg ut et spesifikt, godt beskyttet industriområde. Angriperen utnytter en mindre beskyttet leverandør av industriområdet for å tilegne seg kunnskap om hovedmålet og hvordan det er beskyttet. Dermed kan angriperen utvikle *malware* som er skreddersydd til å utnytte nulldagssårbarheter hos målet og påføre fysisk skade på utstyr. *Malwaren* blir fraktet til stedet gjennom flyttbare medier, og er laget på en slik måte at den ikke blir oppdaget når den sprer seg rundt i systemene. Stuxnet krever en svært sofistikert angriper, som både forstår de fysiske prosessene og kontroll-komponentene og hvordan man utvikler *malware* som kan forflytte seg uten å bli oppdaget. Konsekvensene av Stuxnet kan være stans i produksjon, ødeleggelse av utstyr og skade på personer [Gin20].

2.2.2 Innsideangrep

Et innsideangrep utføres av en ansatt som har, eller har hatt, legitim tilgang til en virksomhets systemer, prosedyrer og informasjon, og som misbruker denne tilgangen. Angriperen utnytter sin posisjon til å handle på en måte som påfører virksomheten tap eller skade [NSM20b]. Et innsideangrep på et OT-system kan gjøres enten på OT- eller IT-siden. Dersom angrepet er på OT-siden kan angriperen eksempelvis stjele passord fra andre teknikere og logge seg på utstyr som kontrollerer fysiske prosesser. Hvis angrepet gjøres på IT-siden, kan for eksempel angriperen stjele innloggingsinformasjon for *remote access* og logge seg på OT-systemet og forsøke å gjøre mest mulig skade ved å trykke seg rundt i systemet. Begge variantene kan resultere i at anlegg stenges helt eller delvis ned [Gin20].

2.2.3 Phishing

I et *phishing*-angrep forsøker angriperen å lure et offer til å utføre en handling [DT20]. Offeret kontaktes vanligvis på e-post [NV19a]. Handlingen kan være å åpne et vedlegg i en e-post, sende penger eller gi fra seg informasjon. *Phishing* kan være et innledende angrep for å få tilgang til systemer for så å fortsette angrepet med for eksempel å spre *ransomware* eller *spyware*. Det er ulike strategier som kan benyttes ved et *phishing*-angrep og jo mer troverdig en *phishing*-e-post er, jo høyere sannsynlighet er det for at angriperen klarer å lure offeret til å utføre den ønskede handlingen. Et *phishing*-angrep kan komme fra både kjente og ukjente avsendere, og en troverdig avsender er en faktor som bidrar i angriper sin favør. Dersom en angriper får kontroll over e-postkontoen til en ansatt, kan hen benytte tilgangen til å sende ut

en *phishing*-e-post som enklere kan lure kollegaer av den ansatte [DT20]. Hvis målet for *phishing*-angrepet er å angripe et OT-system, kan angriperen for eksempel forsøke å få tak i passord for fjerntilganger. Angriperen kan da overvåke OT-systemene, lære seg hvordan de fungerer, og deretter ta kontroll over systemene [Gin20].

2.2.4 Trusselaktører

Det er hensiktsmessig å ha en oversikt over hvilke typer trusselaktører som eksisterer og hvilken motivasjon de ulike typene trusselaktører kan ha for å utføre angrep [NSM20a]. Kunnskap om trusselaktørene gjør at man kan sette inn målrettede tiltak for å hindre hver av de i å lykkes med angrep. Progoulakis mfl. [PNR+21] presenterer fem ulike typer trusselaktører: cyberkriminelle, statlige aktører, innsideaktører, cyberterrorister og cyberaktivister/hacktivister [PNR+21]. Disse er forklart under. Telenor sin rapport "Digital Sikkerhet 2021" trekker frem flere av de samme aktørene, blant annet stater og kontraktører, organiserte kriminelle og hacktivister [TN21].

Cyberkriminelle

Cyberkriminelle er hackere eller organiserte kriminelle med et økonomisk insentiv [PNR+21]. De oppnår økonomisk gevinst gjennom å stjele eller manipulere fysiske verdier eller eiendeler. Informasjonssikkerhetsselskapet mnemonic trekker i sin rapport "2021 Security Report" frem at denne typen trusselaktører spiller på frykt [mAS21]. Fra mars 2020 så mnemonic at cyberkriminelle stadig utnyttet usikkerheten rundt COVID-19-pandemien i sine angrep, for eksempel i *phishing*-e-poster [mAS21].

Statlige aktører

Statlige aktører er fiendtlige stater med mål om politiske fordeler, spionasje, ødeleggelse av digitale eiendeler eller sabotasje [PNR+21]. PST trekker i sin trusselvurdering for 2022 frem statlig etterretningsvirksomhet som en sentral trussel og konstaterer at "trusselen fra statlige nettverksoperasjoner er alvorlig og vil vedvare også i 2022" [PST22a]. De understreker også at statlig etterretningsvirksomhet fra Russland og Kina utgjør den største trusselen [PST21]. I en pressemelding fra 18.mars 2022 uttaler PST at de som følge av krigen i Ukraina vurderer at etterretningstrusselen fra Russland i Norge har økt [PST22b]. NSM tydeliggjør i sin risikovurdering for 2022 at "statlige trusselaktører viser en økende vilje til å utnytte våre sårbarheter" [NSM22]. Aktørene kombinerer flere angrepstyper, deriblant cyberoperasjoner, påvirkningsoperasjoner og oppkjøp og investeringer. I tillegg utnytter og rekrutterer statlige aktører enkeltpersoner for å få tilgang på informasjon [NSM22]. Etterretningstrusselen omfatter både offentlige og private selskap, samt teknologimiljøer og forskingsinstitutter. Eventuell etterretningsaktivitet mot petroleumsindustrien i Norge vil kunne ha langsiktige og store konsekvenser både for nasjonal sikkerhet, økonomi og militære [PST20].

Innsideaktører

Innsideaktører kan være uforsiktige ansatte som forårsaker uønskede hendelser eller misfornøyde ansatte som stjeler digital informasjon, ødelegger digitale eiendeler eller saboterer med hensikt om personlig vinning [PNR+21]. mnemonic tekker frem innsideaktører som en trussel i sin rapport "2021 Security Report" [mAS21] og legger vekt på at en innsideaktør kan være både utilsiktet og tilsiktet. En utilsiktet innsider forårsaker skade på en bedrifts eiendeler uten ondsinnet hensikt, mens en tilsiktet innsider utnytter en bedrifts tillitt og skader bevisst dens eiendeler [mAS21].

Cyberaktivister/hacktivister

Cyberaktiviser, også kalt hacktivister, er grupper som har politiske eller ideologiske formål. Disse forårsaker sabotasje av digital infrastruktur gjennom målrettede angrep [PNR+21]. Hacktivister ønsker anerkjennelse og synlighet og aktiviteten de utfører har derfor oftest konsekvenser som forstyrrer slik at det blir lagt merke til [NSM15]. Eksempler på angrep som typisk utføres av denne gruppen trusselaktører er Denial of Service (DoS)[11]-angrep, lekkasje av sensitiv informasjon og endring av nettsider [NSM15].

Cyberterrorister

Cyberterrorister er terrorgrupper med mål om å sabotere eller ødelegge fysiske eiendeler som følge av politiske eller ideologiske årsaker [PNR+21]. Cyberterrorister kan omtales som ekstreme aktivister med en høyere villighet til å forårsake skade og ødeleggelse [NSM15]. Terrorister bruker ofte internett til propaganda, planlegging og innhenting av informasjon. British Journal of Political Science [SGBC22] publiserte i 2021 en artikkel som konstaterer at cyberterror forårsaker andre reaksjoner enn tradisjonelle former for terror, noe som bekrefter at det er behov for nye og tilpassede politiske modeller for digital terror.

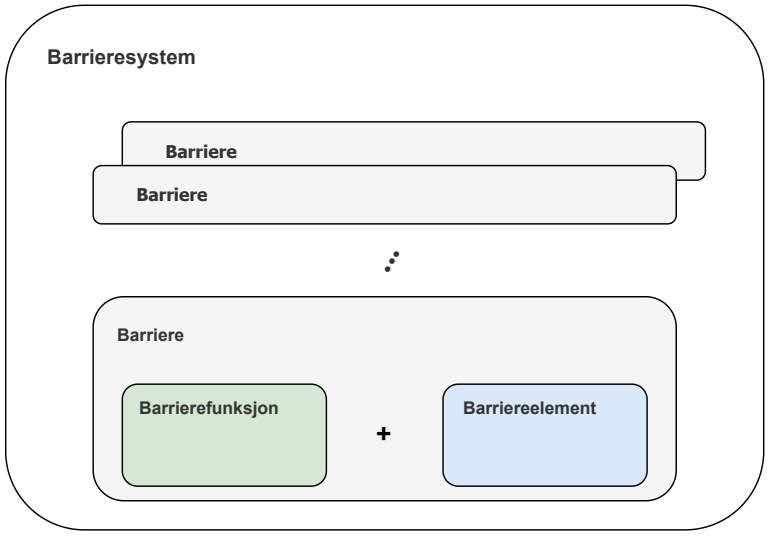
[11] Tjenestenektangrep.

2.3 Barrierer

En barriere er et tiltak som skal forhindre eller minske konsekvensene av uønskede hendelser [PSA17; ØWFR14; HØST15]. Hver barriere består av en barrierefunksjon og et eller flere barriereelementer. Barrierefunksjonen er oppgaven barrieren skal utføre, og barriereelementet er tiltak eller løsninger som bidrar til å realisere barrierefunksjonen [PSA17]. Begrepene utdypes i kapittel 2.3.1 og 2.3.2. Et eksempel på en barriere kan være en branndør der barrierefunksjonen er å hindre brann fra å spre seg og barriereelementet er selve døren.

I følge "Forskrift om styring og opplysningsplikt i petroleumsvirksomheten" (styringsforskriften) §5 [SF5] skal det "etableres barrierer som til enhver tid kan a) identifisere tilstander som kan føre til feil, fare- og ulykkessituasjoner, b) redusere muligheten for at feil, fare- og ulykkessituasjoner oppstår og utvikler seg, c) begrense mulige skader og ulemper" [SF5]. I praksis er det nødvendig å koordinere flere barrierer slik at man totalt får ønsket grad av beskyttelse. En samling av flere barrierer kalles et barrieresystem [PSA17] og er illustrert i figur 2.3.

Styringsforskriften §5 [SF5] sier også at dersom man trenger flere barrierer "skal det være tilstrekkelig uavhengighet mellom barrierene" [KO20]. Dette er for at enkelthendelser som kan (og vil) oppstå ikke skal få for store konsekvenser. I tillegg bidrar dette til at en trussel må passere flere lag med barrierer for at en katastrofal hendelse skal oppstå [HØ16].



Figur 2.3: Et barrieresystem består av en eller flere barrierer. Hver barriere har en barrierefunksjon og et barriereelement. Figuren er adaptert fra [KV21].

2.3.1 Barrierefunksjon

Barrierefunksjonen er oppgaven barrieren skal løse eller det den skal gjøre [HØ16]. Et eksempel på en barrierefunksjon kan være å forhindre gasslekkasjer. En barrierefunksjon kan deles videre inn i sub- og sub-sub-funksjoner.

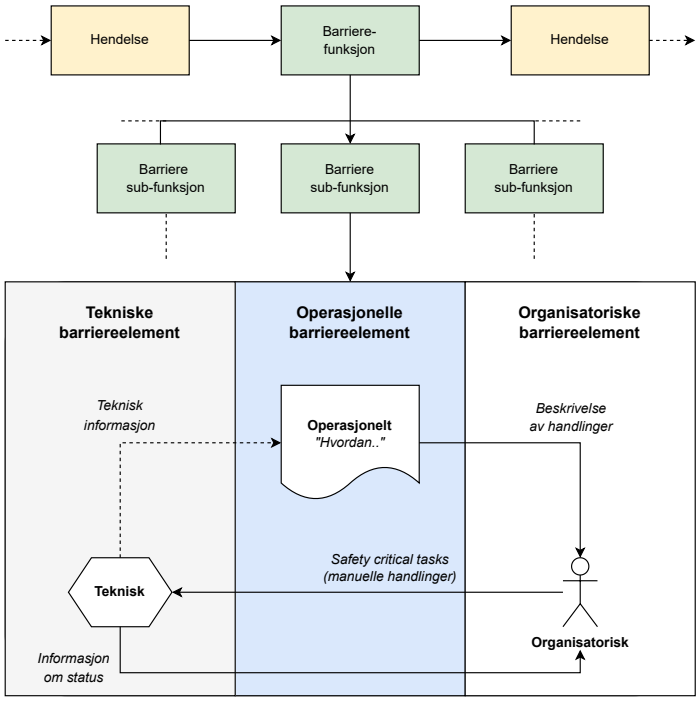
2.3.2 Barriereelement

Barriereelementet er et teknisk, operasjonelt eller organisatorisk tiltak eller løsning som bidrar til å realisere en barrierefunksjon [PSA17]:

1. **Tekniske barriereelement:** Utstyr og systemer som bidrar til å realisere en barrierefunksjon. Et eksempel på et teknisk barriereelement kan være en sensor som måler trykk.
2. **Operasjonelle barriereelement:** Handlinger og aktiviteter som personale må utføre for å bidra til å realisere en barrierefunksjon. Eksempler på operasjonelle barriereelementer er å oppdage feil og sette igang tiltak.
3. **Organisatoriske barriereelement:** Personale med definerte roller og spesifikk kompetanse som bidrar til å realisere en barrierefunksjon. Et eksempel på organisatorisk barriereelement er en ansatt som oppdager feil og setter igang tiltak.

For å realisere en barrierefunksjon kreves som regel et samspill mellom tekniske, operasjonelle og organisatoriske barriereelementer [HØ16]. Samspillet er illustrert i figur 2.4. De organisatoriske barriereelementene er de ansatte som er direkte involvert i realiseringen av en barrierefunksjon, mens de operasjonelle barriereelementene er prosedyrer og handlinger som kreves for denne realiseringen. I denne oppgaven brukes fellesbetegnelsen ikke-tekniske barriereelementer for å omtale organisatoriske og operasjonelle barriereelementer samlet. Figur 2.4 markerer også *Safety Critical Tasks (SCTs)*[12] som er manuelle handlinger som benytter de operasjonelle barriereelementene for å realisere barrierefunksjonen. Basert på Ptil sin definisjon av barriereelementer, tilsvarer en SCT det operasjonelle barriereelementet [PSA17; HØ16].

[12] Sikkerhetskritiske oppgaver.



Figur 2.4: Samspill mellom barrierefunksjon og barriereelementer. Figuren er adaptert fra [HØ16].

De organisatoriske barriereelementene til en barrierefunksjon er rollene som er direkte involvert i realiseringen av barrieren [HØ16]. Altså er dette personalet som er ansvarlig for å utføre oppgaver relatert til hver enkelt barrierefunksjon. For organisatoriske barriereelementer kan det være nyttig å skille mellom normal drift og nødssituasjoner når man skal identifisere rollene til personalet. Det kan være én person som har ansvar for å fullføre en gitt oppgave under normale forhold, og en annen som har ansvaret i en nødssituasjon. Typisk er det få roller som er ansvarlig for flere oppgaver. Eksempler på roller som gjerne er involvert i realisering av mange oppgaver er kontrollromsoperatører, operasjonelt personale som driver med vedlikehold eller inspeksjon, og teknikere [HØ16].

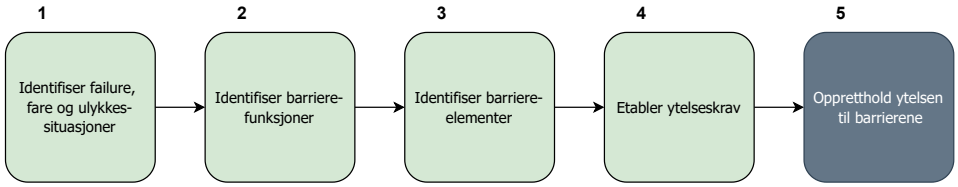
Operasjonelle barriereelementer er handlinger og aktiviteter som er en del av utførelsen av en barrierefunksjon [HØ16]. Operasjonelle barrierer kan defineres som de tiltakene der det ikke er beskrevet nøyaktig hvordan man skal ta beslutninger eller handle i en gitt situasjon [McL17]. Ansvaret ligger på individer med den nødvendige kompetansen til å handle riktig og i tråd med kultur, retningslinjer, og begrensninger satt av organisasjonen. McLeod [McL17] mener dermed at operasjonelle barrierene avhenger dermed av beslutnings- og problemløsningsevnen til enkeltpersoner.

2.3.3 Ytelsespåvirkende faktorer og ytelseskrav

En ytelsespåvirkende faktor (YPF)[13] er en faktor som er avgjørende for at en barriere skal fungere som tiltenkt [HØ16]. Eksempler på YPF-er kan være øvelse og trening, kompetanse, tilgjengelighet, arbeidsmengde eller kultur. Etter Styringsforskriften §5 skal det utvikles ytelseskrav for alle barriereelementer [SF5]. Ytelseskravene skal reflektere risikobildet til hver enkelt fasilitet. Kravene kan for eksempel være knyttet til responstid og bemanning. For ikke-tekniske barrierer kan man ha både direkte og indirekte ytelseskrav. Direkte krav vil være direkte knyttet til barriereelementet, mens et indirekte krav vil være krav knyttet til YPF-er [HØ16].

2.4 Barrierestyring

Barrierestyring er koordinerte aktiviteter for å etablere og vedlikeholde barrierer slik at de kan oppfylle sine funksjoner til enhver tid [PSA17]. Barrierestyringsprosessen er illustrert i figur 2.5. Det er ulike måter å praktisere barrierestyring på, men én løsning kan være inkludere den som en del av risikostyringsprosessen [HØ16]. Her må man først identifisere mulige fare-og ulykkessituasjoner. Basert på situasjonene som er identifisert, må det avgjøres hvilke barrierefunksjoner og -elementer som er nødvendige. For hver barriere må det bestemmes hvilke ytelseskrav som kreves, og hvilke faktorer som påvirker ytelsen til barrieren [PSA17].



Figur 2.5: Hovedpunktene i barrierestyringsprosessen for å etablere og vedlikeholde barrierer. Figuren er adaptert fra [PSA17].

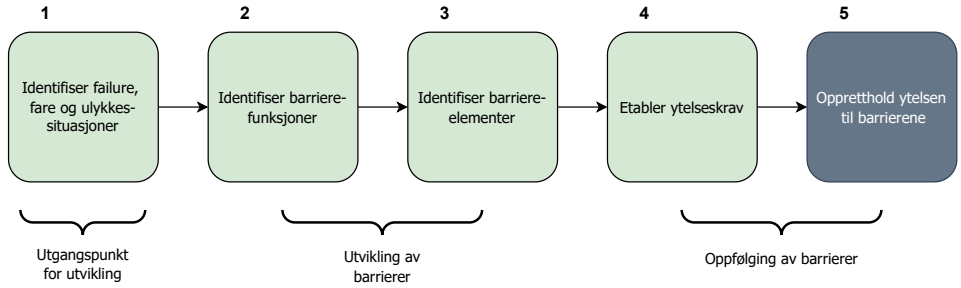
I barrierestyringsprosessen kan det skilles mellom designfasen, der barrieren blir etablert, og operasjonsfasen, der barrieren blir fulgt opp og vedlikeholdt. I designfasen ligger fokuset på å identifisere og utforme barrierer som bidrar til tilstrekkelig reduksjon av risiko under drift. For å bestemme hvilke barrierer som er nødvendige krever det at man har evaluert og vurdert risikoen knyttet til systemet, og valgt et godtatt risikonivå [PSA17]. Det er gunstig å jobbe strukturert med utviklingen av barrierer slik at man i størst mulig grad får dekket behovet som kreves for møte et visst risikonivå. I operasjonsfasen ligger fokuset på oppfølging og vedlikehold for å sørge for at barrierene er tilgjengelige til enhver tid. Dersom en barriere er svekket,

[13] Engelsk: Performance influencing factor (PIF).

må det implementeres hjelpetiltak [HØ16]. Fokuset i denne oppgaven vil ligge på designfasen, altså på å utvikle barrierene.

2.4.1 Utvikling av barrierer

Utviklingen av barrierer er en del av barrierestyringsprosessen og består av steg 2 og 3 i figur 2.5 [HØ16]. I forkant av barriereutviklingen må man identifisere fare- og ulykkessituasjoner (steg 1 i figur 2.5). Fare- og ulykkessituasjoner er en sentral del av risikobildet til et system, og er et naturlig utgangspunkt for utviklingen av barrierer, da hensikten med barrierene er å begrense konsekvensene av disse situasjonene. Figur 2.6 er en utvidelse av figur 2.5 der det er markert hva vi mener er utgangspunktet for utviklingen av barrierer (steg 1), hva som er selve utviklingen av barrierene (steg 2 og 3) og hva som er knyttet til å følge opp barrierene (steg 4 og 5). Oppgaven fokuserer på utvikling av barrierer, så steg 2 og 3 i prosessen er utdypet under.



Figur 2.6: Hovedpunktene i prosessen med å utvikle og vedlikeholde barrierer inneholder definerte faser. Figuren er adaptert fra [PSA17].

Steg 2: Identifisere barrierefunksjoner

For å identifisere barrierefunksjoner tar man utgangspunkt i fare- og ulykkessituasjonene fra steg 1. Målet er å identifisere de funksjonene som må være på plass for å forhindre eller minske omfanget av fare- og ulykkessituasjonene. Hver barrierefunksjon kan brytes ned til sub-funksjoner som igjen kan brytes videre ned til sub-sub-funksjoner [HØ16]. Ved å bryte ned barrierefunksjonene gjør man det tydelig hva som kreves for å realisere en funksjon.

Steg 3: Identifisere barriereelementer

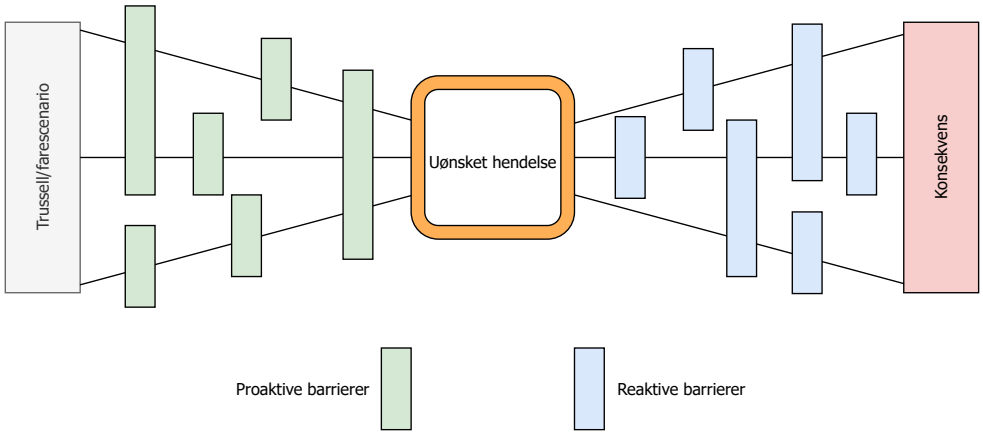
Etter at de nødvendige barrierefunksjonene er identifisert og brutt ned i sub-funksjoner og eventuelt sub-sub-funksjoner, er neste steg å realisere disse ved å identifisere barriereelementer. Her er målet å finne riktig kombinasjon av tekniske, operasjonelle

og organisatoriske barriereelementer for å realisere barrierefunksjonene [HØ16]. Dette er illustrert i figur 2.4.

2.4.2 Bow-tie

Å plassere barrierer i et bow-tie-diagram er nyttig i barrierestyringen [AM15]. Et bow-tie-diagram er formet som en sløyfe (engelsk: bow-tie), der "knuten" i midten av figuren typisk representerer et ulykkesscenario eller en uønsket hendelse [BFM+18]. Helt til venstre i bow-tien plasseres truslene som kan forårsake den uønskede hendelsen, helt til høyre plasseres konsekvensene av hendelsen.

En bow-tie er en visualisering av hvordan barrierer kan settes inn i et system. En barriere vil være enten proaktiv eller reaktiv avhengig av om den settes inn før eller etter den uønskede hendelsen inntreffer [Rau14]. En proaktiv barriere skal hindre at en hendelse skjer, mens en reaktiv barriere skal redusere konsekvensene dersom hendelsen har skjedd [DNV16]. Barrierer kan være proaktive eller reaktive uavhengig av om barriereelementet er teknisk, operasjonelt eller organisatorisk [Liu20]. Figur 2.7 viser et eksempel på et bow-tie-diagram. De grønne og blå boksene markerer barrierer, proaktive i grønt til venstre, reaktive i blått til høyre.



Figur 2.7: Bow-tie-diagram med proaktive barrierer til i grønt til venstre, reaktive barrierer i blått til høyre. Figuren er adaptert fra [Rau14].

2.5 Barrierer og bow-ties for cybersikkerhet

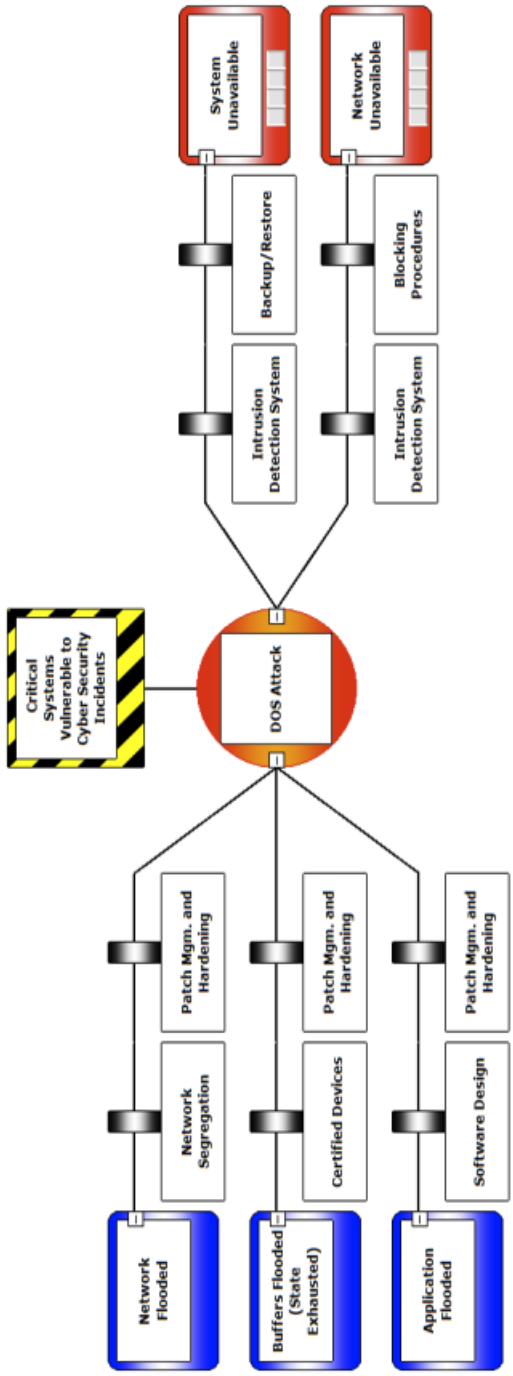
Barrierebegrepet har sitt opphav fra *safety*-domenet [GPMH], der både barrierestyring og bow-tie-diagrammer er etablerte metoder for å redusere sannsynlighet for, og konsekvensene av, farer. Liu [Liu20] foreslår at metoder som anvendes for *safety*-barrierer, kan brukes som en mulig løsning for å bedre cybersikkerheten. I tillegg presiseres viktigheten av at personer fra *safety*-domenet utnytter sin kunnskap også for å beskytte systemer fra cybersikkerhetsangrep. Barrierer for cybersikkerhet blir presentert som et forslag til videre forskning, og blir derfor ikke spesifisert ytterligere i artikkelen [Liu20].

Grøtan mfl. [GPMH] peker på at det å anvende barrieremodellen også for cybersikkerhet vil være hensiktsmessig på flere måter, men at det også har sine begrensninger. En av begrensningene som trekkes frem er evnen til å håndtere skjulte eller fremvoksende sårbarheter som ligger utenfor det man kan være forberedt på. For å håndtere slike uventede hendelser understrekes det at mennesker vil spille en sentral rolle [GPMH].

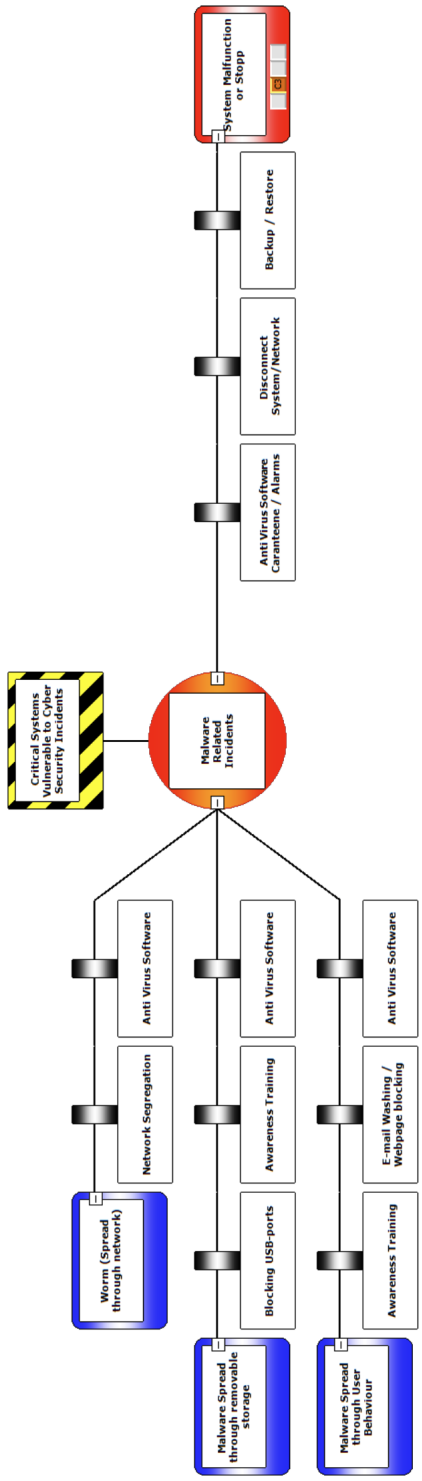
I "Visualizing Cyber Security Risks with Bow-Tie Diagrams" [BFM+18] observerer Bernsmed mfl. at bow-ties er nyttige for å få en oversikt over årsaker til og konsekvenser av en uønsket hendelse, men at de er dårligere på å fange utførelsen av et angrep i detalj. Det nevnes også at siden én trussel kan føre til ulike uønskede hendelser, kan det fort bli mye repetisjon og overflødighet dersom man har en samling med bow-ties som tar for seg ulike trusler [BFM+18].

Flere rapporter fra DNV[14] [KO20; DNV16] presenterer bow-ties med barrierer for cybersikkerhet. Felles for rapportene er at barrierene som presenteres er relativt overordnede og lite konkrete. Det er heller ikke eksplisitt vist hva som er barrierefunksjon, og hva som er barriereelement. Rapporten "Cyber security SIS og egensikre komponenter, kommunikasjonsprotokoller" [KO20] omhandler oljebransjen, og trekker frem at barrierer også kan beskrive cybersikkerhetstiltak. I rapporten presenteres det kun ett eksempel på en bow-tie for et DoS-angrep (se figur 2.8). DNV sin "Cyber security resilience management for ships and mobile offshore units in operation" [DNV16] tar for seg styring av cybersikkerhetsbarrierer for skip og andre bevegelige enheter offshore. Selv om praksisen ikke gjelder petroleumsindustrien direkte, kan man tenke seg at de samme prinsippene i stor grad er overførbare til for eksempel offshore oljeplattformer. I rapporten presenteres bow-ties for flere typer angrep, et eksempel er vist i figur 2.9. Det presiseres at noen tiltak for cybersikkerhet, slik som *security awareness training*[15] vanligvis ikke regnes som barrierer. Tiltakene er likevel behandlet som barrierer i figur 2.9 for eksempelets skyld [DNV16].

[14] Tidligere DNV GL.
[15] Bevissthetstrening for cybersikkerhet.



Figur 2.8: Eksempel på barrierer for et DoS-angrep. Figuren er hentet fra [KO20].



Figur 2.9: Eksempel på barrierer for et malware-angrep. Figuren er hentet fra [DNV16].

2.6 Menneskelig ytelse

Mennesker er fleksible, tilpasningsdyktige og gode på å vurdere uventede situasjoner, men også følelsesstyrte og tilbøyelige til å gjøre feil [PSA17; McL17]. Innenfor cybersikkerhet blir mennesker ofte omtalt som det svakeste leddet, blant annet på grunn av mulighetene for at mennesker kan bli lurt og gjøre ting ved uhell [TN; TL21]. Mennesker har også ulike nivåer av årvåkenhet og menneskers fysiske og psykiske prestasjon blir påvirket av mange ulike faktorer. McLeod [McL17] trekker frem fire harde sannheter om menneskelig ytelse. Det kan være vanskelige å designe for håndtering av sannhetene, men det er viktig at de tas hensyn til fordi de påvirker hvordan mennesker reagerer og håndterer situasjoner. De fire sannhetene McLeod [McL17] presenterer er:

1. **Opplevelse av situasjonen:** Menneskets ytelse avhenger sterkt av hvordan mennesket som er involvert opplever situasjonen. Følelser, tanker og holdninger er faktorer som blir påvirket av situasjonen og som er med å avgjøre menneskets ytelse.
2. **Samhandling med teknologi:** Hvordan grensesnittet til systemer og utstyr er utformet påvirker hvordan mennesker samhandler med teknologien.
3. **Enkleste utvei:** Mennesker velger gjerne den enkleste måten å gjøre ting på, til tross for at det kan være mer risikabelt.
4. **Irrasjonalitet:** Man kan ikke regne med at mennesker tar rasjonelle valg.

For å håndtere disse svakhetene, er det viktig med kompetansebygging, bevisstgjøring og opplæring i rutiner og bruk av systemer [NSM19a; DT18]. Gode prosedyrer og evnen til å følge disse blir trukket frem som viktig for å at mennesker skal kunne håndtere uønskede hendelser. Undersøkelser viser nemlig ofte at uønskede hendelser ikke ville skjedd dersom ansatte hadde fulgt satte prosedyrer [McL17]. Dette forutsetter samtidig at organisasjonen må ha på plass alle nødvendige prosedyrer og at disse er konkrete, tydelige og oppdaterte. I tillegg må prosedyrene være tilgjengelige når de trengs, og de ansatte må ha kompetanse til å kjenne igjen situasjoner og avgjøre hvilke prosedyrer de skal anvende i de ulike situasjonene. Prosedyrene og kompetansen er ikke alltid tilstrekkelige, noe som kan gjøre det vanskelig for et menneske å faktisk følge prosedyrene selv om de eksisterer [McL17].

Som vi vil se mer om i kapittel 2.7, er en standard en felles oppskrift på hvordan noe skal lages eller gjennomføres [STA]. Standarder har dermed som mål å legge et grunnlag som er felles for de fleste organisasjoner, slik at så mange som mulig kan anvende standarden. Hver organisasjon må så selv tilpasse tiltakene til sin drift.

Grøtan mfl. [GPMH] mener at standarder, som for eksempel IEC 62443, av natur har et mindre uttalt fokus på menneskelige faktorer. Menneskelige faktorer er ikke nedvurdert med overlegg, men menneskelig praksis relatert til implementasjonen av standarden er i mindre grad spesifisert [GPMH]. I samme artikkel understrekes også viktigheten av de menneskelige tiltakene sammen med standardene for å få en mer dynamisk og helhetlig beskyttelse. Ettersom trusselbildet alltid er i forandring, må man kontinuerlig være på vakt for uforutsette hendelser og nye angrepsmetoder [GPMH].

Selv om mennesker blir omtalt som det svakeste ledd, er det også viktig å bemerke at mennesker har evnen til å gripe inn og forstå situasjoner på en måte tekniske systemer ikke kan. Systemer blir ofte definert med antagelse om at de er autonome systemer som kontrolleres av en rekke tekniske komponenter. Ved å gjøre dette risikerer man å overse hvor viktig menneskets rolle er for å sikre både *safety* og *security* [CWKL20]. I tillegg trekker McLeod [McL17] frem at flere hendelser har blitt avverget nettopp fordi kompetente mennesker er i stand til å analysere en situasjon og avvike fra satte prosedyrer.

2.7 Standarder for cybersikkerhet i OT-systemer

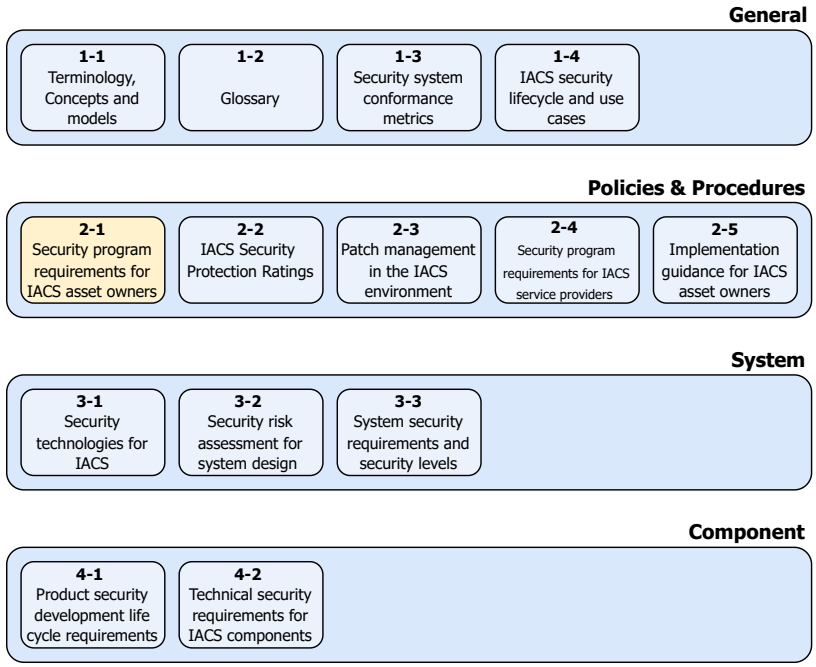
En standard er en felles oppskrift på hvordan noe skal lages eller gjennomføres, og har som hensikt å gjøre det enklere og tryggere å både bygge og drifte et samfunn [STA]. Mange standarder ser på *security* og *safety* som separate felter, og tar for seg enten den ene eller den andre. *Security*-standardene har fokusert på krav knyttet til konfidensialitet, integritet og tilgjengelighet. Hensikten med *security*-standardene har i stor grad vært å håndtere målrettede trusler og sårbarheter i systemene, for å kunne nå de sikkerhetsmålene man har satt seg. *Safety*-standardene fokuserer på sin side på utilsiktede farer og miljøfarer som kan føre til fysisk skade på mennesker, eiendeler eller natur. Det å ha separate standarder for *safety* og *security* fører med seg ulike utfordringer, siden *security*-trusler i økende grad kan utrette fysiske skader. Dette har åpnet for å diskutere behovet for standarder som kombinerer *security* og *safety* [CKKL19].

En standard som tar for seg begge perspektiver er IEC 62443, som omhandler cybersikkerhet i OT-systemer [Dav18]. Standarden omfatter cybersikkerhetstiltak som er nødvendig for å sikre pålitelig og sikker drift av et automatisert driftsanlegg. Ettersom cybersikkerhet er avhengig av de tre faktorene teknologi, prosess og mennesker tar standarden for seg tiltak innen alle disse områdene [Kob22]. Det er altså viktig å håndtere både de tekniske- og de ikke-tekniske tiltakene som IEC 62443 presenterer. For å sikre dette fokuseres det på å definere hvilke roller som er involvert i hva, og hvem som utfører hvilke oppgaver [DNV17]. Standarden praktiserer *defense-in-depth*[16]-konseptet for å realisere et samspill mellom de tekniske- og ikke-tekniske

[16] Forsvar i dybden.

tiltakene. *Defense-in-depth* går ut på at man implementerer komplementære cybersikkerhetstiltak som hver for seg gir et lag med forsvar. Sammen utgjør tiltakene flere lag med forsvar som en angriper må komme seg gjennom får å nå et angrepsmål [IEC10].

IEC 62443 består av de fire hoveddelene *General, Policies & Procedures, System og Component*[17]. Hoveddelene er delt videre inn i underkapitler som vist i figur 2.10. Oppgaven er avgrenset til å se på kravene i IEC 62443-2-1, fordi vi anså kravene som omhandler retningslinjer og prosedyrer for eierne av systemene som de mest aktuelle. Den nyeste offisielle versjonen av denne delen av standarden, IEC 62443-2-1:2010 [IEC10], er fra 2010. For å bruke et mer oppdatert sett med krav har vi hentet ut kravene fra en presentasjon av en nyere versjon av standarden, "Cybersecurity needs a holistic approach: Deep dive in ISA/IEC 62443-2-1" [Kob22]. Videre i oppgaven refereres denne versjonen av standarden til som ISA/IEC 62443-2-1.



Figur 2.10: Oversikt over de ulike delene i ISA/IEC 62443. Figuren er adaptert fra [ISA21].

Selv om IEC 62443 er en viktig standard for å sikre god beskyttelse mot cyberangrep i OT-systemer, kan den være vanskelig å anvende i praksis. Et problem er at den anses som uferdig og vanskelig å ta i bruk. Det er en ressurskrevende jobb å skulle

[17] Generelt, retningslinjer og prosedyrer, system og komponent.

drive en virksomhet i henhold til standarden, noe som kunne vært annerledes dersom standarden var enklere å anvende. Det er dermed det et behov for å forstå prinsippene i standarden for videre å kunne ta den ut i praksis [HOJ+21].

2.8 MITRE

MITRE er en amerikansk ideell organisasjon som jobber for offentlighet, industri og akademia for å skape et tryggere samfunn [MTa]. Et av feltene MITRE har ekspertise på er cybersikkerhet, og for å bidra til bedre cybersikkerhet har MITRE utviklet ATT&CK-rammeverket.

ATT&CK er en kunnskapsbase som tar for seg en cyberangripers atferd og taksonomi under et angrep. Kunnskapsbasen er delt inn i de tre delene "ATT&CK for Enterprise", "ATT&CK for Mobile" og "ATT&CK for ICS". "ATT&CK for Enterprise" tar for seg angriperens atferd ved angrep mot IT-nettverket og skytjenestene til en bedrift, som til slutt ender med at angriper tar kontroll over systemene [MTc]. Det er denne delen som brukes i oppgaven, da oppgaven skal se på angrep som starter i IT-nettverket. Hensikten med ATT&CK er å beskrive vanlige taktikker, teknikker og prosedyrer angripere bruker, slik at man har bedre forutsetninger for å kunne forsvare seg [MTc]. Taktikkene er målet til angriperen i hvert steg av angrepet. Hver taktikk innebærer et sett med teknikker som beskriver hvordan angriperen oppfyller målet i hvert steg. MITRE beskriver også ulike mottiltak for å forvare seg mot teknikkene til angriperne. Fordelen med MITRE er at det tydeliggjør hvordan en angriper oppfører seg. Denne informasjonen kan man bruke til å planlegge hvordan man best kan forsvare seg mot ulike angrep. Rammeverket mangler en beskrivelse av hvordan man skal sette mottiltakene inn i et system for å kunne velge og prioritere hva som skal implementeres.

Det er beskrevet totalt 14 taktikker i "ATT&CK for Enterprise". Taktikkene er presentert i tabell 2.2.

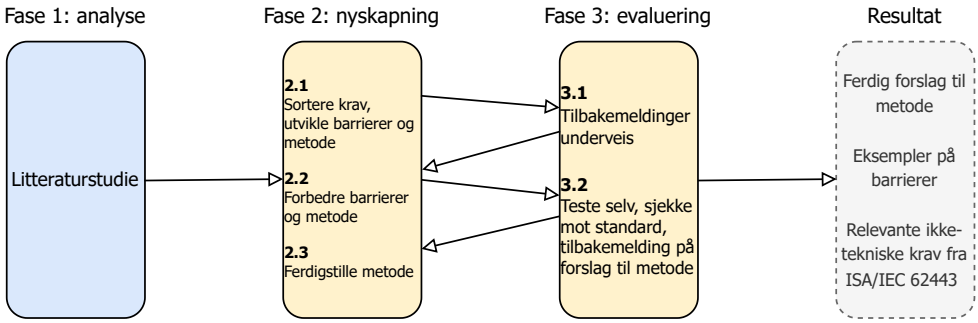
Nummer	Taktikk/steg	Forklaring
1	Undersøkelse (Reconnaissance)	Angriper prøver å samle informasjon hen kan bruke for å planlegge fremtidige angrepsoperasjoner.
2	Ressursutvikling (Resource Development)	Angriper prøver å etablere ressurser hen kan bruke til å støtte angrepsoperasjoner.
3	Innledende tilgang (Initial Access)	Angriper prøver å komme seg inn i nettverket.
4	Utførelse (Execution)	Angriper prøver å kjøre ondsinnet kode.
5	Utholdenhet (Persistence)	Angriper prøver å opprettholde fotfeste i systemet.
6	Eskalering av privilegier (Privilege Escalation)	Angriper prøver å tilegne seg høyere nivå av tilganger.
7	Unngå oppdagelse (Defense Evasion)	Angriper prøver å unngå å bli oppdaget.
8	Tilgang til innloggingsinformasjon (Credential Access)	Angriper prøver å stjele innloggingsinformasjon.
9	Oppdagelse (Discovery)	Angriper prøver å kartlegge systemet.
10	Lateral bevegelse (Lateral Movement)	Angriper prøver å bevege seg gjennom systemet.
11	Innsamling (Collection)	Angriper prøver å samle inn relevant data om målet sitt.
12	Kommando og kontroll (Command and control)	Angriper prøver å kommunisere med kompromitterte systemer for å kontrollere de.
13	Eksfiltrering (Exfiltration)	Angriper prøver å stjele data.
14	Påvirkning (Impact)	Angriperen prøver å manipulere, påvirke eller ødelegge systemer og data.

Tabell 2.2: Stegene i MITRE ATT&CK for Enterprise [MTb].

Kapittel 3
Forskningsmetode

Hensikten med denne oppgaven var å undersøke om barrierekonseptet også kan anvendes innen cybersikkerhet. Vi ville derfor utvikle en metode for å finne cybersikkerhetsbarrierer, samt presentere eksempler på barrierer vår metode kan produsere. Siden oppgaven vil bringe ny kunnskap til verden ved hjelp av et nytt artefakt, barriereutviklingsmetoden, er *teknologivitenskap* valgt som undersøkelsesdesign. Med teknologivitenskap utvikler man ny kunnskap gjennom nye eller forbedrede artefakter [Stø19, s. 1].

Teknologivitenskap kjennetegnes ved at den er delt inn i tre faser: en analysefase, en nyskapningsfase og en evalueringsfase. Hver fase gjennomføres flere ganger. Fasene vi brukte er illustrert i figur 3.1. I denne oppgaven besto analysefasen av en litteraturstudie for å kartlegge behovet for metoden vår, i tillegg til å samle nødvendig bakgrunnsinformasjon for å kunne begynne utviklingen. I fase 2.1 fant vi relevante ikke-tekniske krav fra ISA/IEC 62443-2-1 og utviklet barrierer og metode, før artefaktet i fase 3.1 ble evaluert gjennom samtaler og diskusjoner med industrien. Samtalene fullførte første iterasjon av prosessen. I fase 2.2 ble tilbakemeldingene fra bransjen brukt til å utvikle metoden videre. Til slutt, i fase 3.2, ble metoden evaluert ved å teste den på nye tilfeller, å undersøke hvilke krav fra ISA/IEC 62443-2-1 metoden bidro til å oppfylle og å få en ny runde med tilbakemeldinger. Som en del av fase 3.2 ble altså de relevante ikke-tekniske kravene fra fase 2.1 brukt til å sjekke om de identifiserte barrierene bidro til å dekke kravene. En sjekk på om de identifiserte barrierene faktisk bidrar til å oppfylle kravene kan fungere som en evaluering på om metoden finner barrierer som tiltenkt. Resultatet fra fase 3 ble brukt for å vurdere og diskutere det endelige resultatet.



Figur 3.1: De tre fasene i teknologivitenskapsprosessen. Figuren er adaptert fra [Stø19, s. 20].

En viktig del av vår teknologivitenskapsprosess, var å gjennomføre grundige samtaler med et lite utvalg ressurspersoner fra industrien. Vi ønsket å samle data i form av meninger, og det var dermed naturlig å bruke et kvalitativt undersøkelsesopplegg som en del av prosessen. I en kvalitativ undersøkelse prøver man å forstå hvordan individer eller grupper oppfatter og tolker et fenomen [Jac15, s. 133]. Da undersøkes ofte få enheter, og data samles inn som meninger formidlet gjennom språk og handlinger [Jac15, s. 125]. En kvalitativ undersøkelse kan betegnes som åpen, fordi forskeren legger så få føringer som mulig på hvilken data som skal samles inn før undersøkelsen begynner. Først etterpå blir dataene sortert, strukturert, og sett i sammenheng med hverandre [Jac15, s. 127].

3.1 Analyse av artefaktbehov

For å få et inntrykk av hva som fantes av tidligere forskning, artikler og rapporter knyttet til cyberbarrierer og hvilke utfordringer petroleumsindustrien står overfor når det gjelder cybersikkerhet, gjennomførte vi en litteraturstudie. Vi ville også bruke studien til å bekrefte behovet for forskning knyttet til barrierestyring for cybersikkerhet. Hovedfokuset i oppgaven var å utvikle metoden for å identifisere cybersikkerhetsbarrierer, og der var samtaler med industrien den mest sentrale informasjonskilden. Vi prioriterte grundige intervjuer fremfor en grundig litteraturstudie og studien ble derfor gjennomført og presentert på en overordnet måte.

Litteraturstudien tok utgangspunkt i fire hovedtema: sammenkobling av IT og OT, trusler for OT-systemer i petroleumsindustrien, ulike angrepsscenarioer og barrierer. For å undersøke temaene søkte vi i databasene Google Scholar og NTNU Oria, i tillegg til å motta litteratur fra veiledere. For temaene sammenkobling av IT og OT, trusler for OT-systemer i petroleumsindustrien og angrepsscenarioer ønsket vi

hovedsakelig å få en oversikt over temaene for å opparbeide oss et faktagrunnlag. Søket på barrierer ble gjennomført grundigere, da vi ville undersøke hva som fantes av forskning på barrierer for cybersikkerhet og ikke-tekniske barrierer. Søkene på hvert av temaene er utdypet under, innholdet i funnene fra litteraturstudien er presentert i kapittel 2 - Bakgrunn, og en oppsummering av funnene om barrierer er presentert i kapittel 4 - Resultat.

Sammenkobling av IT og OT

For å studere skillet mellom IT- og OT-systemer, og hvilke konsekvenser sammenkoblingen har for systemer i petroleumsindustrien, tok vi utgangspunkt i rapporten "Grunnprinsipper for IKT-sikkerhet i industrielle IKT-systemer" [JWBK21] som vi ble tildelt av veiledere. Videre fant vi forskning på utfordringer rundt sammenkoblingen ved å utføre søk i databasene Google Scholar og NTNU Oria med ulike kombinasjoner av søkeordene *"IT"*, *"OT"*, *"safety"*, *"security"*, *"cyber"* og *"petroleum"*. Vi har også mottatt flere artikler og rapporter fra veiledere om temaet, brukt kildelistene til artikler og rapporter, i tillegg til å supplere med informasjon som har dukket opp gjennom undersøkelse av andre temaer.

Trusler for OT-systemer i petroleumsindustrien

Det ble undersøkt rapporter fra anerkjente aktører som jobber med å kartlegge og holde seg oppdatert på trusselbildet for å få en oversikt over truslene petroleumsindustrien står overfor. For at barrierene vi identifiserte skulle være mest mulig aktuelle for et trusselbilde som er i stadig endring, så vi stor verdi i å bruke så oppdatert informasjon som mulig.

Waterfall Security Solutions er, i følge de selv, en global leder innen teknologi for industriell cybersikkerhet [Gin20]. Målet til selskapet er å hjelpe til med å beskytte fysiske ressurser og industrielle prosesser fra cyberangrep [WF]. De bidrar til dette blant annet med rapporten "The Top 20 Cyber Attacks On Industrial Control Systems" [Gin20]. *Dragos* er et sikkerhetsselskap som jobber med å beskytte OT-systemer mot angrep, gjennom utvikling av verktøy og kunnskapsdeling [Dra]. I rapportene "Global Oil and Gas Cyber Threat Perspective" [Dra19] og "Oil & Natural Gas Cyber Threat Perspective" [Dra22] vurderer de truslene, risikoene og trusselaktørene som er aktuelle for olje- og gassindustrien. De tre nevnte rapportene er utgangspunktet for vurderingen av trusselbildet i denne oppgaven. I tillegg ble det brukt rapporter fra anerkjente, norske aktører, slik som Telenor, Nasjonal Sikkerhetsmyndighet, Etterretningstjenesten og PST for å se hvilke trusler som regnes som de største for petroleumsindustrien i Norge.

Angrepsscenarioer

Masteroppgaven "Preparedness Exercises for Cyber Attacks Against Industrial Control Systems in the Petroleum Industry" [SH21] fra 2021 utarbeidet scenarioer for cyberangrep mot petroleumsindustrien. Masteroppgaven er relativt ny, og det ble gjennomført både en litteraturstudie og samtaler med industrien. Angrepsscenarioene er derfor velbegrunnede og dermed et godt utgangspunkt for arbeidet med vår oppgave. Resultatet fra kartleggingen av trusselbildet i kapittel 2.2 ble brukt til å vurdere hvilke av angrepsscenarioene som var mest relevante. En komplett beskrivelse av angrepsscenarioene vi har brukt i vår oppgave finnes i tillegg A.

Barrierer

En kombinasjon av søk på Google Scholar og NTNU Oria ble brukt for å innhente relevant litteratur om barrierer. I tillegg mottok vi relevante artikler og rapporter fra veiledere. Resultatene inkluderte litteratur om barrierer, barrierestyring, barrierer for cybersikkerhet og ikke-tekniske barrierer. Søkene på Google Scholar og NTNU Oria ble gjennomført med ulike kombinasjoner av søkeordene *"barrier management"*, *"cyber security"*, *"petroleum"*, *"non-technical"*, *"operational"* og *"organisational"*. Videre tok oppgaven utgangspunkt i rapportene "Guidance for barrier management in the petroleum industry" [HØ16] fra SINTEF, "Barrier management in Operation for the Rig Industry" [ØWFR14] fra DNV og "Barrier Memorandum 2017" [PSA17] fra Petroleumstilsynet for definisjoner knyttet til barrierer og barrierestyring. En del av litteraturen ble også funnet i kildelistene til rapportene og artiklene som er lest.

Søkene ble spisset inn mot allerede eksisterende litteratur om barrierer for cybersikkerhet med søket *"barrier management" AND ("cyber security" OR "cybersecurity")* på NTNU Oria og Google Scholar. Søket ga henholdsvis 17 og 48 treff, der ingen av artiklene på Oria var relevante for oppgaven, mens fem artikler på Google Scholar var relevante. Vi ønsket også å undersøke fordelene og ulempene med ikke-tekniske barrier. Søkene *("barrier management" AND ("nontechnical" OR "non technical" OR "organizational" OR "operational") AND "petroleum")* ble gjort i NTNU Oria og Google Scholar. Søket ble spesifisert til å gjelde petroleumsindustrien for å begrense antall treff. Søket ga henholdsvis 85 og 501 resultater, der vi brukte to av resultatene fra Google Scholar.

3.2 Nyskapning

I nyskapningsfasen ble hovedleveransen i denne masteroppgaven utviklet, nemlig et forslag til en metode for å identifisere ikke-tekniske barrierer for cybersikkerhet. Metoden fikk navnet Metode for identifisering av Ikke-tekniske CyberSikkerhetsbarrierer (MICS). MICS ble utviklet ved at vi selv identifiserte barrierer for et valgt angrepsscenario. Med utgangspunkt i stegene vi gjennomførte for å identifisere barrierene, ble

det utviklet et forslag til en generell metode, presentert i kapittel 4.3. Før utviklingen begynte, hentet vi ut ikke-tekniske krav fra ISA/IEC 62443-2-1. Underveis i prosessen ble det også gjennomført tilbakemeldingssamtaler med industrien for å få innspill til utviklingen.

3.2.1 Identifisering av relevante ikke-tekniske krav i ISA/IEC 62443-2-1

Før utviklingen av barrierene og MICS begynte, definerte vi de relevante ikke-tekniske kravene i ISA/IEC 62443-2-1. IEC 62443 er en viktig standard for cybersikkerhet i OT-systemer i petroleumsindustrien. Derfor kan det gi verdi for industrien om barrierene som ble identifisert med MICS bidro til å dekke ikke-tekniske krav i standarden. Tillegg C viser kravene vi har definert som ikke-tekniske, mens tillegg D viser kravene vi har definert som tekniske i ISA/IEC 62443-2-1.

Det første steget var å sortere ut de ikke-tekniske kravene ved å gå gjennom krav for krav og identifiserte de kravene der aktiviteten utføres utelukkende eller delvis av mennesker. For hvert krav så vi etter hva som skulle gjøres, og stilte spørsmålet: "kan/bør dette gjøres av mennesker?". For noen krav var det spesifisert at det kunne utføres av mennesker. Noen krav kunne ha både manuelle og automatiske operasjoner som måtte være på plass for å oppfylle kravet. De kravene som spesifiserte prosedyrer for å få på plass tekniske løsninger, ble tatt med som ikke-tekniske krav. Kravene vi identifiserte som ikke-tekniske, samt en begrunnelse for hvorfor de enkelte kravene ble valgt, er presentert i tabell 4.1.

Vi avgrenset oss videre ved å finne barrierer som kan settes inn *under* et angrep. For å identifisere de relevante kravene, ble det sett på hvilke krav som burde være på plass *før* et angrep starter og hvilke tiltak som kunne iverksettes *under* et angrep. De ikke-tekniske kravene i ISA/IEC 62443-2-1 som er relevante *under* et angrep er markert i gult i tabell 4.1. De ikke-tekniske kravene som bør være på plass *før* et angrep starter er skrevet i grått i tabell 4.1.

3.2.2 Utvikling av barrierer og MICS

Barrierene ble identifisert med utgangspunkt i et angrepsscenario som ble utdypet etter stegene fra MITRE. For å finne barrierene ble det brukt litteratur om barrierestyring for *safety* i petroleumsindustrien, trusselbildet i petroleumsindustrien, informasjon om tidligere angrep og ISA/IEC 62443-2-1. Eksempelbarrierene er vist i kapittel 4.4. MICS ble utviklet ved å se på stegene vi selv gikk gjennom for å identifisere barrierer og så generalisere de. De fem stegene vi gjennomførte er beskrevet nedenfor, i tillegg forklares et sjette steg som beskriver hvordan MICS ble utviklet.

Steg 1: Fant angrepsscenario

For å identifisere barrierer starter man med å definere fare- og ulykkessituasjoner (se kapittel 2.4.1). Prosessen vår begynte derfor med å velge et angrepsscenario å se nærmere på. Vi tok utgangspunkt i masteroppgaven "Preparedness Exercises for Cyber Attacks Against Industrial Control Systems in the Petroleum Industry" [SH21] fra 2021, der en del av resultatet var angrepsscenarioer for cyberangrep i petroleumsindustrien. Fordi vi prioriterte å bruke tid på å utarbeide MICS, fremfor å utvikle egne angrepsscenarioer, valgte vi å gjenbruke et scenario fra denne oppgaven.

Basert på funn om trusselbildet for petroleumsindustrien (se kapittel 2.2), ble utgangspunktet "Scenario 1: Ransomware" (se tillegg A.1) som beskriver et *ransomware*-angrep initiert av en *phishing*-e-post. Angrepet fortsetter etter at systemene er kryptert, og ender med at angriperen tar kontroll over OT-systemet. Et tradisjonelt *ransomware*-angrep stopper når systemene er kryptert, og er først og fremst et angrep som hindrer tilgang, fremfor at angriper tar kontroll over styringen av systemene. Denne oppgaven velger likevel å referere til angrepsscenarioet som kun et *ransomware*-angrep for å være konsistent med navnet på scenarioet.

Steg 2: Gikk gjennom tiltak fra ISA/IEC 62443-2-1

Etter å ha valgt et angrepsscenario, skrev vi ut noen av stegene i angrepet. Deretter ble de relevante ikke-tekniske tiltakene i ISA/IEC 62443-2-1 gjennomgått, og de tiltakene vi umiddelbart tenkte burde være satt inn for å forsvare seg mot angrepet ble plassert. Gjennomgangen av standarden satte i gang tankeprosessen for hvilke tiltak som burde være dekket for å være beskyttet mot angrepet, og var nyttig for å få et inntrykk av hva standarden krevde.

Steg 3: Plasserte angrepsscenario langs tidslinje

Angrepsscenarioet ble detaljert ved å plassere stegene i MITRE-rammeverket langs en tidslinje. For hvert steg plasserte vi tilsvarende hendelse i angrepsscenarioet. Dette resulterte i en detaljert oversikt over stegene en angriper kunne ha foretatt seg underveis i angrepet. Målet med barrierene er å hindre angriperen fra å komme seg fra et steg i tidslinjen til det neste, og en oversikt over hvert steg gjorde det tydeligere hvilke tiltak som måtte plasseres hvor. MITRE er et velkjent rammeverk som kartlegger angriperens oppførsel og tilstedeværelse i et system under et cyberangrep.

Steg 4: Utarbeidet utkast til barrierer

I steg 4 forsøkte vi å identifisere barrierer som kunne settes inn for å hindre eller begrense omfanget av angrepet. Utfordringen her var å vite når et tilstrekkelig antall barrierer var funnet, noe som kan være en utfordring i den virkelige verden også. For å få dekket så mange tiltak som mulig med barrierene våre, hentet vi informasjon fra

ulike kilder. Tidligere *ransomware*-angrep i petroleumsindustrien og på OT-systemer ble undersøkt, for eksempel Colonial Pipeline og Norsk Hydro (se kapittel 2.2.1). Det er utarbeidet flere rapporter om angrepene og om ulike tiltak som kunne vært satt inn for å ha hindret eller redusert omfanget av angrepene. Tiltakene ble brukt som inspirasjon til barrierer i vårt angrepsscenario. Det ble i tillegg supplert med barrierer basert på litteratur og tilbakemeldingssamtaler fra veiledere og ressurspersoner fra industrien. Underveis i arbeidet noterte vi begrunnelser for hver barriere, som en forsikring om at hver barriere var relevant.

Steg 5: Ferdigstilte barrierene

Barrierene ble ferdigstilt ved å formulere barrierefunksjoner på lik form, der alle begynte med et verb. Videre ble det fylt ut operasjonelle og organisatoriske barriereelementer, og YPFer der det var naturlig. For å få et oversiktlig bilde av barrierene plasserte vi de til slutt i bow-tie-modellen.

Steg 6: Utviklet generell metode

For å lage MICS, ble det hentet inspirasjon fra de foregående stegene (1 til 5) og vi forsøkte å generalisere disse til en metode som skulle være mulig for industrien å ta i bruk på andre angrepsscenarioer. Detaljer som kun var relevante for "Scenario 1: Ransomware" ble fjernet. Det ble i tillegg vurdert hva som var en naturlig rekkefølge for stegene. Steg 2 og 3 byttet plassering i MICS, fordi det å finne og detaljere angrepsscenarioet er naturlig etterfølgende steg. Deretter kan standarden undersøkes som et steg på veien mot å finne barrierer i steg 4 og 5. Prosessen med å utvikle metoden gikk over flere iterasjoner, der samtaler med industrien var en viktig del av utviklingen.

3.3 Evaluering

Underveis i utviklingsprosessen ble ustrukturerte intervjuer brukt for å få tilbakemeldinger på barrierene og metoden. Underveistilbakemeldingene var en del av fase 3.1 i figur 3.1, og ble brukt for å forbedre barrierer og MICS i fase 2.2. Den utbedrede versjonen av MICS ble evaluert på flere måter. Først testet vi metoden selv på flere scenarioer. Videre ble det undersøkt hvordan barrierene vi hadde kommet frem til, bidro til å oppfylle de relevante ikke-tekniske kravene i ISA/IEC 62443-2-1. I tillegg ble en ny runde med tilbakemeldingssamtaler med ressurspersoner fra industrien gjennomført. Den siste evalueringen tilsvarer fase 3.2 i figur 3.1, og resultatene fra denne fasen ble brukt til å ferdigstille MICS og å diskutere resultatet.

3.3.1 Tilbakemeldingssamtaler underveis

Det ble gjennomført samtaler med ressurspersoner fra, eller med tilknytning til, petroleumsindustrien for å få innspill og tilbakemeldinger på metoden og barrierene våre underveis i utviklingsprosessen. Samtalene ble brukt som en ressurs for å få bekreftet eller avkreftet om vi var på rett spor, og for å få innspill til hva vi brude fokusere på. Ettersom vi ønsket at intervjuobjektene skulle snakke om det de mente var mest relevant, ble samtalene gjennomført som ustrukturerte intervjuer. I et ustrukturert intervju bestemmes et tema for samtalen, men utover dette er det ingen føringer på hvilken retning samtalen skal ta [Rob11, s. 280]. I intervjuene var det overordnede temaet barrierene og MICS.

Vi valgte å notere det som ble sagt underveis i samtalene fremfor å ta opp. Dette fordi det viktigste var å få med innholdet i det som ble sagt og ikke hvordan setninger ble formulert eller hvilke ord som ble brukt. For å få med oss mest mulig av samtalene, tok én ansvar for å stille spørsmål som dukket opp underveis, mens den andre hadde ansvar for å notere. Rett etter samtalen ble de viktigste punktene oppsummert for å sørge for at vi hadde samme oppfatning av det som ble sagt. Vi oppsummerte også kort de punktene vi ville ta med videre for å forbedre utkastet.

Etter samtalene ble metoden justert basert på noen av tilbakemeldingene. Tilbakemeldingene innebar blant annet at en tydelig kontekst for metoden burde settes, altså hva den skal brukes til og av hvem. I tillegg kom det frem at ulike selskaper har ulike definisjoner på noen av begrepene som blir brukt i barrierestyring. For å gjøre kontekst og begrepsbruk tydelig, ble det laget en innledning der metodens kontekst ble presisert og begrepene som er brukt i metoden ble forklart etter de definisjonene vi har valgt. Basert på tilbakemeldingene valgte vi også å konkretisere og detaljere stegene i metoden, slik at den skulle bli enklere å anvende direkte. I tillegg ble noen nye barrierer lagt til på tidslinjen.

3.3.2 Teste MICS på flere scenarioer

MICS ble testet på to nye scenarioer fra "Preparedness Exercises for Cyber Attacks Against Industrial Control Systems in the Petroleum Industry" [SH21] med hensikt å evaluere hvordan metoden fungerer i praksis. Scenarioene vi valgte for testing var "Scenario 2: Angrep med USB som aktiverer 4G" (se tillegg A.2) og "Scenario 5: IACS innsideangrep" (se tillegg A.3). Scenario 2 og 5 ble valgt fordi vi ønsket angrep hadde som et litt annet hendelsesforløp enn scenario 1, men som det likevel var mulig å sammenligne.

3.3.3 Mappe barrierene mot krav i ISA/IEC 62443-2-1

Som en del av evalueringen ble det undersøkt om barrierene vi identifiserte med MICS, var i tråd med ISA/IEC 62443-2-1. Derfor ble alle relevante ikke-tekniske krav fra standarden gått gjennom, og vi fant de barrierene for "Scenario 1: Ransomware" som var med på å oppfylle hvert krav.

3.3.4 Evalueringssamtaler med industrien

Samtalene med industrien ble gjennomført som semistrukturerte intervjuer, der vi hadde en predefinert intervjuguide (se tillegg B). Intervjuene foregikk over en periode på to uker. Før samtalene fikk intervjuobjektene tilsendt intervjuspørsmålene, MICS, beskrivelse av "Scenario 1: Ransomware" og eksempelbarrierene knyttet til scenarioet.

Semistrukturerte intervjuer

I et semistrukturert intervju brukes en intervjuguide med en liste med temaer man ønsker å få dekket i løpet av intervjuet, i en gitt rekkefølge og med en gitt ordlyd. Rekkefølgen og ordlyden kan likevel endres i løpet av intervjuet basert på flyten i samtalen [Rob11, s. 280]. Vi valgte å gjennomføre semistrukturerte intervjuer fremfor ustrukturerte intervjuer i denne fasen, fordi vi ville ha noen spørsmål satt på forhånd. Å ha predefinerte spørsmål ga et grunnlag for å sammenligne svarene fra de ulike intervjuobjektene, i tillegg til at vi fikk dekket noen utvalgte temaer som var viktige for å få en tilstrekkelig evaluering av MICS og barrierene. Vi ønsket likevel at intervjuobjektene fikk rom til å styre samtalen i den retningen de mente var relevant, og at vi hadde mulighet til å stille oppfølgingsspørsmål.

Fokusgrupper

Tre av samtalene ble utført som en form for fokusgrupper. I et fokusgruppeintervju samles en gruppe mennesker for å diskutere et gitt emne basert på åpne spørsmål [Rob11, s. 293–294]. Et gruppeintervju vil skape mer data på kortere tid enn et individuelt intervju. Det kan også oppleves tryggere for deltakerne å sitte sammen i en gruppe, i tillegg til at gruppediskusjoner kan føre til flere, og mer spontane svar [Tjo20, s. 123–124]. Det er ulike oppfatninger rundt hva som er den ideelle størrelsen på en gruppe. Robson [Rob11, s. 295] foreslår mellom 6 og 12 personer. I denne oppgaven valgte vi å intervjue folk i par, og vi hadde derfor en gruppestørrelse som var langt mindre enn det Robson foreslår. Grunnen til dette var av hensyn til kapasitet og tidsbegrensning knyttet til oppgaven. Vi mener likevel vi oppnådde flere av fordelene et gruppeintervju gir, ved at det også med to personer vil oppstå diskusjon og at partene kan bygge videre på hverandres ideer.

En svakhet med fokusgrupper er at gruppen kan utvikle en felles forståelse rundt det som diskuteres. Dette kan føre til at individuelle meninger forsvinner, slik at

resultatet av diskusjonen blir det gruppen som helhet mener. En løsning for å minske dette problemet er ha mer enn én fokusgruppe slik at gruppene kan fungere som kontroll for hverandre [Jac15, s. 161–162]. Ved at vi gjennomførte flere intervjuer med mindre grupper, fremfor ett intervju med en større gruppe, kunne vi sammenligne resultatene fra hvert intervju, og dermed få et mer nyansert og presist bilde.

Analyse av data

Etter å ha gjennomført intervjuene, ble dataene vi hadde samlet inn analysert for å kunne vurdere hvordan funnene relaterte til forskningsspørsmålene. Fordi vi hadde samlet inn kvalitative data, valgte vi å bruke tematisk koding for analysen. Tematisk koding er en generell metode for analyse av kvalitative data, og går ut på å kode og gruppere data i temaer [Rob11, s. 467]. En kode er i denne sammenhengen de mest grunnleggende elementene i dataene man har samlet, som også kan knyttes til det fenomenet man undersøker. Et tema er en samling av koder som passer sammen [Rob11, s. 478–479]. Vi begynte analysen med å gjøre oss kjent med dataene, ved å lese gjennom, oppsummere og diskutere hvert intervju. Videre ble hvert intervju systematisk gått gjennom og det ble identifisert koder. Kodene ble så samlet i temaer. For hvert tema ble alle utdrag fra intervjuene med koden som tilhørte det gitte temaet samlet. Ved å se på sammenhengen mellom de identifiserte temaene, kunne vi til slutt å tolke og diskutere funnene våre.

3.4 Troverdighet av undersøkelsen

For å evaluere troverdigheten i oppgaven diskuterer dette kapittelet de tre faktorene validitet, reliabilitet og generaliserbarhet.

3.4.1 Validitet

"En evaluering er gyldig (også kjent som valid) hvis den evaluerer det den er ment å evaluere" [Stø19, s. 121]. Validitet handler altså om hvor gyldige resultatene av forskningen er og kan inkludere at man har fått tak i riktige kilder og om kildene gir riktig informasjon. Hvorvidt kilden evner å gi riktig informasjon kan være knyttet kildens kunnskap om og erfaring med fenomenet som skal undersøkes. Det handler også om kildens vilje til å gi rett informasjon. Validiteten vil styrkes dersom man får informasjon fra flere uavhengige kilder [Jac15, s. 229–231].

For å øke graden av validitet sørget vi for å intervjue personer som hadde mye kunnskap om, og praktisk erfaring med, enten barrierestyring, cybersikkerhet eller begge deler. Det ble ansett som sannsynlig at kildene hadde et ønske om å bidra til forskning på deres fagfelt, og at de dermed hadde insentiv til å oppgi riktig informasjon. På en annen side kan det være problematisk dersom representantene

ønsker å sette sin bedrift i best mulig lys, for eksempel ved å ikke nevne problematiske faktorer. Det at vi har snakket med ti personer totalt, fra ulike deler av industrien, gjør at vi kan sammenligne innspillene fra mange kilder, noe som kan være med å styrke validiteten.

En annen strategi for å sikre validitet i vår oppgave, er ved å bruke triangulering. Triangulering handler om å bruke flere perspektiver, for eksempel to ulike metoder for datainnsamling eller flere observatører, for å se om resultatene bekrefter hverandre [Rob11, s. 158]. I denne oppgaven ble det både gjennomført en litteraturstudie og intervjuer. Intervjuene inkluderte flere personer med ulike roller i industrien, og vi kunne dermed sammenligne resultatene for å få et helhetlig bilde.

3.4.2 Reliabilitet

"En evaluering er pålitelig (også kjent som reliabel) hvis den kan gjentas og gir tilnærmet samme resultat hver gang den gjentas" [Stø19, s. 121]. Reliabilitet handler dermed om hvorvidt resultatene fra en undersøkelse kan reproduseres, altså om andre kan gjenta undersøkelsen og komme frem til de samme resultatene og tolkningene. For kvalitative undersøkelser vil dette innebære åpenhet rundt, og tilstrekkelig detaljerte beskrivelser av, forskningsmetode og analysestrategi [Sil06, s. 282–288]. God dokumentasjon er altså en forutsetning for reliabilitet [Stø19, s. 121].

For å styrke graden av reliabilitet i oppgaven, er det beskrevet nøye hvordan vi har kommet frem til resultatene våre. Søkene er dokumentert med hvilke databaser det er søkt i, og hvilke søkeord som er brukt. For at det skal være mulig å gjennomføre tilsvarende intervjuer som i oppgaven, er det presentert hvilket type selskap intervjuobjektene jobber i, samt hvilken bakgrunn de har. Bakgrunn og bedrift for hvert intervjuobjektene er vist i tabell 3.1. Ettersom det er gjennomført kvalitativ datainnsamling gjennom samtaler, vil det være vanskelig å produsere nøyaktig de samme svarene på nytt, men ved å presentere intervjuobjektene på en oversiktlig måte vil man kunne finne intervjuobjekter med tilsvarende bakgrunn.

Alias	Erfaring	Selskap
Person A	Lang erfaring innen cybersikkerhet, risikostyring og barrierestyring. Spesialiserer seg for tiden ytterligere mot barrierer.	Stort og anerkjent universitet i Norge.
Person B	Lang erfaring innen risikostyring, cybersikkerhet, *safety*, og industriell sikkerhet.	Selskapet driver forskningstjenester, blant annet innen olje og gass.
Person C	Lang fartstid innen barrierestyring rettet mot *safety*, i tillegg til erfaring med cybersikkerhet.	Selskapet opererer i mange land og er eksperter innen blant annet risikostyring og forbedring av sikkerhet. Selskapet har bred erfaring og lang fartstid innen sikkerhet og industrielle systemer.
Person D	Lang erfaring med både IT og OT, i tillegg til lang fartstid innen cybersikkerhet.	Stort oljeselskap som blant annet driver leting, utbygging og produksjon på norsk sokkel.
Person E	Lang erfaring med OT og cybersikkerhet, i tillegg til å ha god kjennskap til IEC 62443.	Samme som for person D.
Person F	Lang erfaring med både *safety* og *security* i petroleumsindustrien.	Selskapet er leverandør til ulike sektorer og er ledende innen energiteknologi. I olje- og gassbransjen ligger fokuset deres blant annet på sikkerhet.
Person G	Lang erfaring med cybersikkerhet.	Samme som for person F.
Person H	Ekspert på barrierer og cybersikkerhet. Har spesielt hatt fokus på industriell cybersikkerhet innen olje og gass. Meget god kjennskap til IEC 62443.	Jobber blant annet i et selskap som er sentralt når det gjelder standarder. Er samtidig konsulent for et selskap som blant annet retter seg mot olje- og gassbransjen, samt cybersikkerhet.

Person I	Lang fartstid innen *safety* og risikohåndtering i petroleumsindustrien.	Selskapet jobber med å bedre kommunikasjon og innsikt i industrielle systemer. På kundelisten står store selskaper innen olje- og gassbransjen.
Person J	Lang erfaring innen IT, infrastruktur og cybersikkerhet.	Samme som for person I.

Tabell 3.1: Oversikt over personer vi har gjennomført samtaler med.

3.4.3 Generaliserbarhet

Det er vanskelig å si å si noe om hvorvidt MICS er en metode som vil fungere generelt for industrien, når den kun er evaluert av et begrenset antall personer og testet på noen få scenarioer. Vi har snakket med et lite utvalg personer med forbindelser til petroleumsindustrien, men med litt ulik bakgrunn. Tilsammen dekker intervjuobjektene felter som cybersikkerhet, *safety* og barrierestyring i petroleumsindustrien. At intervjuobjektene har litt ulik bakgrunn kan være med på å styrke generaliserbarheten, men det begrensede antallet personer vi har snakket med svekker den. Samtidig fikk vi lignende tilbakemeldinger fra flere av intervjuobjektene, noe som kan tyde på at også flere vil kunne være enige. MICS er heller ikke testet i bruk på flere enn tre scenarioer. Et såpass lite antall er for få til å kunne si noe om hvorvidt metoden fungerer på alle andre scenarioer.

3.5 Etikk og personvern

I denne oppgaven snakket vi med flere representanter fra industrien. Gjennom disse samtalene kan vi få innblikk i bedrifters sikkerhet og eventuelle sikkerhetshull. I slike samtaler kan det dukke opp informasjon som i verste fall kan utnyttes av angripere, for eksempel hvis intervjuobjektene blir revet med og ikke er kritiske nok når de snakker. For å redusere risikoen for at sensitiv informasjon ble delt med oss, sendte vi ut spørsmålene vi skulle stille på forhånd. Dermed fikk intervjuobjektene mulighet til å forberede seg og tenke gjennom hva de ønsket å dele.

All informasjon innhentet fra intervjuene ble anonymisert i oppgaven. Navn på personer er fullstendig anonymisert, mens beskrivelse av personens erfaring og informasjon om selskapet er beskrevet på en overordnet måte. Fordi Norge er et lite land, kan det likevel være mulig å identifisere hvilket selskap det er snakk om. For at man i så fall ikke skal kunne knytte informasjon i oppgaven direkte til et selskap, er informasjonen fra intervjuene presentert som en samlet oppsummering slik at det ikke skal være mulig å avgjøre hvem som har sagt hva.

Kapittel 4
Resultater

I dette kapittelet presenteres resultatene fra analysefasen, nyskapingsprosessen og evalueringen. Først oppsummeres funnene fra litteraturstudien, før kravene fra ISA/IEC 62443-2-1 som vi har definert som ikke-tekniske presenteres. Videre presenteres metoden vi har kommet frem til for å identifisere ikke-tekniske cybersikkerhetsbarrierer, MICS. Deretter vises barrierene identifisert for "Scenario 1: Ransomware", sammen med en begrunnelse for hvorfor de ble valgt. Barrierene blir så plassert i en bow-tie sammen med barrierer for to andre angrepsscenarioer. Til slutt presenteres resultatene fra tre valideringsstrategier: teste metoden på flere scenarioer, mappe de foreslåtte barrierene mot ISA/IEC 62443-2-1 og gjennomføre tilbakemeldingssamtaler med industrien.

4.1 Litteraturstudie

Litteraturstudien viste at det finnes en del forskning på barrierer og barrierestyring, men at det er mindre som gjelder spesifikt for petroleumsindustrien og enda mindre som går på barrierestyring for cybersikkerhet. Av artiklene som omhandler barrierer for cybersikkerhet, er det en del som kun fremmer dette som et forslag for videre forskning. Noen artikler presenterer bow-ties med eksempler på cybersikkerhetsbarrierer for konkrete trusselscenarioer for OT-systemer. Barrierene er stort sett overordnede og udetaljerte og gjerne vist som eksempler eller illustrasjoner, uten å gå mer i dybden. For ikke-tekniske barrierer viste litteraturstudien at mennesker har både styrker og svakheter når de bidrar til realiseringen av barrierefunksjoner. Mennesker har evnen til å tilpasse seg uventede situasjoner, men er også tilbøyelige til å gjøre feil. Kvaliteten på prosedyrer og kompetanse trekkes frem som viktige faktorer for å sikre god menneskelig ytelse. En annen observasjon handlet om hvilke begreper som brukes i forbindelse med barrierestyring. Industrien er ikke alltid er enig om hvilke definisjoner som gjelder for de ulike begrepene, noe som er med på å skape forvirring.

4.2 Ikke-tekniske krav i ISA/IEC 62443-2-1

Tabell 4.1 viser kravene vi identifiserte som ikke-tekniske, samt en begrunnelse for hvorfor hvert krav ble valgt. En fullstendig beskrivelsene av kravene finnes i tillegg C. Kravene som står i grått, er de som må være på plass før et angrep skjer. Kravene som er markert i gult er kravene som er aktuelle under et angrep, og er dermed de kravene som er aktuelle for metoden foreslått her. Alle krav til utstyr, prosesser og personell bør være fastsatt før oppstart av et anlegg, men noen av oppgavene utføres først under en uønsket hendelse.

Krav	**Begrunnelse for ikke-teknisk**
ORG 1.1: Information security management system (ISMS)	Koordinering av sikkerhet i IACS med ISMS kan gjøres manuelt.
ORG 1.2: Background checks	Bakgrunnssjekker kan gjøres manuelt.
ORG 1.3: Security roles and responsibilities	Tildeling av roller og ansvar kan gjøres manuelt.
ORG 1.4: Security awareness training	Organisering og planlegging av *security awareness training* gjøres av mennesker
ORG 1.5: Security responsibilities traiining	Organisering og planlegging av *cybersecurity training* gjøres av mennesker
ORG 1.6: Supply chain security	Spesifisering av krav til verdikjede-prosessen kan gjøres manuelt.
ORG 2.1: Security risk mitigation	Identifisering og håndtering av risiko kan gjøres delvis manuelt.
ORG 2.2: Processes for discovery of security anomalies	Kravet spesifiserer at man enten skal gjøre prosessen manuelt eller automatisk.
ORG 2.3: Secure development and support	Det å sikre at komponenter utvikles og støttes ved hjelp av formelt definerte og sikre prosesser kan gjøres i kombinasjon av manuelt og automatisk. Eksempelvis kan det å sette kravene for hva som er greit er en manuell jobb, mens selve sjekkene kan være automatiske.

ORG 2.4: SP reviews	Det å bekrefte at et SP[1] er brukt riktig kan gjøres både manuelt og automatisk, eller i kombinasjon. Eksempelvis kan det å bestemme hva som er riktig bruk være en manuell prosess.
ORG 3.1: Physical access control	Det å kontrollere fysiske tilganger kan være manuelt eller automatisk. Det å bestemme tilgangene er typisk en manuell jobb.
CM 1.1: Asset inventory baseline	Prosessen med å verifisere, dokumentere og vedlikeholde enheter vil være både manuell og automatisk. For eksempel vil dokumentasjon typisk være en manuell jobb.
CM 1.2: Infrastructure drawings/ documentation	Verifisering og vedlikehold av tegninger og dokumentasjon kan gjøres manuelt.
CM 1.3: Configuration settings	Dokumentasjon av konfigurasjonsinnstillinger og å sjekke samsvar med dokumentasjonen kan gjøres manuelt.
CM 1.4: Change control	Autorisering, validering og godkjenning endringer i konfigurasjoner kan gjøres i en kombinasjon av automatisk og manuelt. Eksempelvis vil det å godkjenne endringer typisk være en manuell prosess.
NET 1.1: Segmentation from non-IACS networks	En del av det å definere og håndheve retningslinjer for segmentering og kommunikasjon kan gjøres manuelt, da spesifikt å definere retningslinjene.
NET 1.2: Documentation of network segment interconnections	Det å dokumentere og opprettholde sammenkoblinger mellom nettverkssegmenter kan gjøres delvis manuelt.
NET 1.4: Network autonomy	En del av det å sikre at et IACS kan fungere uten tilkobling til eksternt nettverk kan gjøres manuelt.
NET 1.5: Network disconnection from external networks	Det å sikre at et IACS kan kobles fra eksterne nett er en delvis manuell prosess fordi det krever planlegging.
NET 1.6: Internal network access control	Mitigering eller håndtering av risiko er en delvis manuell prosess.
NET 1.7: Device connections	Identifisering og autentisering enheter kan skje både automatisk og manuelt.
NET 2.1: Wireless protocols	Det å sikre at protokoller som brukes er akseptert for bruk i IACS av industri- og sikkerhetsmiljøene kan gjøres manuelt.

[1] Sikkerhetsprogram (Security Program).

NET 2.3: Wireless properties and addresses	Det å sikre at trådløse nett er konfigurert med egenskaper og nettverksadresser som minimerer nyttig informasjon for angripere kan gjøres delvis manuelt og delvis automatisk. Eksempelvis kan det å bestemme hva som skal konfigureres gjøres manuelt.
NET 3.1: Remote access applications	Det å sikre at applikasjoner som brukes er akseptert for bruk i IACS av industri- og sikkerhetsmiljøene kan gjøres manuelt.
NET 3.2: Remote access connections	Autorisering, autentisering og dokumentering kan gjøres både manuelt og automatisk.
COMP 1.2: Dedicated portable media	Sikring av at bærbare medier er dedikert til en spesifikk bruk kan gjøres både manuelt og automatisk.
COMP 2.1: Malware free	Det å sikre at enheter er fri fra kjent *malware* kan være delvis manuell med eksempelvis å finne hvilke *malware* som er aktuelle.
COMP 2.3: Malware protection software validation and installation	Sikring av at software[2] er testet før det installeres er en prosess som kan være delvis manuell og delvis automatisk.
COMP 3.1: Security patch authenticity/integrity	Sikring av at patcher er verifisert for autentisering og integritet er en prosess som kan gjøres delvis manuelt og delvis automatisk.
COMP 3.2: Security patch validation and installation	Sikting av at patcher er testet for kompatibilitet, godkjent for installering og vedlikeholdt er prosesser som kan gjøres delvis manuelt. I tillegg kan det å godkjenne alle stegene av denne prosessen være en manuell jobb.
COMP 3.3: Security patch status	Sikring av at status dokumenteres kan være en delvis manuell jobb.
COMP 3.4: Security patching retention of security	Sikring av at installering av patcher ikke reduserer risikoen vil være en delvis manuell prosess der noen må ta en vurdering og avgjørelse før, under og etter installeringen.
COMP 3.5: Security patch mitigation	Det å vurdere sikkerhetsoppdateringer kan være delvis manuell ettersom evaluering og adressering av risiko kan gjøres manuelt.
DATA 1.1: Data classification	Identifisering og klassifisering av data kan gjøres manuelt og automatisk, eventuelt en kombinasjon.
DATA 1.2: Protection of data	Det å sikre at data beskyttes kan være delvis manuell. Spesielt det å bestemme hvordan de ulike dataene skal beskyttes.

[2] Programvare

DATA 1.5: Data retention	Det å sikre at retningslinjer og funksjoner støtter sikkerhetsoperasjoner før, under og etter en cyberhendelse kan gjøres delvis manuelt.
DATA 1.6: Data purging	Det å sørge for at alle data som krever beskyttelse slettes/fjernes når en enhet tas ut av drift kan gjøres manuelt og automatisk og det kan være lurt å dobbeltsjekke manuelt.
DATA 1.7: Cryptographic mechanisms	Sikring av at krypteringen som brukes er akseptert av industri- og sikkerhetsmiljøene kan gjøres delvis manuelt.
DATA 1.8: Key management	Sikring av at bruk, beskyttelse og håndheving av levetiden til kryptografiske nøkler følger praksis og anbefalinger kan gjøres delvis manuelt.
DATA 1.9: Public key infrastructure (PKI)	Sikring av at bruken av PKI følger en praksis som er akseptert av industri- og sikkerhetsmiljøene kan gjøres delvis manuelt.
USER 1.1: User identity assignment	Det å sikre at det brukes en prosess for å tildele identifikatorer, autentiseringer og roller til brukere er en delvis manuell prosess der eksempelvis roller defineres manuelt.
USER 1.2: User identity removal	Sikring av at en prosess implementeres kan gjøres manuelt.
USER 1.4: Access rights assignment	Det å sikre at en prosess for å tildele, gå gjennom og fjerne tilgangsrettigheter kan gjøres delvis manuelt.
USER 1.5: Least privilege	Det å sikre at brukere får tilgang og kun riktige tilganger vil være en delvis manuell prosess der det å bestemme hva som er riktige tilganger gjøres manuelt.
USER 1.8: User authentication	Det å sikre at alle menneskelige brukere identifiseres og autentiseres på alle IACS-grensesnitt som kan brukes av mennesker kan gjøres delvis manuelt ved f.eks å kartlegge og ha oversikt over hvor alle grensesnittene er.
USER 1.9: Multifactor authentication	Sikring av at MFA brukes kan være en delvis manuell prosess ved f.eks å kartlegge og bestemme hvor det kan og skal brukes.
USER 1.11: Password protection	Implementering av retningslinjer for passord vil være en delvis manuell prosess ettersom retningslinjene må fastsettes.
USER 1.12: Shared and disclosed/compromised passwords	Implementering av en prosess for å håndtere avslørte eller kompromitterte passord vil være en delvis manuell prosess ettersom man må bestemme hvordan situasjonene skal håndteres.

USER 2.2: Administrative rights authorization	Det å bestemme tilgangskontroller vil være en manuell prosess.
USER 2.3: Multiple approvals	Det å kreve godkjenning fra to eller flere personer for handlinger som kan medføre alvorlig innvirkning på industriprosessen vil være delvis manuell ettersom det å bestemme hvilke handlinger dette gjelder vil være en manuell jobb. I tillegg kan selve godkjenning gjøres manuelt (eksempelvis at man må trykke på den og den knappen).
USER 2.4: Manual elevation of privileges	Det å sikre at det kreves heving av privilegier for alle operasjoner som krever høyere privilegier kan gjøres delvis manuelt ettersom det å bestemme hvilke operasjoner dette gjelder kan gjøres manuelt.
EVENT 1.1: Event detection	Det å oppdage hendelser kan gjøres manuelt.
EVENT 1.2: Event reporting	Rapportering av hendelser kan gjøres manuelt.
EVENT 1.7: Event analysis	Analysering av hendelser kan gjøres manuelt.
EVENT 1.8: Incident handling and response	Det å benytte og opprettholde en prosess for å evaluere og respondere på hendelser kan gjøres delvis manuelt.
EVENT 1.9: Vulnerability handling	Adressering og identifisering sårbarheter kan gjøres manuelt.
AVAIL 1.1: Continuity management	Det å benytte og opprettholde planer er en delvis manuell prosess der det å definere og vedlikeholde planene kan gjøres delvis manuelt.
AVAIL 1.2: Resource management	Det å sikre at IACS-en er beskyttet fra failures som følge av strømbrudd, overbelastning eller hardware[3] failures kan være delvis manuell ettersom det krever planlegging og kartlegging for å få dette til.
AVAIL 1.3: DoS attacks	Det å sikre at IACS-en er beskyttet mot DoS-angrep kan være en delvis manuell prosess fordi det å finne ut og definere hvordan man beskytter mot DoS-angrep kan gjøres manuelt.
AVAIL 2.3: Backup verification	Det å sjekke integriteten til *backup*[4] kan gjøres manuelt.

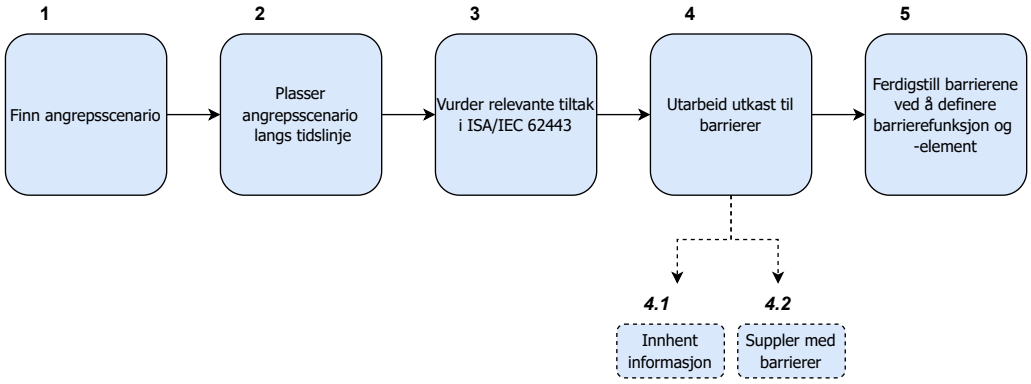
[3] Maskinvare
[4] Sikkerhetskopi.

AVAIL 2.4: Backup media	Det å sikre at *backup* håndteres og lagres på en sikker måte kan være en delvis manuell prosess fordi det må planlegges, bestemmes og defineres hva som er sikkert nok, og bestemmelsene må også opprettholdes.
AVAIL 2.5: Backup restoration	En del av det å sikre at en IACS kan gjenopprettes fra en sikkerhetskopi kan være manuell. Eksempelvis kan det å sjekke *backup* være en delvis manuell prosess.

Tabell 4.1: Begrunnelse av hvilke krav fra ISA/IEC 62443-2-1 [Kob22] som er ikke-tekniske. Kravene markert i grått er de som på være på plass før et angrep skjer, mens kravene som er markert i gult er kravene som er aktuelle under et angrep.

4.3 MICS

MICS er en metode for å identifisere ikke-tekniske barrierer for cybersikkerhet, og er illustrert i figur 4.1. Målet med metoden er å identifisere ikke-tekniske cybersikkerhetsbarrierer for relevante angrepsscenarioer. Metoden kan anvendes på nye angrepsscenarioer for å analysere angrepene før eller etter at de har skjedd. Dersom man identifiserer et nytt mulig angrepsscenario, kan MICS brukes for å være forberedt ved et eventuelt angrep. Hvis man derimot har blitt utsatt for et angrep, kan man i etterkant bruke metoden for å identifisere barrierer for å minske konsekvensene av et eventuelt nytt angrep. Metoden finner barrierer som skal settes inn under et angrep, og ikke barrierer som hindrer angrepet i utgangspunktet.



Figur 4.1: Stegene i MICS.

Metoden bruker følgende definisjoner:

- ***Barriere:*** Et tiltak som skal forhindre eller minske konsekvensene av uønskede hendelser.
- ***Barrierefunksjon:*** Oppgaven barrieren skal løse eller utføre.
- ***Barriereelement:*** Tiltak eller løsning som bidrar til å realisere en barrierefunksjon.
- ***Operasjonelt barriereelement:*** Handlinger og aktiviteter som personale må utføre for å bidra til å realisere en barrierefunksjon.
- ***Organisatorisk barriereelement:*** Personale med definerte roller og spesifikk kompetanse som bidrar til å realisere en barrierefunksjon.
- ***Ikke-tekniske barriere:*** Barriere der barriereelementet er operasjonelt og/eller organisatorisk.
- ***Ytelsespåvirkende faktor:*** Faktor som er avgjørende for at en barriere skal fungere som tiltenkt.

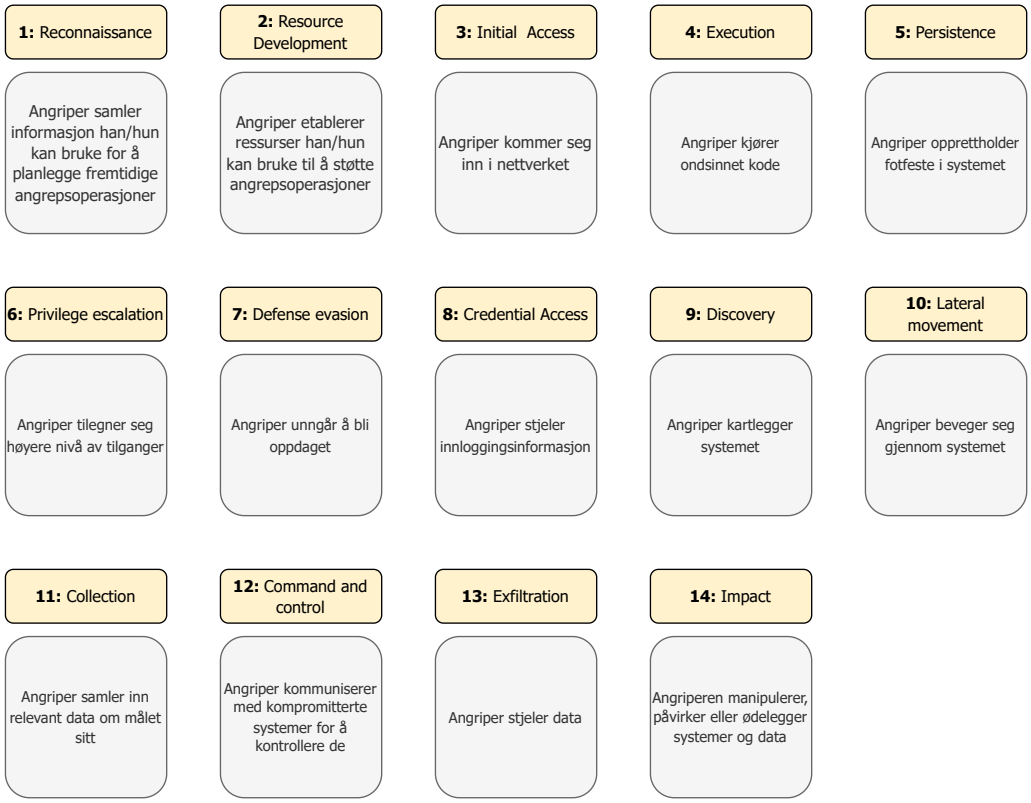
Under beskrives hvert av stegene i MICS i detalj.

Steg 1: Finn angrepsscenario

Velg ut et relevant angrepsscenario ved å vurdere trusselbildet til egen bedrift. For å gjøre dette må man først bestemme hvilket system som skal vurderes. Det må avgjøres hvor en angriper har mulighet til å komme seg inn i systemet og hvor angriperen kan ende opp for å skape en uønsket hendelse. Basert på hvilket system som er i fokus, velges et relevant angrepsscenario for et cyberangrep ut.

Steg 2: Plasser angrepsscenario langs tidslinje

Plasser det valgte angrepsscenarioet inn i de ulike fasene i MITRE-rammeverket. MITRE beskriver de ulike stegene en angriper går gjennom i løpet av et cyberangrep og brukes i denne metoden for å utdype angrepsscenarioet. På den måten får man bedre oversikt over hva som skjer i løpet av angrepet, noe som kan gjøre det enklere å se hvordan og når angriperen kan stoppes. MITRE er også med på å inkludere et IT-perspektiv i den tradisjonelle barrierestyringen. Stegene i MITRE er vist i figur 4.2 som *gule* bokser, mens de *grå* boksene er aktiviteten angriperen gjennomfører i hvert steg. Det kan også være nyttig å markere hvor angriperen beveger seg fra IT- til OT-delen av systemet i tidslinjen. For noen angrep vil ikke alle de 14 stegene gjennomføres av angriper og man kan da markere dette på ønsket måte.



Figur 4.2: De 14 stegene et angrep består av i MITRE-rammeverket [MTb].

Steg 3: Vurder relevante tiltak i ISA/IEC 62443-2-1

Anvend den detaljerte versjonen av angrepet fra steg 2 og vurder hvilke av de ikke-tekniske tiltakene i ISA/IEC 62443-2-1 som bør være på plass for å hindre en angriper i å gå fra ett steg til det neste. Hensikten er å få oversikt over hvilke tiltak i standarden som bør være dekket av barrierene og på den måten starte tankeprosessen rundt konkrete barrierer som kan settes inn. De tiltakene i ISA/IEC 62443-2-1 vi har vurdert som ikke-tekniske og som kan settes inn under et angrep er presentert i tabell 4.2. For noen angrepsscenarioer vil ikke alle kravene være like relevante, og kan i så fall utelukkes for det gitte scenarioet.

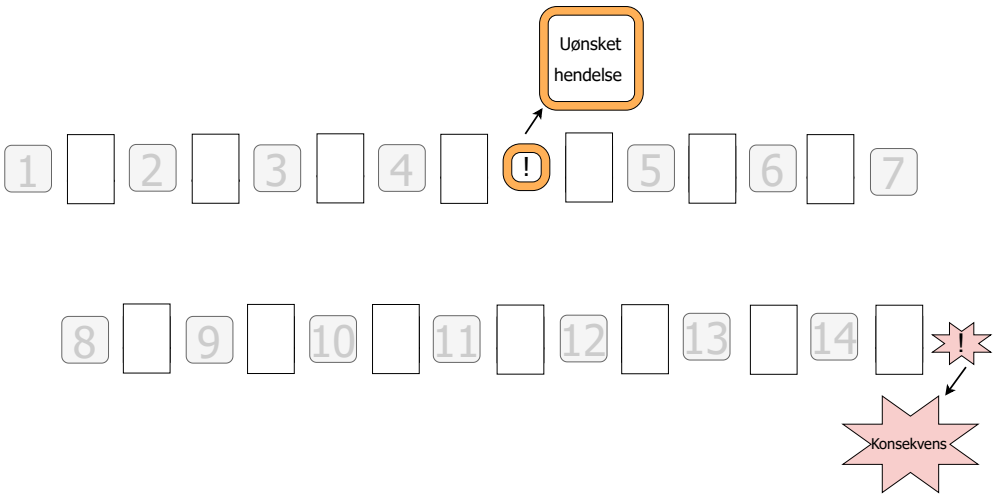
Beskrivelse	**Krav**
ORG 2.2: Processes for discovery of security anomalies	The asset owner shall ensure that the organization periodically uses manual or automated processes to discover and address: a) undocumented and unauthorized devices/software connected to or communicating within the IACS, b) undocumented and/or unauthorized network traffic, c) undocumented vulnerabilities in the IACS, and d) other security anomalies and non-conformities.
NET 1.4: Network autonomy	The asset owner shall ensure that the IACS is able to operate as designed when disconnected from external networks (for example, fail-safe operation, safe shut down, restricted operation and normal operation).
NET 1.5: Network disconnection from external networks	The asset owner shall ensure that the IACS is able to be disconnected from external networks to protect itself from actual or suspected threats.
NET 1.6: Internal network access control	The asset owner shall ensure that security risks associated with communications between internal IACS network segments are mitigated, or otherwise managed.
DATA 1.1: Data classification	The asset owner shall ensure that all IACS data requiring safeguarding are identified and classified according to their protection requirements.
DATA 1.2: Protection of data	The asset owner shall ensure that all data requiring safeguarding, whether at rest or in motion (electronically or physically), shall be protected from compromise according to their classification.
DATA 1.5: Data retention	The asset owner shall ensure that data retention policies and capabilities support security operations before, during and after a cyber event.

USER 1.5: Least privilege	The asset owner shall ensure that only IACS users are assigned access rights to the IACS, and they are only granted the access rights that they require to perform their assigned tasks.
USER 1.8: User authentication	The asset owner shall ensure that all human users are identified and authenticated on all IACS interfaces that can be used by human users to access the IACS. This includes, but is not limited to: a) device interactive human user login interfaces, b) application interfaces such as web servers, file transfer protocol (FTP) servers and OPC servers, and c) remote desktop interfaces that provide human users login access to IACS devices over the network.
USER 1.12: Shared and disclosed/compromised passwords	The asset owner shall ensure that a process is implemented for managing shared and disclosed/compromised passwords.
USER 2.2: Administrative rights authorization	The asset owner shall ensure that IACS users who are logged onto the OS with administrative privileges are not able to access control system functions of the IACS.
USER 2.3: Multiple approvals	The asset owner shall ensure that approval by two or more users are required for actions that can result in serious impact to the industrial process, unless failure to perform the action can result in a greater impact to the industrial process.
USER 2.4: Manual elevation of privileges	The asset owner shall ensure that explicit elevation of privileges, including supervisor overrides, are required for all operations that require elevated privileges.
EVENT 1.1: Event detection	The asset owner shall ensure that IACS events are detected to support security management activities that include reporting, logging, analysis and response (immediate or delayed).
EVENT 1.2: Event reporting	The asset owner shall ensure that IACS events are reported in a timely manner.
EVENT 1.7: Event analysis	The asset owner shall ensure that security-related events are analyzed to identify and characterize attacks, security compromises and security incidents.
AVAIL 1.2: Resource management	The asset owner shall ensure that the IACS is protected from resource/equipment failures due to power disruptions, capacity/processing overloads and hardware failures.

Tabell 4.2: Relevante ikke-tekniske krav fra ISA/IEC 62443-2-1 [Kob22].

Steg 4: Utarbeid utkast til barrierer

Finn forslag til barrierer som kan settes inn for å hindre eller begrense omfanget av det valgte angrepet. I dette steget vil det innebære å skrive ned utkast til ikke-tekniske tiltak som kan settes inn for å hindre angriperen fra å bevege seg fra ett steg i angrepet til det neste. Figur 4.3 viser hvordan barrierer er plassert mellom hvert steg i MITRE (fra figur 4.2). Merk at det ikke er sikkert den uønskede hendelsen kommer etter steg 4, så dette må eventuelt tilpasses for de spesifikke angrepsscenarioene.



Figur 4.3: Plassering av barrierer mellom de 14 stegene i MITRE langs en tidslinje.

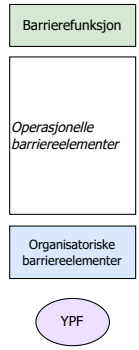
Prosessen med å identifisere barrierer har ikke nødvendigvis en definert slutt, da det er vanskelig å fastslå nøyaktig når man har identifisert nok barrierer til å håndtere et angrep. Under følger to delsteg, steg 4.1 og 4.2, som er inkludert for å finne flere relevante barrierer.

Steg 4.1: Innhent informasjon om hva som kan stoppe angrepet
Oppsøk informasjon om tidligere angrep som ligner på det utvalgte angrepsscenarioet og les eventuelle rapporter som er utarbeidet i etterkant av angrepene. Rapportene kan inneholde foreslåtte tiltak som kunne begrenset eller forhindret angrepet og kan være en inspirasjon til å definere barrierer for angrepsscenarioet.

Steg 4.2: Suppler med barrierer basert på egne erfaringer og diskusjoner
Suppler med barrierer basert på egen erfaring eller diskusjoner med interne eller eksterne parter. Interne parter kan være ansatte i bedriften med kompetanse innen barrierer eller *security*. Eksterne parter kan for eksempel være konsulenter med kompetanse innen cybersikkerhet. Ansatte som har jobbet i bransjen lenge vil ha større grunnlag for å utnytte egen erfaring, mens andre må i større grad basere seg på litteratur og diskusjoner. For å i etterkant kunne forstå tanken bak barrierene som har blitt valgt, bør begrunnelser for valg av barrierer dokumenteres.

Steg 5: Ferdigstill barrierene

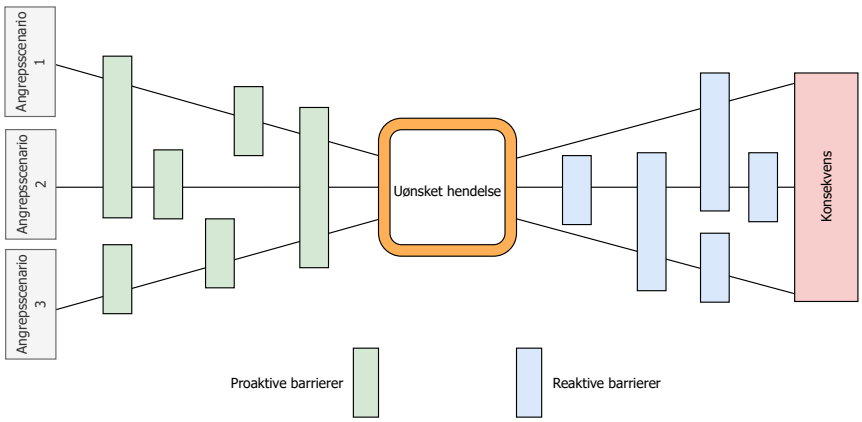
Ferdigstill barrierene ved å skrive alle barrierefunksjonene på lik form slik at de begynner med et verb. Ettersom MICS er en metode for å identifisere ikke-tekniske barrierer skal man for hver barrierefunksjon identifisere operasjonelle og organisatoriske barriereelementer. Et eksempel på hvordan barrierene kan illustreres er vist i figur 4.4 der barrierefunksjon, operasjonelle barriereelementer, organisatoriske barriereelementer og ytelsespåvirkende faktor er markert. Ytelsespåvirkende faktorer kan plasseres der man ønsker å understreke faktorer som er viktig for å forbedre ytelsen til barrierene.



Figur 4.4: Mal for barrierer med barrierefunksjon, barriereelementer og ytelsespåvirkende faktor.

Etter å ha gjennomført steg 1-5 står man igjen med en tidslinje som beskriver angriperens steg i detalj, samt konkrete barrierer for å hindre angriperen fra å komme fra et steg til neste. For å sette dette inn i en større kontekst for bedriften kan barrierene puttes inn i en bow-tie sammen med andre angrepsscenarioer som resulterer i samme uønskede hendelse. Dette gir en total oversikt over hvilke barrierer som bør være på plass for å hindre spesifikke uønskede hendelser. For å forenkle

bow-tien trenger man ikke å skrive barrierer som er like for flere angrepsscenarioer flere ganger. Bow-tie-modellen er illustrert i figur 4.5.



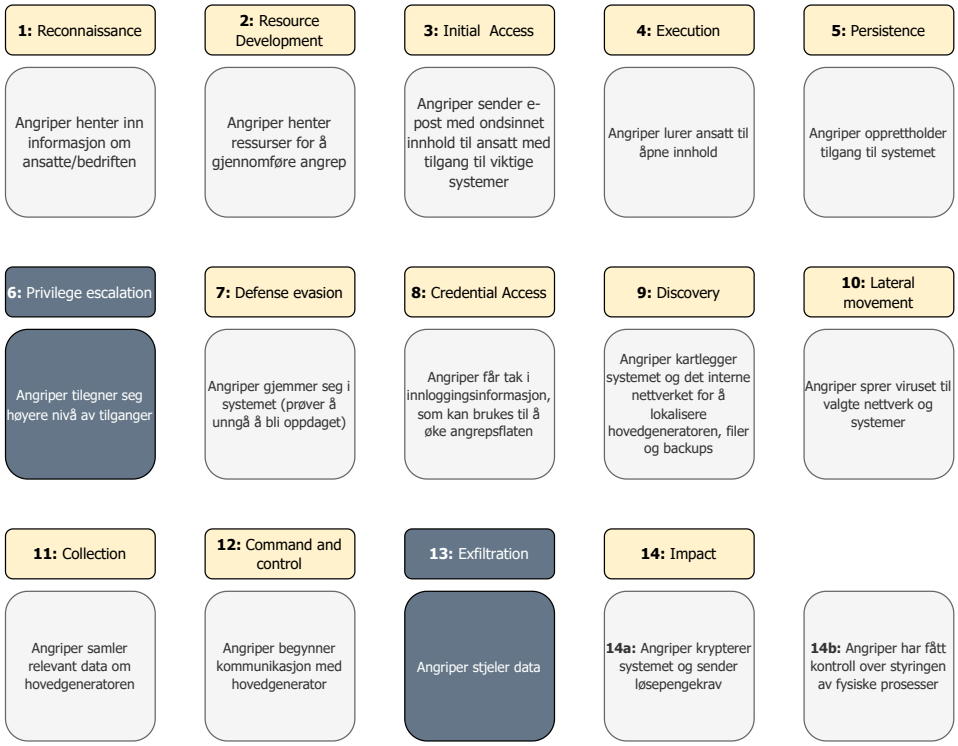
Figur 4.5: Bow-tie for oversikt over barrierer.

4.4 Barrierer for "Scenario 1: Ransomware"

Ved å bruke MICS for "Scenario 1: Ransomware" (tillegg A.1), ble det identifisert 27 barrierer. Figur 4.6 viser angrepets hendelsesforløp satt inn i de 14 stegene i MITRE-rammeverket, og figur 4.7 viser en tidslinje med stegene sammen med en oversikt over plasseringen til de ulike barrierene. Figur 4.8 og 4.9 viser innholdet i barrierene. Tabell 4.3 viser en begrunnelse av hver barriere. Til slutt er barrierene plassert i en bow-tie sammen med barrierer fra flere angrepsscenarioer i figur 4.10.

4.4.1 Angrepet plassert i MITRE

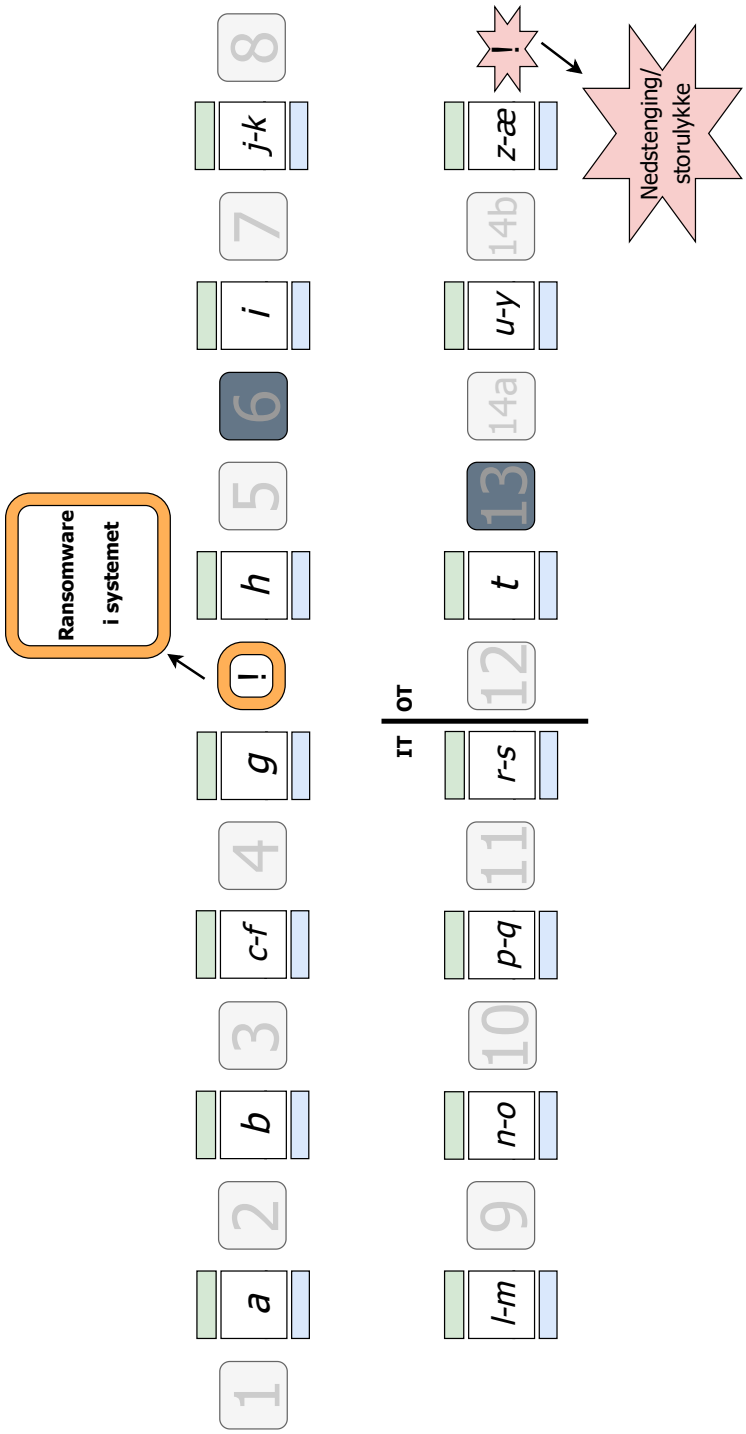
Figur 4.6 viser scenarioet satt inn i de 14 stegene i MITRE-rammeverket. Stegene som er regnet som relevante for scenariet er vist i lys grå, de stegene som ble regnet som mindre relevante for scenarioet er markert i mørk grå. Steg 6 og steg 13 er regnet som mindre relevante. Steg 6 fordi den ansatte som åpner e-posten allerede har høyt nivå av tilganger til viktige deler av systemet, og steg 13 fordi angriperen i scenarioet ikke stjeler noe data.



Figur 4.6: Stegene i hendelsesforløpet for "Scenario 1: Ransomware" satt inn i de 14 stegene i MITRE-rammeverket. Stegene som er regnet som relevante for scenariet er vist i lys grå, stegene som ble regnet som mindre relevante er markert i mørk grå.

4.4.2 Tidslinje med barrierer

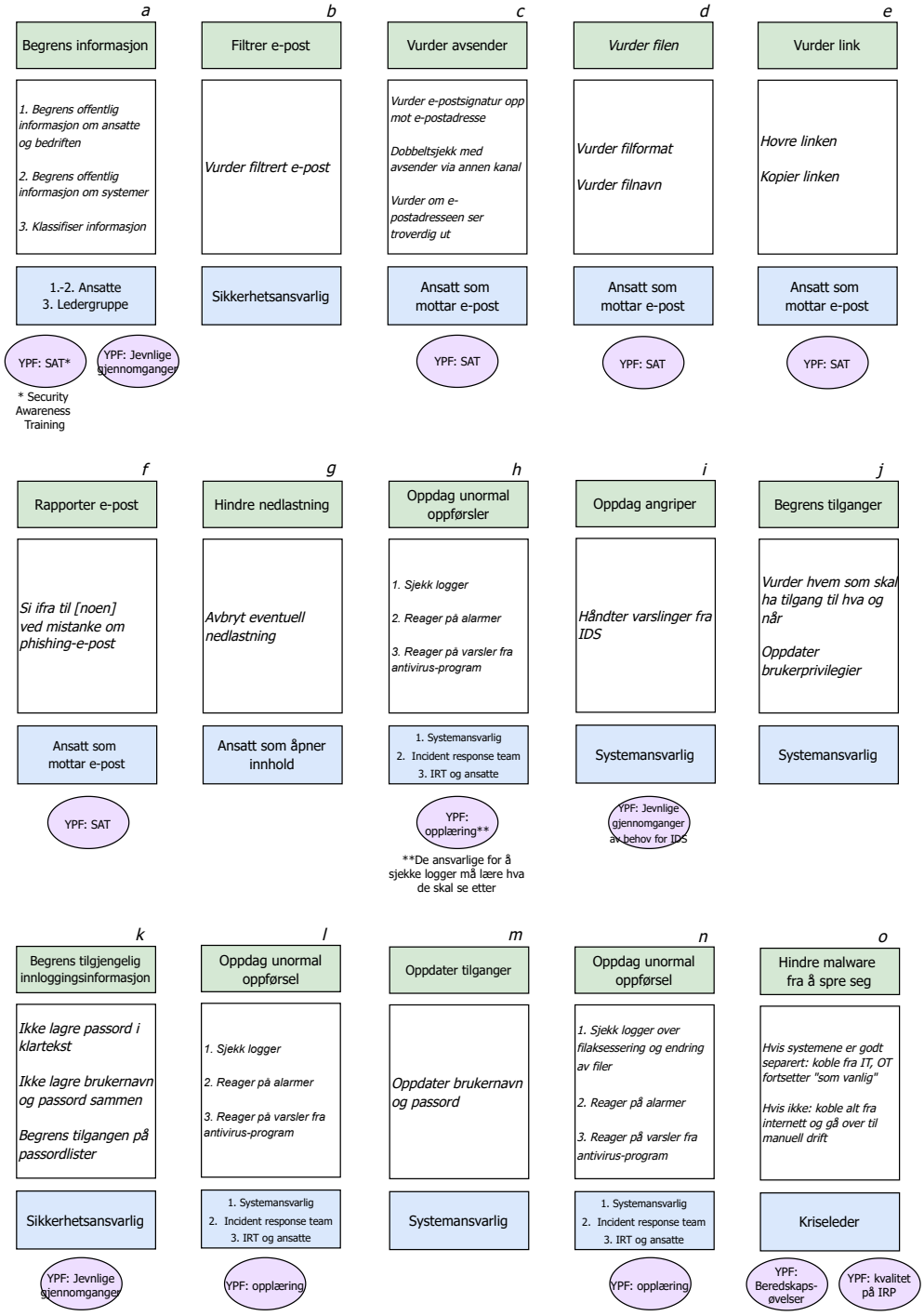
Figur 4.7 viser en tidslinje med stegene fra MITRE sammen med en oversikt over hvor ulike barrierer er plassert. Den oransje firkanten viser tidspunktet der *ransomware* kommer inn i systemet, og representerer dermed den uønskede hendelsen. Barrierene som er plassert før dette punktet er proaktive, mens barrierene etter dette punktet er reaktive. Streken før steg 12 markerer tidspunktet der angriperen beveger seg fra IT-delen av nettverket til OT-delen. Her har altså angriperen kommet seg forbi DMZ (se kapittel 2.1.3). Den røde stjernen viser den ytterste konsekvensen av angrepet, som i dette tilfellet er satt til å være total nedstenging eller en storulykke. En mulig konsekvens av angrepet kan være blokkering av kritiske sikkerhetsfunksjoner, noe som kan påvirke muligheten til å stenge ned systemer ved for eksempel ved lekkasje, for høyt trykk eller for høy varme.



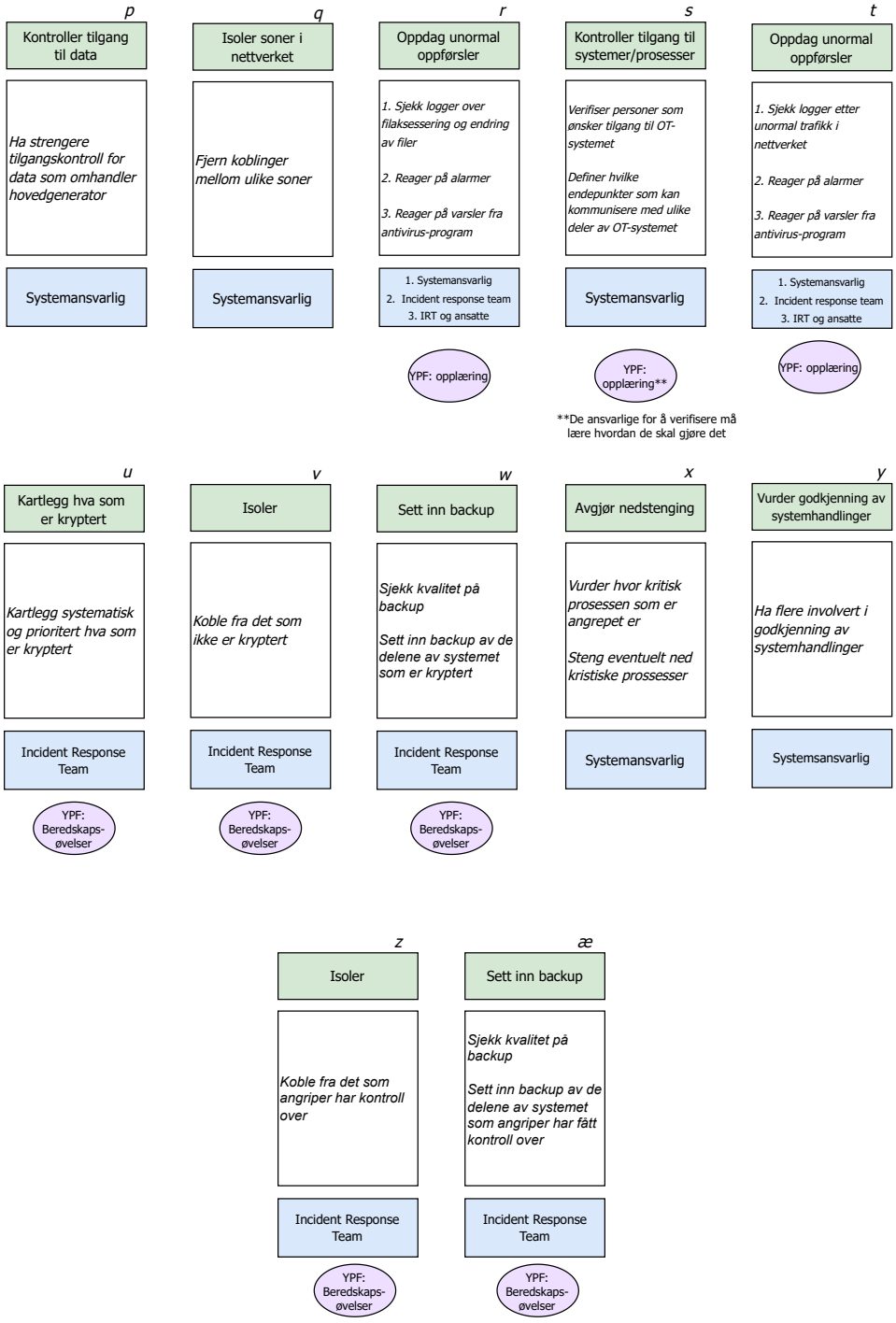
Figur 4.7: Tidslinje for "Scenario 1: Ransomware" (tillegg A.1) med oversikt over barrierer. Bokstavene refererer til barrierene.

4.4.3 Barrierer

Figur 4.8 og 4.9 viser de identifiserte barrierene for “Scenario 1: Ransomware”. Grønn boks viser barrierefunksjon, hvit boks viser eksempel på operasjonelt barriereelement, blå boks viser eksempel på organisatorisk barriereelement og lilla oval viser eksempel på ytelsespåvirkende faktor.



Figur 4.8: Barrierer for "Scenario 1: Ransomware" (1/2). Grønn boks viser barrierefunksjon, hvit boks viser eksempel på operasjonelt barriereelement, blå boks viser eksempel på organisatorisk barriereelement og lilla oval viser eksempel på ytelsespåvirkende faktor.



Figur 4.9: Barrierer for "Scenario 1: Ransomware" (2/2). Grønn boks viser barrierefunksjon, hvit boks viser eksempel på operasjonelt barriereelement, blå boks viser eksempel på organisatorisk barriereelement og lilla oval viser eksempel på ytelsespåvirkende faktor.

Begrunnelse av barrierene

Tabell 4.3 viser en begrunnelse for hvorfor hver av barrierene vist i figur 4.8 og 4.9 er tatt med. Barriere *a* er et tiltak som må settes inn i forkant av et slikt angrep som det beskrevet i "Scenario 1: Ransomware". Barrieren er likevel inkludert fordi et angrep som initieres av en *phishing*-e-post begynner allerede når angriperen henter inn informasjon. Både mengden og typen informasjon som er tilgjengelig kan direkte påvirke hvor realistisk en angriper klarer å lage en *phishing*-e-post og dermed sannsynligheten for at angrepet lykkes.

Barriere	Begrunnelse
a	Informasjon om ansatte og bedriften kan brukes til å skreddersy *phishing*-e-poster til enkeltpersoner, noe som øker troverdigheten. NSM anbefaler derfor virksomheter å vurdere hvor mye informasjon om ansatte som skal ligge åpent på internett [NSM21a]. Fra samtaler med industrien fant vi at det også kan være gunstig å klassifisere informasjonen bedriften håndterer for å ha kontroll på hvilken type informasjon som kan ligge offentlig og ikke.
b	Bedrifter blir anbefalt å ha automatisk filtrering av e-post [DT20] for å blokkere ut *phishing*-forsøk. Ved å vurdere den filtrerte e-posten vil man for eksempel kunne se om det er unormalt mange *phishing*-forsøk rettet mot bedriften og eventuelt be ansatte om være ekstra oppmerksomme.
c	En måte å oppdage at noen forsøker å utgi seg for å være en annen, er å sjekke om avsenders underskrift i e-posten samsvarer med e-postadressen [NV19a]. Dersom man mistenker å ha mottatt en *phishing*-e-post bør man dobbeltsjekke med den angitte avsender via en annen kanal, for eksempel over telefon, for å bekrefte eller avkrefte dette [NTB19].
d	Vedlegg kan inneholde *malware* og man bør derfor være forsiktig dersom man mottar vedlegg via e-post [AK21]. I første omgang bør filformat og filnavn vurderes. I tillegg kan det være gunstig å dobbeltsjekke med avsender at filen var ment til deg og at den er trygg å åpne [AK21].
e	Dersom en e-post inneholder en link bør denne sjekkes grundig før man eventuelt trykker på den. En måte å vurdere linken på er ved å holde musepekeren over (hovre linken) for å se hva den faktiske nettadressen linken fører til er [NV19a; AK21]. En annen metode er å skrive adressen inn i nettleseren manuelt [NV19a].

f	I en bedrift bør man ha rutine for å varsle ved mistanke om *phishing*-forsøk. Da trenger man en ansvarlig som er kontaktperson for de ansatte [AK21; NS21]. Varslingen er viktig for at den ansvarlige skal kunne håndtere situasjonen videre [NS21], for eksempel ved å bevisstgjøre andre ansatte om at de bør være ekstra oppmerksomme. Dermed kan man hindre at andre ansatte blir lurt. For at så mange som mulig skal kunne rapportere *phishing*-forsøk, bør det være lav terskel for å gjøre dette. Et eksempel er Microsoft sin e-posttjeneste, Outlook, der du kan markere en e-post som et *phishing*-forsøk [MS22]. Andre alternativ kan være at man manuelt varsler ved å videresende e-posten til en angitt e-postadresse [NTNU].
g	Dersom man laster ned et vedlegg fra en mottatt e-post og kommer på at vedlegget eller avsender ikke ble vurdert, bør man avbryte nedlastingen for å forsøke å stoppe ondsinnet kode i å infisere datamaskinen.
h	Bedrifter anbefales å ha logger over all bruk av internett, samt bedriftens systemer og nettverk [NV20]. Det anbefales også spesifikt å ha logger over innlogginger på kontoer, skriving til fil og utføring av oppgaver [TL21]. Videre anbefales det å jevnlig gå gjennom logger for å avdekke unormal oppførsel [NV20]. Basert på samtaler med industrien kom det frem at det å reagere på alarmer og varsler fra antivirusprogrammer også bidrar til å kunne oppdage unormal oppførsel, og til å oppdage det i tide.
i	Basert på samtaler med industrien fant vi at det er viktig å ha rutiner for håndtering av varslinger fra Intrusion Detection System (IDS)[5]. Det er fordelaktig å vite hva man skal gjøre med varslene fra IDS-ene for å raskest mulig få kartlagt situasjonen og få stoppet angriperen.
j	Det er anbefalt å begrense autorisasjoner og tilgang til systemer, samt å bruke strenge tilgangskontroller. Man bør også sørge for at brukere har unike ikke-administratorkontoer under normal drift og at administratorkontoer kun skal brukes i utvalgte tilfeller og i begrensede tidsrom. Det er også anbefalt å begrense fysisk tilgang til systemer for å redusere risikoen for blant annet innsideangrep [TL21]. For å redusere risiko skal ikke flere enn nødvendig ha tilgang til ulike systemer eller deler av systemer. NSM anbefaler også at brukere som trenger administratorrettigheter skal ha to kontoer [NSM19b]. Basert på dette kan man tenke at det er mulig å oppdatere brukerprivilegier dersom man for eksempel mistenker at angriperen har fått rettigheter til å endre sensitive filer. Da kan det spesifikke brukerprivilegiet endres for å hindre angriperen i å utnytte det.

[5] Inntrengingsdeteksjonssystem.

k	NSM er tydelig på at man skal unngå lagring av passord i klartekst [NSM19b]. Basert på tidligere hendelser der passord og brukernavn har kommet på avveie har man sett at passord og brukernavn heller ikke bør lagres sammen [Bek19; e2419]. I tillegg ser man ofte at passordlister ligger ubeskyttet på en felles lagringsplass i bedrifter eller i e-post-servere. Dette er informasjon angripere kan finne og bruke for å få tilgang til systemer [Bek19].
l	Samme begrunnelse som barriere *h*.
m	Det er viktig å ha rutiner for å oppdatere passord dersom man mistenker det er på avveie [NV19b]. I bedrifter er det i tillegg viktig å innføre rutiner for å bytte standardpassord på nytt utstyr [NSM19b]. Gjennom samtaler med industrien kom det også tydelig frem at dersom ansatte slutter i en bedrift er det viktig å ha rutiner for å fjerne de fra systemene, noe som innebærer at brukernavn og passord slettes. Det samme gjelder dersom ansatte bytter stilling internt. Da skal tilgangene oppdateres og de gamle tilgangene skal slettes.
n	Samme begrunnelse som barriere *h*. Her er det i tillegg spesifisert at man skal sjekke logger over filaksessering og endring av filer ettersom angriperen i steg 9 (i figur 4.7) blant annet bruker filaksessering til å kartlegge systemet.
o	Dersom *malware* oppdages i IT-nettverket er det å koble fra nettverk og servere en taktikk for å hindre spredning. Dette ble blant annet gjort under angrepet på Norsk Hydro [Bri19]. En forutsetning for dette er at IT- og OT-nettverkene er godt segmenterte, som vist i kapittel 2.1.3. Gjennom samtaler med industrien fant vi at man ofte kan fortsette noe av driften manuelt dersom deler av nettverk stenges ned. Ved god separering i nettverket vil man da kunne holde større deler av det totale nettverket oppe og heller stenge av mindre deler ved eventuelle angrep.
p	Som vi så for barriere j er det anbefalt med strenge tilgangskontroller [TL21]. Ettersom angriper i neste steg samler relevant data om hovedgenerator, er det her spesielt viktig at denne dataen har strenge tilgangskontroller.
q	Som vist i kapittel 2.1.3 er det hensiktsmessig å dele systemer og nettverk inn i soner, blant annet for å kunne begrense og avgrense konsekvensene av uønskede hendelser [TBH+21]. Før steg 11 (i figur 4.7) vil man da kunne hindre angriper fra å komme seg inn i kritiske soner i nettverket ved å koble de fra. Gjennom samtaler med industrien kom det samtidig frem at alt ikke nødvendigvis kan kobles fra. Derfor er det viktig å på forhånd være klar over hvilke systemer og soner som kan kobles fra og ikke. Det er også viktig at man trener på å koble systemer fra hverandre slik at det gjøres på riktig måte.

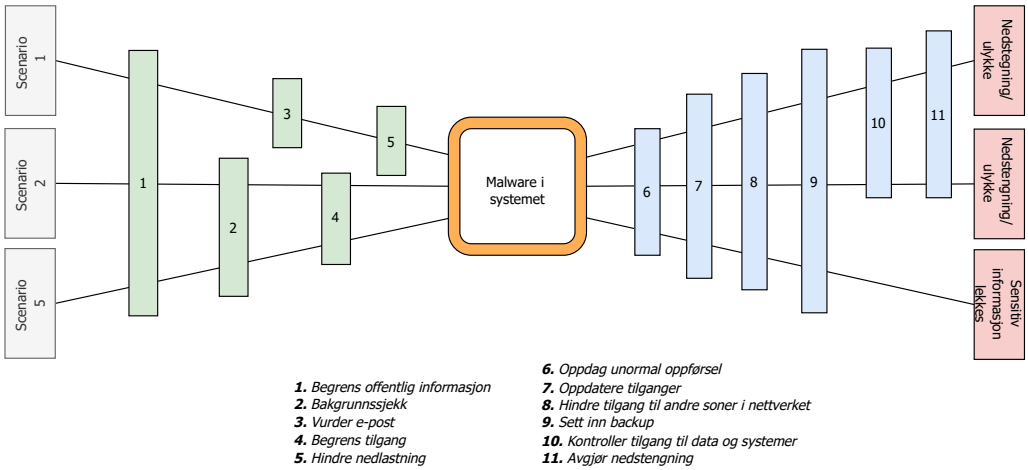
r	Samme begrunnelse som barriere h. Her er det i tillegg spesifisert at man skal sjekke logger over filaksessering og endring av filer ettersom angriperen i steg 11 (i figur 4.7) samler relevant informasjon om hovedgeneratoren. Denne informasjonen kan for eksempel finnes i filer.
s	Som vi så for barriere j er det anbefalt med strenge tilgangskontroller, i tillegg til å begrense fysisk tilgang til systemer, dette for å redusere risikoen for blant annet innsideangrep [TL21]. Gjennom samtaler med industrien forsto vi at det er spesielt viktig å verifisere personer som ønsker å bevege seg fra IT-delen av systemet over til OT-delen. Verifisering av personer kan for eksempel skje via en telefonsamtale, slik at terskelen for å bli verifisert blir høyere. Det er også gunstig å definere hvilke endepunkter som kan kommunisere med ulike deler av OT-systemet, som en del av prosessen med å kontrollere tilgang til systemer og prosesser.
t	Samme begrunnelse som barriere h. Her er det i tillegg spesifisert at man skal sjekke logger etter unormal nettverkstrafikk ettersom angriperen i steg 12 (i figur 4.7) starter kommunikasjon med hovedgenerator og dette er som kan oppdages ved å undersøke nettverkstrafikk.
u	Når man er under angrep som innebærer at systemer blir kryptert, er et viktig steg i beredskapen å analysere og vurdere hendelsen før man forsøker å gjenopprette mest mulig. For å kunne sette inn *backup* som erstatter det som er kryptert, er det nyttig å kartlegge hva som er kryptert og om *backup*en er kryptert [Gri22]. NSM understreker at det er viktig å kun sette inn *backup* man er helt trygg på etter et angrep [NSM21b].
v	En strategi for å hindre *malware* fra å spre seg er å koble fra det som er infisert, slik at det som foreløpig ikke er berørt av angrepet forblir uberørt [NSM21b].
w	Etter et angrep ønsker man å erstatte det kompromitterte systemet. Derfor er det viktig å ha gode rutiner rundt *backup* [NSM21b; Gri22]. *Backup* må tas og den må lagres, helst fysisk separat fra det originale systemet. *Backup*en må holdes oppdatert, og må sjekkes og godkjennes før de eventuelt settes inn i systemene [Gri22].
x	Under angrepet på Norsk Hydro ble det nødvendig å stenge ned prosesser for å hindre at angriperen tok full kontroll over disse [Bri19]. Under samtaler med industrien ble det lagt vekt på viktigheten av å tenke nøye gjennom hvilke prosesser man stenger. Det viktigste er å stenge potensielt farlige prosesser som innebærer for eksempel varme og trykk, og som kan føre til eksplosjoner.

y	Gjennom samtaler med industrien fant vi at man kan ha en mer kompleks prosess for å godkjenne at handlinger for å gjøre det vanskeligere for en angriper å overta fysiske prosesser. For eksempel kan man bestemme at to personer må godkjenne en handling som vil føre til store endringer i systemet eller prosesser.
z	Samme begrunnelse som barriere *v*.
æ	Samme begrunnelse som barriere *w*.

Tabell 4.3: Begrunnelse av barrierer i figur 4.8 og 4.9.

Bow-tie diagram

For å validere MICS, ble metoden anvendt på flere scenarioer, "Scenario 2: Angrep med USB som aktiverer 4G" (tillegg A.2) og "Scenario 5: IACS innsideangrep" (tillegg A.3). Dette er ytterligere beskrevet i kapittel 4.5.1, og vi kom frem til to nye sett med barrierer. Den uønskede hendelsen i disse to scenarioene er også former for *malware* i systemet. For å få et mer helhetlig bilde og en oversikt over relevante barrierer for *malware*-angrep, er barrierene samlet i et bow-tie diagram som er vist i figur 4.10. Her er noen barrierer slått sammen til mer overordnede oppgaver for at figuren skal bli mest mulig oversiktlig.



Figur 4.10: Bow-tie-diagram med barrierer for "Scenario 1: Ransomware", "Scenario 2: Angrep med USB som aktiverer 4G" og "Scenario 5: IACS innsideangrep" fra tillegg A.

4.5 Validering av MICS

Tre ulike strategier ble brukt for å validere MICS. Den første var å teste metoden på flere scenarioer. Videre er det gjort en mapping mellom de foreslåtte barrierene og ISA/IEC 62443-2-1. I tillegg er det gjennomført samtaler med industrien for å få tilbakemeldinger på metoden.

4.5.1 Teste på flere scenarioer

MICS er testet på ytterligere to scenarioer, "Scenario 2: Angrep med USB som aktiverer 4G" (tillegg A.2) og "Scenario 5: IACS innsideangrep" (tillegg A.3). Under testingen ble det observert at metoden fungerte for å identifisere barrierer for de nye scenarioene. For hver test gikk prosessen litt raskere, både fordi vi ble mer vant til å bruke metoden, men også fordi det var mulig å gjenbruke noen barrierer. En utfordring vi møtte på, var at det var vanskeligere å detaljere angrepet i henhold til MITRE i den delen av angrepet der angriper er i OT-delen av systemet. Jo tidligere angriperen kom seg inn i OT-systemet, jo mer krevende var det altså å plassere angrepet i henhold til stegene i MITRE.

4.5.2 Mapping av barrierer mot krav i ISA/IEC 62443-2-1

Tabell 4.4 viser mappingen mellom barrierene identifisert for Scenario 1: Ransomware", opp mot de relevante ikke-tekniske kravene ISA/IEC 62443-2-1. Alle kravene dekkes av minst en barriere, og de fleste har mange barrierer knyttet til seg. Altså bidrar barrierene til å dekke de relevante kravene.

Krav	**Barrierer som bidrar til å oppfylle kravet**
ORG 2.2: Processes for discovery of security anomalies	b, c, d, e, f, h, i, l, n, r, t
NET 1.4: Network autonomy	q, v, x, z
NET 1.5: Network disconnection from external networks	o
NET 1.6: Internal network access control	q, v, z
DATA 1.1: Data classification	a, k

DATA 1.2: Protection of data	a, j, k, m, p
DATA 1.5: Data retention	m, p, s
USER 1.5: Least privilege	j, m, p, s, y
USER 1.8: User authentication	j, p, s
USER 1.12: Shared and disclosed/compromised passwords	k, m
USER 2.2: Administrative rights authorization	j, s, y
USER 2.3: Multiple approvals	y
USER 2.4: Manual elevation of privileges	j, p, s, y
EVENT 1.1: Event detection	f, h, i, l, n, r, t
EVENT 1.2: Event reporting	f
EVENT 1.7: Event analysis	b, f, u
AVAIL 1.2: Resource management	Alle barrierene

Tabell 4.4: Relevante ikke-tekniske krav fra ISA/IEC 62443-2-1 [Kob22], samt hvilke av de identifiserte barrierene som bidrar til å oppfylle kravene.

4.5.3 Samtaler med industrien

Samtalene med industrien ga gode innspill til hva som fungerte med MICS og hvilke utfordringer metoden har. Intervjuobjektene har til sammen bred erfaring innen barrierestyring og cybersikkerhet i petroleumsindustrien og har gode forutsetninger for å se nye aspekter ved metoden. Tilbakemeldingene er oppsummert under.

Ikke-tekniske barrierer. Den generelle tilbakemeldingen fra intervjuobjektene var at MICS virket som en god måte å tilnærme seg det å identifisere ikke-tekniske bar-

rierer. De ikke-tekniske barrierene vi hadde identifisert for "Scenario 1: Ransomware" med MICS, var velkjente og nyttige tiltak. Samtidig ble det presisert at selskaper i praksis vil måtte konkretisere tiltakene ytterligere, for eksempel ved å presisere enkeltpersoners navn.

Det ble også nevnt at selv om metoden finner ikke-tekniske barrierer, vil disse ofte være tett knyttet til tekniske barrierer. Ofte kreves det en samhandling mellom tekniske og ikke-tekniske elementer for å realisere en barriere. Et eksempel kan her være passord der retningslinjene er ikke-tekniske, mens selve sjekken som gjøres når en ansatt lager et passord vil være teknisk.

ISA/IEC 62443. En del av intervjuobjektene syntes det var vanskelig å svare på hvorvidt MICS bidrar til å dekke kravene fra ISA/IEC 62443-2-1. Fordi standarden er så omfattende, opplevde noen av intervjuobjektene at de ikke kjente standarden godt nok til å kunne gi et konkret svar. Samtidig kom det kommentarer på at det er bra at standarden benyttes i metoden, da man oppnår en felles base å referere til. Det ga også mening å bryte ned kravene slik vi har gjort det, med å identifisere hvilke krav som er aktuelle og kategorisere det på samme måte som i standarden. Det var konsensus om at metoden bidrar godt til å dekke deler av standarden, men at brukere må være klar over at ikke alle kravene i standarden vurderes.

Steget med å finne krav fra standarden er arbeidskrevende. I praksis vil ikke alle ha mulighet til å velge ut krav fra standarden, fordi den er for omfattende og mange ikke er tilstrekkelig kjent med den. Et forslag til forarbeid var å lage en database der alle kravene er listet og kategorisert, slik at man enkelt kunne funnet krav som var relevante i gitte tilfeller. Jobben som vi har gjennomført med å sortere ut de ikke-tekniske tiltakene fra standarden i en egen tabell er et steg på veien. Industrien sliter med å sette IEC 62443 i system, og denne oppgaven bidrar med en byggestein i det store bildet.

Relevans av scenarioet. Tilbakemeldingene fra intervjuobjektene var at et *ransomware*-angrep er relevant for petroleumsindustrien. Det er flere kjente tilfeller av *ransomware*-angrep, og et slikt angrep kan resultere i tap av kontroll. Samtidig var det vanskelig å si om det er det mest relevante angrepsscenarioet, blant annet fordi man i bransjen mistenker at mange tilfeller ikke blir rapportert om til offentligheten. Videre vil et slikt angrepsscenario kunne være mer relevant for mindre bedrifter med færre ressurser, ettersom de store bedriftene ofte har høy grad av overvåkning av systemene sine og god segregering av nettverk. Det kan også hende at angrep direkte mot OT-systemene, for eksempel ved å koble inn en USB, kan være vel så relevant som at *ransomware* sprer seg via IT-nettverket. Det ble også trukket frem at angrepstyper som krever mindre av en angriper, for eksempel et DoS-angrep, kan være mer sannsynlig.

MITRE. Intervjuobjektene var enige om at MITRE-rammeverket var et fornuftig valg for MICS. Det er hensiktsmessig å anvende et veldefinert, globalt rammeverk som mange viser til. Fordi det er velkjent, oppnår man en grunnleggende enighet om begreper. Dette gjør diskusjoner mer effektive og hindrer misforståelser.

MITRE deler angrepet opp i flere konkrete steg, noe som er passende for vårt formål. Fokuset for metoden var å finne barrierer som må være på plass under selve angrepet. I den konteksten gir MITRE-rammeverket mening, fordi det handler om å minske konsekvensene av angrepet i seg selv, og ikke om å redusere sannsynligheten for at et slikt angrep kan skje. Ved å bruke MITRE har vi funnet et rammeverk for å identifisere alle oppgavene et *Security Operations Center (SOC)*[6] må gjøre for å hindre at *ransomware* sprer seg.

Deltakerne mente det var tillitsvekkende at vi brukte MITRE som utgangspunkt for tidslinjen, for så å finne tiltak mellom hvert steg som passer som barrierer. En anerkjent, systematisk metode sikrer man at å få belyst ulike sider ved et angrep. Slik kan man unngå hull midt i kjeden av hendelser der det ikke er satt inn tiltak.

Barrierebegreper. I løpet av intervjuene ble et tydelig at man i ulike selskaper bruker barrierebegrepene litt ulikt. Et av intervjuobjektene mente at de foreslåtte barrierene er oppgaver som kan stoppe et hendelsesforløp, men at disse oppgavene ikke kan defineres som barrierefunksjoner. For å finne barrierefunksjonene måtte vi ha gått ett nivå opp slik at flere mindre oppgaver samlet bidrar til å oppfylle funksjonen. Et eksempel som ble presentert er at hvis barrierefunksjonene er å begrense spredning, innebærer dette både å detektere og isolere. Intervjuobjektet påpekte også at industrien selv sliter med å finne gode barrierefunksjoner.

MICS i praksis. MICS ble beskrevet som detaljert og systematisk, om enn noe omfattende. Under intervjuene ble det trukket frem at siden metoden er forholdsvis lang, kan det påvirke hvor effektiv den er. Noen av intervjuobjektene påpekte også at dersom man ser for seg å bruke metoden på mange angrep, vil det i flere tilfeller kunne ende opp ganske like resultater og mange av de samme barrierene.

Det var delte tilbakemeldinger knyttet til om MICS vil kreve for mye ressurser. På den ene siden ble det trukket frem at kostnad er en utfordring, og at det i en bedrift kan være vanskelig å få tak i nok ressurser for å bedre cybersikkerheten. Samtidig mente et intervjuobjekt at de tidkrevende aspektene som er beskrevet i metoden, er ting som uansett bør være på plass i en bedrift for å være godt nok beskyttet, og at man derfor ikke kan si at metoden er for ressurskrevende. Videre poengterte flere av intervjuobjektene at arbeidet som er gjennomført med å sortere ut krav fra ISA/IEC 62443 er nyttig. Samtidig ble det understreket at når man sorterer ut krav,

[6] Sikkerhetssenter.

er det viktig å ikke overse andre sentrale aspekter. I tillegg inneholder andre deler av ISA/IEC 62443 såkalte *Security Levels (SL)*[7] som beskriver ulike krav avhengig av modenhetsgraden til bedriften. I praksis kan det hende bedriften ønsker å sikte seg inn mot spesifikke nivåer, og da er dette noe man må ta hensyn til. Derfor vil det kunne være interessant å videreutvikle metoden til å også inkludere SL i fremtiden.

I praksis bør det også legges til et steg som inkluderer en implementeringsplan. En slik plan vil da kunne inkludere informasjon som hvor barrierene skal implementeres og en plan for å sjekke hvor godt barrierene fungerer.

Bruksområde. Intervjuobjektene syntes det var fornuftig å bruke MICS i analysesammenheng, både for nye angrepstyper og angrep bedriften har blitt utsatt for tidligere. For nye angrepstyper er det gunstig å detaljere angrepet for å forstå hendelsesforløpet for så å identifisere barrierer og tiltak man kan iverksette for å beskytte seg. Når det gjelder angrep en bedrift har blitt utsatt for vil det være gunstig å detaljere hvordan angrepet skjedde og markere hvilke tiltak man faktisk hadde og identifisere hva som manglet for at angrepet skulle ha blitt håndtert bedre. Altså vil metoden kunne anvendes både før og etter et angrep, enten for å forberede seg eller for å granske hva som har skjedd.

Flere av intervjuobjektene foreslo at resultatene fra analyser kunne brukes videre til trening og opplæring. Resultatet fra metoden innebærer steg for å stoppe et angrep. De ansatte kan få opplæring i disse stegene og deretter trene på hvert steg for å være forberedt hvis et angrep skulle skje.

[7] Sikkerhetsnivåer.

Kapittel 5
Diskusjon

Det overordnede forskningsspørsmålet (FS) i denne oppgaven er hvordan man kan identifisere ikke-tekniske cybersikkerhetsbarrierer ut fra relevante angrepsscenarioer. I kapittel 1.1 ble det definert to delspørsmål, DS 1 og DS 2, som er med på å svare på FS. DS 1 handler om hvilke barrierer som er relevante for et *ransomware*-angrep, og det å identifisere disse barrierene var en viktig del av å lage en generell metode for å identifisere cybersikkerhetsbarrierer. I DS 2 var målet å avgjøre hvilke krav fra ISA/IEC 62443-2-1 som burde være dekket av barrierene. Vi mener at å inkludere standarden gjør metoden mer nyttig for industrien, da det er denne standarden som brukes i industrien og barrierer kan være en måte å konkretisere tiltak herfra.

Først diskuteres de to delspørsmålene, DS 1 og DS 2, i henholdsvis kapittel 5.1 og 5.2. I kapittel 5.1 ser vi på hvilke ikke-tekniske barrierer som er relevante for å hindre et *ransomware*-angrep mot et OT-system i petroleumsindustrien. Dette inkluderer også hvor relevant angrepsscenarioet vi tok utgangspunkt og de foreslåtte barrierene er. I kapittel 5.2 diskuteres valg av krav fra ISA/IEC 62443-2-1, før diskusjonen rettes mot MICS i kapittel 5.3. Der diskuteres bruken av MITRE, hva som hindrer MICS fra å kunne anvendes av industrien, hvordan MICS fungerer for andre angrepsscenarioer og hvilke bruksområder metoden kan ha. Mot slutten av kapittelet diskuteres metodens relevans og nyskapning, ved å vurdere tilbakemeldinger fra industrien, hvordan MICS skiller seg fra lignende metoder og digitalisering av bransjen. Til slutt diskuterer vi svakhetene ved MICS og oppsummerer hvordan vi har svart på forskningsspørsmålene.

5.1 Ikke-tekniske barrierer for et ransomware-angrep mot et OT-system

Målet med MICS er at den skal identifisere cybersikkerhetsbarrierer ut fra *relevante* angrepsscenarioer, og det er derfor viktig at scenarioet metoden ble utviklet basert på, "Scenario 1: Ransomware", er et relevant angrepsscenario. Scenarioet er hentet

fra en masteroppgave [SH21] som inkluderte utvikling av realistiske angrepsscenarioer i petroleumsbransjen. Fra denne oppgaven ble det valgt ut et scenario basert på trusselbildet i petroleumsindustrien (se kapittel 2.2). Dermed hadde vi et godt utgangspunkt for å finne et relevant scenario. *Ransomware* ble valgt ettersom dette er en økende trussel for OT-systemer i petroleumsindustrien, og slike angrep kan ha store konsekvenser. Basert på dette anser vi at et *ransomware*-angrep er et godt utgangspunkt for utviklingen av metoden vår.

Samtalene med industrien bekreftet at et *ransomware*-angrep er et relevant angrepsscenario for petroleumsindustrien. Slike angrep har skjedd før og har hatt store konsekvenser. Samtidig kan det være vanskelig å avgjøre hvor ofte slike angrep skjer, da bedrifter gjerne skjuler det dersom de blir angrepet. Store bedrifter med gode systemer for overvåkning døgnet rundt, har også mindre sjanse for å bli utsatt for slike angrep. En del av intervjuobjektene mente at andre former for *ransomware*-angrep kunne være mer sannsynlig. Selv om det er mulig at *ransomware* sprer seg til OT-nettverket via IT-nettverket, kan det være mer reelt at *ransomware* infiserer OT-nettverket direkte. *Ransomware* kan for eksempel plasseres direkte i OT-nettverket via en innsideaktør som plugger inn en USB.

Et *ransomware*-angrep som ender med at angriperen får kontroll over systemer, slik det er beskrevet i "Scenario 1: Ransomware", vil kreve en sofistikert angriper med tilgang til mye ressurser. Noen av intervjuobjektene mente at mindre sofistikerte angrep, slik som et *DoS*-angrep, kunne være mer relevant for petroleumsindustrien. Årsaken er at et slikt angrep er enklere å gjennomføre og at angriperen ikke trenger like mye kunnskap for å gjennomføre angrepet. På en annen side viser funnene om trusselbildet at trusselen fra utenlandsk etterretning, for eksempel fra Russland, øker, noe som kan øke sannsynligheten for mer sofistikerte angrep. Et *ransomware*-angrep er altså reelt og relevant for petroleumsindustrien, men det kan også være andre, enklere angrep som kan være vel så relevante.

Da vi skulle identifisere ikke-tekniske barrierer, støttet vi oss både på standarden, litteratur om sikkerhetstiltak og litteratur om tidligere angrep for å finne relevante tiltak. Underveis i barriereutviklingen kom også intervjuobjektene med innspill til hvilke barrierer som burde settes inn under et *ransomware*-angrep. Sammen ga litteratur og intervjuer et godt bilde av aktuelle ikke-tekniske barrierer. Tabell 4.3 viser en begrunnelse for hvorfor hver barriere er relevant. Under evalueringssamtalene med industrien fikk vi tilbakemeldinger på at de identifiserte barrierene var velkjente og nyttige tiltak. På en annen side er det vanskelig å påstå at alle nødvendige ikke-tekniske barrierer er med i vårt eksempel. Barrierene er ment som nettopp et eksempel, og ikke som en fullstendig liste over tiltak som må være på plass. Hovedfokuset i evalueringssamtalene var MICS, og ikke eksempelbarrierene, noe som kan ha ført til at intervjuobjektene ikke har sett like nøye gjennom alle barrierene.

Vi har kun definert barrierer som skal settes inn underveis i et angrep for å hindre angriperen fra å komme seg til neste steg i *ransomware*-angrepet. En naturlig konsekvens av dette er at det vil være noen tiltak som ikke dekkes av eksempelbarrierene, men som likevel kan være viktige for å hindre nettopp et *ransomware*-angrep. Det er for eksempel en del tiltak som må være på plass fra før, for at man kan sette inn de nødvendige barrierene underveis i angrepet. Et eksempel er segmentering. Både IT- og OT-nettverket må være godt segmentert for at det skal være mulig å isolere nettverket under angrep.

Underveis i samtalene fikk vi et innspill på at noen av barrierene vi har identifisert kunne samles til mer komplette barrierer slik at barrierefunksjonen alltid er noe som griper inn og faktisk hindrer hendelsen. For eksempel vil ikke det å vurdere filen i et e-post-vedlegg i seg selv stoppe en hendelse, men være en del av en større oppgave som går på å hindre at *ransomware* kommer inn i systemet. En utfordring her er at barrierebegrepene praktiseres ulikt i industrien, noe som gjør det vanskelig å definere barrierefunksjoner alle er enig i at er på riktig form. Oppgaven presenterer de barrierene som ble utviklet før siste runde med tilbakemeldinger ettersom flertallet mente disse var gode og relevante for angrepet.

Som litteraturstudien viste, finnes det allerede rapporter som presenterer eksempler på cybersikkerhetsbarrierer, blant annet for *malware*. Barrierene i denne oppgaven skiller seg fra disse ved at de er mer konkrete og detaljerte. Vi har også laget et skille mellom hva vi mener er barrierefunksjonen, og hva som er barriereelementet. Målet er at barrierene skal være enklere for et menneske å iverksette. I tillegg er våre barrierer basert på et detaljert angrepsscenario og plassert langs en tidslinje, slik at det er tydelige hva som må skje på hvilket tidspunkt under et angrep. I eksempelbarrierene er det tydelig hva som er en YPF, og hva som er en barriere. For eksempel er *security awareness training* plassert som en YPF, da det ikke er en barriere som griper inn under en hendelse, men øker ytelsen til barrieren. Jo bedre trening den ansatte som skal realisere en barriere har fått, jo mer sannsynlig er det at den ansatte klarer å realisere barrieren, og jo bedre ytelse vil barrieren ha.

5.2 Valg av krav fra ISA/IEC 62443

ISA/IEC 62443-2-1 er inkludert i MICS fordi vi mener at det kan være nyttig for petroleumsindustrien. IEC 62443 er den standarden som brukes for cybersikkerhet i OT-systemer, og som industrien må forholde seg til. Samtidig er det et problem at standarden er vanskelig å anvende i praksis. Den er svært omfattende og kan oppfattes som uoversiktlig. Derfor er det å kunne bruke barrierer som en metode for å konkretisere standarden, samt hente ut de viktigste punktene som bør være på plass, en måte å gjøre standarden mer praktisk anvendelig. Industrien må forholde seg til standarden, så å få den eksemplifisert og konkretisert ved hjelp av barriere

kan være nyttig. Gjennom samtaler med industrien fikk vi positive tilbakemeldinger på inkluderingen av IEC 62443 i metoden.

Selv om IEC 62443 er en anerkjent standard i petroleumsindustrien, finnes det likevel andre kjente standarder som tar for seg cybersikkerhet. ISO/IEC 27000-serien [ISO27] er en standard som retter seg mot cybersikkerhet i IT-systemer, og som vi valgte å ikke inkludere i oppgaven. Fordelen med å kun inkludere IEC 62443 er at resultatet i oppgaven er mer direkte overførbart til industrien. Samtidig kunne det vært nyttig å inkludere for eksempel ISO/IEC 27000-serien for å få et nytt perspektiv fra en standard som ikke anvendes like mye i petroleumsindustrien, men som er velkjent i andre bransjer.

IEC 62443 er en stor standard, og på grunn av tidsbegrensning er oppgaven avgrenset til å se på én del av standarden, ISA/IEC 62443-2-1. Dermed kunne vi fokusere mer på en enkelt del og bruke den mer aktivt i oppgaven. Samtidig vil det si at ikke hele standarden blir inkludert dersom man bruker MICS. I oppgaven brukes ISA/IEC 62443-2-1, som er et utkast til en nyere versjon av standarden IEC 62443-2-1. Ved å bruke den mest oppdaterte versjonen av utkastet vi har tilgang til, vil resultatet fra oppgaven kunne være mer relevant for industrien. Utkastet vil sannsynligvis være svært likt det som blir den endelige versjonen av den oppdaterte IEC 62443-2-1. Samtidig vil det være en ulempe dersom majoriteten av industrien ikke er kjent med den nyere versjonen. For at brukeren av MICS skal være kjent med de kravene vi mener er aktuelle, har vi inkludert de relevante ikke-tekniske kravene i metoden.

Et mål med oppgaven var å finne ikke-tekniske krav i ISA/IEC 62443-2-1 for å bruke de i MICS. Derfor gikk vi gjennom standarden og sorterte ut de kravene som kan defineres som ikke-tekniske. Andre kan argumentere for at noen av kravene som er inkludert, ikke burde vært det, og motsatt. For å gjøre utvelgelsen av krav sporbar, er det presentert en begrunnelse for hvert krav i kapittel 4.2.

En annen utfordring som oppstår, er at hvilke tiltak som må gjøres av mennesker, og hvilke som kan automatiseres, er i stadig endring. På grunn av digitalisering kan det hende at noen av kravene som nå er identifisert som ikke-tekniske vil regnes som automatiserte, tekniske løsninger om noen år, selv om man velger ut kravene basert på samme kriterier som i denne oppgaven. Fordi industrien er i stadig utvikling, vil det derfor være nødvendig å oppdatere listen med krav med jevne mellomrom.

MICS har som formål å identifisere barrierer knyttet til et spesifikt angrepsscenario og som kan utføres i løpet av angrepet. Det var derfor ønskelig at metoden skulle fange opp de tiltakene som settes inn under et angrep. Følgelig er kravene som bør være på plass før et angrep inntreffer, sortert ut fra listen over ikke-tekniske tiltak. Et eksempel er ORG 1.1 (se tillegg C) som innebærer at man skal ha et system for sikkerhetsstyring. Et slikt system må være på plass i forkant av et angrep. I tabell 4.1

er alle de ikke-tekniske kravene inkludert og de som er identifisert som ikke relevant for MICS er grået ut, slik at det er tydelig hvilke krav vi har sortert bort. En ulempe med å sortere ut krav, er at man mister de barrierene som kunne ha hindret angrepet i utgangspunktet. Ved å kun se på en delmengde av krav, kan man også fort miste oversikten over det totale bildet som kreves for å oppnå helhetlig beskyttelse.

Det at vi har sortert ut krav fra ISA/IEC 62443-2-1 som ikke relevante, påvirker resultatet ved at noen kan være uenig med sorteringen. Selv om oppgaven kom frem til at barrierene som ble identifisert med MICS bidro til å oppfylle de relevante kravene i standarden, hadde resultatet vært et annet dersom sorteringen av kravene hadde vært annerledes. I tillegg mister man muligheten til å vurdere om MICS identifiserer barrierer som er i samsvar med hele ISA/IEC 62443-2-1. Samtidig gjør utvelgelsen av krav metoden enklere å håndtere, fordi krav som ikke er regnet som relevante er sortert bort på forhånd. Flere intervjuobjekter mente at sorteringen som er gjennomført er nyttig, ettersom standarden er stor og overveldende, og få setter seg inn i hele standarden.

5.3 Metode for identifisering av ikke-tekniske cybersikkerhetsbarrierer

Fokuset i oppgaven er ikke-tekniske barrierer, altså barrierer der mennesker er en viktig del av realiseringen av barrierefunksjonen. Vi har sett i litteraturen at menneskelige tiltak ikke alltid er like uttalt og spesifisert i standarder, slik som IEC 62443. Samtidig er mennesker ofte regnet som det svakeste leddet når det gjelder cyberangrep, og kan ofte være grunnen til at et angrep blir vellykket. Dette førte til behovet for å spesifisere ikke-tekniske tiltak. Ulempen med å sette helt konkrete ikke-tekniske tiltak, kan være at man tar bort noe av styrken mennesker har til å kunne vurdere situasjoner selv. Samtidig er det gunstig å ha nøyaktige beskrivelser av hva som skal gjøres når for å håndtere situasjonen ettersom tiltakene er knyttet til spesifikke angrepsscenarioer. Det krever imidlertid at menneskene som skal realisere barrierefunksjonene får mulighet til å øve på å realisere de barrierene som skal settes inn, og ha tilstrekkelig kompetanse til å håndtere situasjonene når de dukker opp.

Intervjuobjektene var enige i at MICS kunne identifisere ikke-tekniske barrierer. De har imidlertid hatt begrenset med tid til å sette seg inn i metoden, så for å verifisere dette sikkert, kreves det at metoden testes i praksis av industrien.

Et aspekt som kom frem under intervjuene som er verdt å merke seg, er begrensningene det gir å kun se på ikke-tekniske tiltak. I praksis vil det nesten alltid være tekniske og ikke-tekniske tiltak som jobber sammen, og én barrierefunksjon vil gjerne trenge både tekniske, operasjonelle og organisatoriske barriereelementer for å realiseres (se kapittel 2.3.2). Det kan derfor oppfattes som kunstig å se på ikke-tekniske barrierer

som et isolert konsept. Ved å kun se på de ikke-tekniske barrierene, kan det fort hende man overser andre viktige tiltak. Ett av intervjuobjektene kunne fortelle at man i praksis ofte blir så opptatt av de tekniske tiltakene, at man glemmer de ikke-tekniske. Med MICS oppstår tilsynelatende det motsatte problemet. For at MICS skal være en komplett metode, burde den dermed utvikles videre til å også omfatte tekniske og ikke-tekniske tiltak sammen.

5.3.1 Kobling mellom identifiserte barrierer og ISA/IEC 62443-2-1

I kapittel 4.5.2 presentertes en mapping mellom eksempelbarrierene identifisert for "Scenario 1: Ransomware" og de relevante ikke-tekniske kravene i ISA/IEC 62443-2-1. I oppgaven var mappingen en strategi for å validere MICS. Under samtalene med industrien kom det et innspill om at en mapping opp mot standarden kunne vært med som et siste steg i metoden. Ideelt sett skulle MICS vært testet på et representativt antall angrepsscenarioer, slik at man kan trekke en konklusjon om hvorvidt metoden generelt identifiserer barrierer som oppfyller kravene i standarden, men dette har ikke vært mulig innenfor tidsrammen av denne oppgaven. Hensikten er likevel at det ikke skal være et behov for å inkludere et steg med mapping i selve metoden.

5.3.2 Rammeverket MITRE

MITRE er et anerkjent rammeverk for angrep mot IT-systemer (se kapittel 2.8). I MICS er MITRE brukt for å beskrive hvert steg i hendelsesforløpet til et angrep. Gjennom samtaler med industrien fikk vi tilbakemeldinger på at MITRE var fornuftig å trekke inn som et ledd i barriereutviklingen, og at det var en oversiktlig måte å detaljere et angrep på. Vi har selv observert at MITRE bidrar til å få detaljert et angrep på en oversiktlig måte, og dette var noe av hensikten med å inkludere rammeverket. Et fast rammeverk bidrar til at prosessen med å beskrive et angrep kan gjøres likt for ulike angrepstyper. Vår vurdering er at dette øker verdien til MICS ved at man lettere vil kunne sammenligne angrep og gjenbruke tiltak fra angrep som er analysert tidligere. I tillegg vil bruk av et veldefinert rammeverk gjøre MICS mer effektiv, fordi man vil ha en felles enighet rundt begrepene som brukes.

I oppgaven har vi valgt MITRE Enterprise, og ikke MITRE ICS, som rammeverk for å utdype våre angrepsscenarioer. Vi la merke til at MITRE Enterprise fungerte best til å beskrive angrep mot OT-systemer dersom angrepet starter i IT-systemet. Det viste seg å være mer intuitivt og naturlig å utdype stegene til angriperen i henhold til rammeverket når angriperen beveger seg i IT-systemene. Årsaken er at MITRE Enterprise beskriver hvordan en angriper oppfører seg ved et angrep på IT-systemer, og det er derfor naturlig at det vil være lettere å beskrive IT-angrep med stegene i rammeverket. For angrep der angriperen kommer tidlig inn i OT-systemene kan

det være mer utfordrende å utdype angrepet slik det er beskrevet i MICS. Dette er ulempen med å bruke MITRE Enterprise, og kunne kanskje vært løst ved å heller se på MITRE ICS. På den andre siden er MITRE Enterprise et anerkjent og mye brukt rammeverk for IT, noe som kan gjøre det enklere å anvende også for å definere barrierer. I tillegg hjelper MITRE Enterprise til med å sette fokus på at angrep mot IT-delen av nettverket også vil kunne ha konsekvenser for OT-delen.

5.3.3 Hindringer for at industrien skal kunne anvende MICS

For at industrien skal kunne anvende MICS, bør den være effektiv og enkel å forstå. MICS har få steg, men hvert steg er beskrevet grundig, noe som kan påvirke hvor effektiv den er. En fordel med lengden på MICS er at stegene er detaljert beskrevet. Høy grad av detaljer kan gjøre metoden enklere å ta i bruk uten å bruke lang tid på å sette seg inn i den. Gjennom intervjuene fikk vi tilbakemeldinger på at stegene var tydelige og at det var forståelig hva som skulle gjøres, noe som kan være et argument for at detaljnivået, og dermed lengden, er gunstig.

MICS kommer til å identifisere de samme barrierene for flere ulike cyberangrep. Dermed vil det være lite effektivt å gjennomføre hele metoden for alle disse angrepene. Overflødighet ble nevnt som et mulig problem under intervjuene, og er også trukket frem som en svakhet med barrierer for cybersikkerhet i kapittel 2.5. Ved bruk av metoden i praksis, vil det derfor være hensiktsmessig å undersøke om barrierer fra andre angrepsscenarioer kan gjenbrukes. Vårt forslag er å opprettholde en bank med barrierer man kan plukke fra. En slik bank er noe som kan være naturlig å bygge opp innad i bedriftene eller gjøres samarbeid på tvers av bedrifter. Uansett må bedrifter spesifisere barrierene til sitt eget bruk, for eksempel med konkrete navn på barriereelementer. Med en barrierebank vil det ikke ta like lang tid å anvende metoden på angrep som ligner på angrep man har analysert tidligere. For at dette skal fungere krever det at bedriftene holder oversikt over tidligere resultater av MICS.

Noen av intervjuobjektene mente at å inkludere IEC 62443 førte til at metoden ble veldig ressurskrevende. Standarden er omfattende og komplisert å sette seg inn i, og det er få som har oversikt over hele standarden. Samtidig ble det sett på som positivt at relevante krav fra ISA/IEC 62443-2-1 allerede var spesifisert i MICS. Dette mente mange ville gjøre det enklere både å håndtere standarden og å anvende metoden. Under en av samtalene ble det fremmet et forslag om å utvikle en database der alle kravene i IEC 62443 var kategorisert, slik at det var oversiktlig hvilke krav som var aktuelle og som man kunne plukke fra. Sorteringen i denne oppgaven kan i så fall være et skritt på veien mot en slik kategorisering.

Intervjuobjektene trakk frem at det ofte er vanskelig å få nok ressurser til å bedre cybersikkerheten. Manglende ressurser kan gjøre at MICS er for omfattende til å kunne anvendes i praksis. Andre mente at selv om det i dag kan være vanskelig å

få ressurser til cybersikkerhet, så trenger det ikke det bety at det alltid må være sånn. For *safety* er det gjerne noen krav man godtar at må være på plass uten at det problematiseres, og dette bør også etterstrebes for *security*. Et av intervjuobjektene var tydelig på at de punktene vi nevner i MICS, slik som oversikt over standarden, tidligere angrep og tiltak, er noe som burde være på plass allerede. Dersom man har tilstrekkelig fokus på cybersikkerhet i industrien, burde MICS derfor være overkommelig for industrien å ta i bruk.

5.3.4 Bruksområder for MICS

MICS kan brukes til å analysere nye angrepstyper og for å skape en oversikt over hvordan man kan beskytte seg mot nye angrepsscenarioer som dukker opp. En forutsetning for dette er at brukeren av metoden er oppdaterte på trusselbildet, noe som kan være en utfordring i praksis. Samtidig er trusselbildet noe man uansett bør være oppdatert på. Dersom en bedrift allerede har vært utsatt for en ny type angrep, kan MICS også brukes i etterkant av angrepet for å få en oversikt over hvilke steg angriperen gjennomførte for å utføre angrepet. Deretter kan det vurderes hvilke barrierer som kunne bidratt til å stoppe angriperen. Analysen av angrepet vil gjøre bedriften mer rustet for lignende angrep i fremtiden. Dette vil gi verdifull informasjon i tilfeller hvor sannsynligheten er stor for å bli utsatt for lignende angrep igjen.

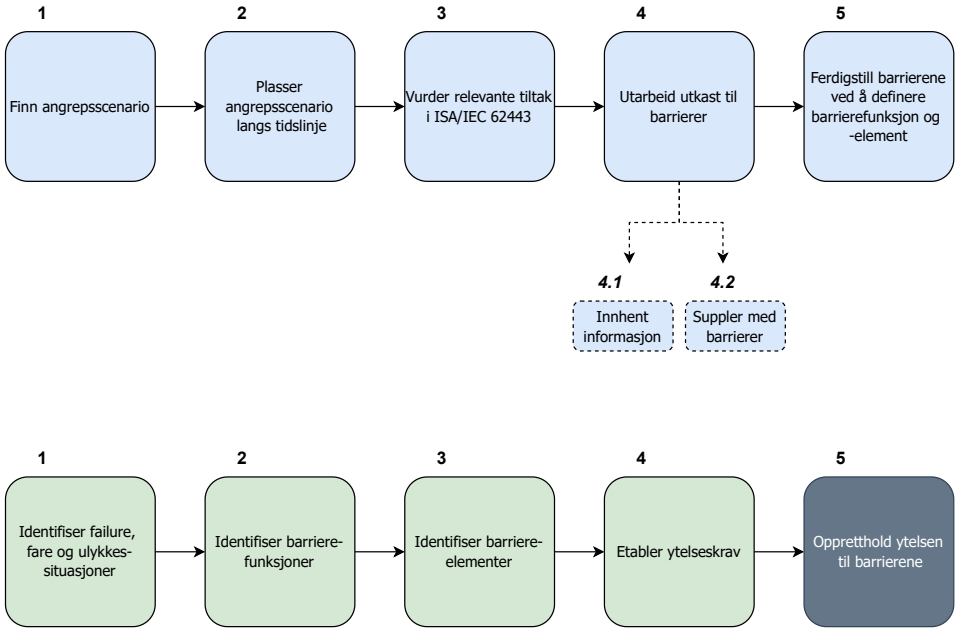
Intervjuobjektene var enige i at MICS fungerer for analyse, samtidig som en del mente metoden også kunne bidra til trening og opplæring. MICS identifiserer barrierer man må trene på å realisere. Ved å bruke MICS som et verktøy for å tilrettelegge for trening, vil den kunne bidra til at personale blir trent i de prosedyrene man har fastsatt. Basert på samtaler med industrien og gjennom litteratur har vi identifisert et problem med at prosedyrer ofte ikke finnes. Hvis de finnes er det ikke alltid ansatte vet om prosedyrene eller har trent på å følge dem. Å anvende resultatet av MICS for trening kan dermed gjøre den mer verdifull.

5.4 Relevans og nyskapning

Som diskutert tidligere i oppgaven ser man en kraftig økning i cybersikkerhetstrusler på verdensbasis. Samtidig er det en trend at IT- og OT-systemer knyttes tettere sammen. Derfor er det viktig å undersøke metoder for å håndtere endringene i trusselbildet. Denne oppgaven har utviklet en metode, MICS, som identifiserer ikke-tekniske barrierer som kan settes inn underveis i et cyberangrep på OT systemer. Ved å innføre barrierebegrepet for cybersikkerhet kan MICS bidra til å se IT- og OT-systemer i sammenheng med hverandre på en ny måte. I kapittel 5.4.1 vil vi gå nærmere inn på forskjellene mellom MICS og SINTEF sin metode for å identifisere barrierer, før vi i kapittel 5.4.2 går nærmere inn på effektene av digitalisering.

5.4.1 MICS sammenliknet med SINTEF sin medode for å identifisere barrierer

I "Guidance for barrier management in the petroleum industry" [HØ16] presenterer SINTEF en prosess for å identifisere barrierer for å hindre ulykkessituasjoner. Prosessen kan beskrives som en metode for å finne *safety*-barrierer, og er utdypet i kapittel 2.4. I denne oppgaven er det sett på utvikling av barrierer for cybersikkerhet, altså *security*-barrierer. Figur 5.1 illustrerer MICS i blått og SINTEF sin metode for barriereutvikling i grønt.



Figur 5.1: Sammenlikning av stegene i MICS og i SINTEF sin metode for barriereutvikling. MICS i blått, SINTEF sin metode i grønt.

Den første forskjellen er at steg 1 i MICS innebærer å finne et angrepsscenario, mens SINTEF sitt steg 1 er å identifisere fare- og ulykkessituasjoner. Altså tar vi ulikt utgangspunkt for utviklingen av barrierene. Dette er naturlig ettersom SINTEF ser på barrierer for å hindre ulykker, mens vi ønsker å stoppe målrettede cyberangrep.

Steg 2 i MICS går ut på å beskrive angrepet i detalj, et steg man ikke finner igjen hos SINTEF. SINTEF tar utgangspunkt i ulykkessituasjoner som kan oppstå og som i mindre grad vil følge et fast mønster. Derfor gir det større verdi å detaljere et angrep, enn å detaljere en uforutsett situasjon. Ved et cyberangrep kan man til en viss grad forvente at angriperen beveger seg på en spesifikk måte, noe som kan bidra

til å identifisere måter å stoppe angriperen på.

I steg 3 bruker MICS en standard, ISA/IEC 62443-2-1, for å finne relevante tiltak. Et slikt steg er ikke inkludert i prosessen fra "Guidance for barrier management in the petroleum industry". En grunn til dette kan være at forfatterne av rapporten har lengre fartstid innenfor fagfeltet, mens vi har undersøkt litteratur i større grad. En fordel ved å bruke IEC 62443, er at man i industrien har krav om å forholde seg til visse standarder. Derfor kan det være fordelaktig at en metode søker å lage barrierer som bidrar til å oppfylle kravene i en standard.

Steg 4 og 5 i MICS omfatter det samme som steg 2 og 3 i SINTEF sin metode. Forskjellen her er at vi har lagt inn et steg, steg 4, som i praksis er et steg der man lager et utkast på barrierer som bør være på plass, samt at man innhenter informasjon og erfaringer fra tidligere angrep. Deretter defineres endelige barrierefunksjoner og -elementer i steg 5. SINTEF sitt steg 2 og 3, altså selve utviklingen av barrierene, fullføres i steg 5 i MICS, selv om prosessen begynner i steg 4 ved idémyldring.

Hovedprinsippene for å identifisere *safety*-barrierer er altså relativt like de vi kom frem til for å identifisere cybersikkerhetsbarrierer, men det er også noen ulikheter. I MICS utvidet er antall trinn som inngår i det å skape et utgangspunkt for å identifisere barrierer utvidet. SINTEF har her ett steg, steg 1, mens MICS har stegene 1, 2 og 3 for å skape utgangspunktet for utviklingen av barrierer. Dette mener vi er hensiktsmessig for de fleste cyberangrep ettersom angripere ofte følger et handlingsmønster som det beskrevet i MITRE-rammeverket.

Videre skiller MICS fra SINTEF ved å ikke dele barrierefunksjonene opp i sub- og sub-sub-funksjoner. I denne oppgaven er selve metoden hovedresultatet og dermed ville vi bruke mest tid på å utvikle den uten å detaljere barrierene ytterligere. Å dele barrierefunksjonene inn i sub- og sub-sub-funksjoner vil imidlertid gjøre det tydeligere og mer presist hva som trengs for å oppnå de ulike barrierefunksjonene. Derfor kunne dette bidratt til at bedrifter kunne ha brukt barrierene vi kom frem til mer direkte. MICS inkluderer heller ikke etablering av ytelseskrav, og stopper når barrierene er identifisert. SINTEF sin metode har på sin side et siste steg som går på å opprettholde ytelsen til barrierene. Steget er ikke inkludert i MICS da det er en metode for å identifisere barrierer, ikke vedlikeholde de.

5.4.2 Digitalisering av bransjen

Petroleumsindustrien er i stadig endring, blant annet som følge av digitalisering, noe som kan påvirke hvor relevant MICS vil være. MICS identifiserer cybersikkerhetsbarrierer, og med økende grad av digitalisering kan metoden bli enda mer relevant. Mer utstyr og flere systemer kobles på nett og angrepsflaten øker. Da kan MICS være en nyttig metode for å kartlegge behovet for tiltak. På den andre siden kan endringer i

bransjen gjøre at metoden blir utdatert, og da spesielt med tanke på relevante krav fra ISA/IEC 62443-2-1. Det kan være nødvendig at metoden blir oppdatert med jevne mellomrom ved å ta en vurdering på hvilke krav som fortsatt er relevante. Dette er arbeidskrevende og kan gjøre metoden mindre attraktiv.

5.5 Svakheter

For å utvikle MICS ble det tatt utgangspunkt i ett angrepsscenario, før ytterligere to scenarioer ble sett på for å validere og teste metoden. Som vi har sett fungerte metoden godt for disse tre scenarioene, noe som indikerer at den også vil kunne fungere bra for andre angrepsscenarioer. Likevel kan ikke dette bekreftes uten at metoden testes på enda flere scenarioer. Ved å teste metoden på flere scenarioer vil man også kunne se tydeligere om barrierene som identifiseres alltid vil være med på å dekke relevante krav i ISA/IEC 62443-2-1.

En utfordring vi møtte på underveis i oppgaven, og spesielt i samtalene med industrien, er at det benyttes ulike definisjoner av begreper innen barrierestyringen. I MICS er det derfor inkludert en tydelig liste over hva som legges i de ulike begrepene, hovedsakelig basert på Ptil [PSA17] sine definisjoner. Selv om denne oversikten er inkludert, kan det oppstå forvirring rundt begrepene. Dersom den som skal bruke MICS i praksis er vant til annen betydning av begrepene, kan det være en uvant omstilling som gjør at metoden blir vanskelig å anvende. En løsning på dette kan være at metoden tilpasses til de begrepene hver enkelt har som praksis i sin drift.

5.6 Svar på forskningsspørsmål

DS 1 handlet om hvilke ikke-tekniske barrierer som var relevante for et *ransomware*-angrep mot et OT-system i petroleumsindustrien, og spørsmålet er i oppgaven tatt stilling til ved å se på et angrepsscenario med *ransomware*. Det er presentert eksempler på relevante barrierer for det spesifikke angrepet, og vi fikk bekreftet av representanter fra industrien at barrierene var relevante. Det som ikke er undersøkt, er om barrierene er like relevante for alle andre typer *ransomware*-angrep, eller om det finnes andre barrierer som også kunne vært relevante.

DS 2 innebar å finne hvilke krav fra ISA/IEC 62443-2-1 som burde være dekket av de ikke-tekniske cybersikkerhetsbarrierene. Vi har gjort vår vurdering av hvilke krav som er relevante og ikke-tekniske. I tillegg er det forklart hvordan vi har tenkt for å finne kravene. Utfordringen med dette at ulike personer vil kunne gjøre ulike vurderinger på hvilke krav som bør være med, noe som gjør det vanskelig å finne ett riktig svar på hva som er aktuelle krav.

For å svare på forskningsspørsmålet ble MICS, en metode for å identifisere ikke-tekniske cybersikkerhetsbarrierer, utviklet. Metoden fungerte godt for angrepsscenarioene den ble testet på og vi fikk gode tilbakemeldinger fra industrien. For å kunne si med sikkerhet at MICS fungerer etter hensikten, bør metoden testes på enda flere scenarioer og i praksis av industrien.

Kapittel 6

Konklusjon og videre arbeid

Oppgaven har undersøkt hvordan barrierebegrepet kan anvendes også for cybersikkerhet. Vi har sett på relevante angrepsscenarioer for å identifisere ikke-tekniske cybersikkerhetsbarrierer som kan hindre eller redusere omfanget av angrepene. Målet var å svare på forskningsspørsmålet "Hvordan kan ikke-tekniske cybersikkerhetsbarrierer identifiseres ut fra relevante angrepsscenarioer for petroleumsindustrien?". For å gjøre dette har vi først svart på de to delspørsmålene, "Hvilke ikke-tekniske barrierer er relevante for et ransomware-angrep mot et OT-system i petroleumsbransjen?" og "Hvilke krav fra ISA/IEC 62443 bør være dekket av de ikke-tekniske cybersikkerhetsbarrierene?".

DS 1 ble besvart ved å identifisere 27 ikke-tekniske barrierer som er relevante for "Scenario 1: Ransomware". Barrierene er vist i figur i figur 4.8 og figur 4.9. Disse ble identifisert ved å studere litteratur om tidligere angrep, samt ved hjelp av tilbakemeldinger fra flere representanter fra industrien. På bakgrunn av dette kan vi konkludere med at de ikke-tekniske barrierene vi kom frem til er relevante for det aktuelle angrepsscenarioet. Det kan likevel finnes andre barrierer som også er relevante.

For å svare på DS 2 om hvilke krav som børe være dekket av de ikke-tekniske barrierene, startet vi med å sortere ut de ikke-tekniske kravene i ISA/IEC 62443-2-1. Deretter identifiserte vi kravene som er relevante under et angrep. Vi valgte å definere dette som de kravene der oppgaven kan utføres under selve angrepet, selv om kravet må fastsettes i forkant av angrepet. MICS inkluderer en liste med de relevante ikke-tekniske kravene som vi mener industrien bør se på når de skal vurdere tiltak i forbindelse med ulike angrepsscenarioer. Listen med krav (presentert i tabell 4.2) er altså vår vurdering av hvilke krav som bør være dekket, og ikke en endelig fasit på hva som er relevante ikke-tekniske krav. Industrien uttrykte at selve sorteringen var nyttig og vil gjøre MICS enklere og mer effektiv å bruke.

Basert på arbeidet med å undersøke DS 1 og DS 2 utarbeidet vi MICS som er en

metode for å identifisere ikke-tekniske cybersikkerhetsbarrierer ut fra relevante angrepsscenarioer for petroleumsindustrien. Barrierene blir ikke-tekniske fordi metoden vurderer de relevante ikke-tekniske kravene i ISA/IEC 62443-2-1, og fordi den ser på barrierer der barriereelementet kan være ikke-teknisk. Det er cybersikkerhetsbarrierer som identifiseres ettersom det i steg 1 av MICS velges ut et relevant cyberangrep. Steg 1 sikrer at man tar utgangspunkt i et angrepsscenario som er relevant for petroleumsindustrien. Bruken av MITRE bidrar til at man lettere får identifisert barrierene ettersom det gir en detaljert oversikt over angriperens atferd.

Oppgaven undersøkte hvordan barrierebegrepet kan anvendes for cybersikkerhet for å bidra til å tette et gap mellom IT og OT. Med MICS har vi identifisert ikke-tekniske barrierer for cybersikkerhet, noe som viser at barrierebegrepet er mulig å anvende på cybersikkerhetstiltak. Basert på tilbakemeldinger fra industrien er arbeidet med å utvikle metoden nyttig, og noe som kan bidra til at petroleumsindustrien kan være bedre forberedt på cyberangrep.

Gjennom arbeidet med oppgaven har vi identifisert hva som kan gjøres for å teste MICS ytterligere, hva som kan inkluderes i metoden for å gjøre den mer nyttig i praksis og hva som må gjøres for å vedlikeholde metoden og holde den aktuell. I tillegg har vi identifisert faktorer som kan være interessant å se på basert på arbeidet i denne oppgaven. Under følger en liste som presenterer det vi har identifisert som videre arbeid:

- Teste MICS på flere scenarioer for å få et bredere spekter og et høyere antall tester.
- Teste metoden i praksis i næringslivet for å undersøke om den fungerer som tiltenkt.
- Inkludere andre deler av ISA/IEC 62443 enn ISA/IEC 62443-2-1 i metoden.
- Undersøke hvordan *Security Levels* fra ISA/IEC 62443 kan trekkes inn i metoden. Hensikten med nivåene er å kunne sikre systemet på en effektiv måte avhengig av hvor kritisk systemet er. Det vil være gunstig å se på hvordan metoden kan justeres for å bestemme sikkerhetsnivå og identifisere barrierer som treffer det valgte nivået.
- Undersøke om MICS vil fungere for å identifisere tekniske barrierer. Da må man bruke de relevante tekniske kravene i ISA/IEC 62443-2-1 istedenfor de som er inkludert i metoden sånn den er nå.
- Inkludere et økonomisk perspektiv i metoden for at industrien skal kunne bruke MICS tilpasset de økonomiske begrensningene man har.

- Inkludere ytelseskrav og ytelsespåvirkende faktorer i MICS i større grad.
- MICS må holdes aktuell og dermed oppdateres med tiden slik at den forblir relevant og holder følge med bransjen når det gjelder digitalisering og eventuelle andre endringer. For eksempel vil de relevante kravene endre seg i takt med digitaliseringen.
- ISO/IEC 27000-serien er en serie standarder som omhandler styring av cybersikkerhet og personvern for IT-systemer. Å vurdere om tiltak herfra kan kombineres med tiltakene fra ISA/IEC 62443 inn i MICS ville vært en interessant øvelse.
- Starte et arbeid der flere i næringslivet går sammen og blir enig om hvilke krav i ISA/IEC 62443 man anser som ikke-tekniske slik at man kan skape en felles enighet og forståelse om dette.
- Utvikle en metode tilsvarende MICS, men med bruk av MITRE ICS. Formålet kan være å sammenligne metodene og undersøke hvilken som fungerer best i praksis for å identifisere barriere for cybersikkerhet.

Referanser

[AK21] M. Asp og O. Kinapel, Slik finner du ut om en e-post er svindel eller ikke, 10. jun. 2021. adresse: https://www.online.no/sikkerhet/slik-finner-du-ut-om-en-e-post-er-svindel-eller-ikke (sjekket 4. apr. 2022).

[AM15] S. S. Alizadeh og P. Moshashaei, «The Bowtie method in safety management system: A literature review», *Scientific Journal of Review*, årg. 4, nr. 9, s. 133–138, 2015.

[Bar22] M. Bartnes, kryptovirus, 21. feb. 2022. adresse: https://snl.no/kryptovirus (sjekket 25. mar. 2022).

[Bek19] B. Bekkevold, Risikobasert autentisering øker produktiviteten, 11. okt. 2019. adresse: https://www.watchcom.no/nyheter/nyhetsarkiv/risikobasert-autentisering (sjekket 4. apr. 2022).

[BFM+18] K. Bernsmed, C. Frøystad mfl., «Visualizing Cyber Security Risks with Bow-Tie Diagrams», i *Graphical Models for Security*, P. Liu, S. Mauw og K. Stolen, red., Cham: Springer International Publishing, 2018, s. 38–56.

[Bri19] B. Briggs, Hackers hit Norsk Hydro with ransomware. The company responded with transparency, 16. des. 2019. adresse: https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency (sjekket 24. mar. 2022).

[CKKL19] N. H. Carreras Guzman, D. Kufoalor mfl., «Combined Safety and Security Risk Analysis using the Ufoi-E Method: A Case Study of an Autonomous Surface Vessel», i *Proceedings of the 29th European Safety and Reliability Conference(ESREL)*, sep. 2019.

[CKL21] N. H. Carreras Guzman, I. Kozine og M. A. Lundteigen, «An integrated safety and security analysis for cyber-physical harm scenarios», *Safety Science*, årg. 144, s. 105 458, 2021.

[CO22] How Do OT and IT Differ? Adresse: https://www.cisco.com/c/en/us/solutions/internet-of-things/what-is-ot-vs-it.html#~q-a (sjekket 21. apr. 2022).

[CWKL20] N. H. Carreras Guzman, M. Wied mfl., «Conceptualizing the key features of cyber-physical systems in a multi-layered representation for safety and security analysis», *Systems Engineering*, s. 189–210, mar. 2020.

[Dav18] P. C. O. David G. Gunter Michael D. Medoff, *Implementing IEC 62443*. exida, 2018, s. 15.

[DNV16] «Cyber security recilience management for ships and mobile offshore units in operation (DNVGL-RP-0496)», DNV GL, tekn. rapp., 2016.

[DNV17] «Cyber security in the oil and gas industry based on IEC 62443», DNV GL, tekn. rapp., 2017.

[Dra] About Dragos. adresse: https://www.dragos.com/about (sjekket 27. apr. 2022).

[Dra19] «Global Oil and Gas Cyber Threat Perspective», Dragos, tekn. rapp., 2019.

[Dra22] «Oil & Natural Gas Cyber Threat Perspective», Dragos, tekn. rapp., 2022.

[DT18] Iverksette styringssystem for informasjonssikkerhet, 30. okt. 2018. adresse: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/iverksette-styringssystem-for-informasjonssikkerhet (sjekket 11. apr. 2022).

[DT20] Phishing - hvordan beskytte virksomheten, 17. jul. 2020. adresse: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/phishing---hvordan-beskytte-virksomheten/hva-er-phishing (sjekket 26. apr. 2022).

[e2419] Hundretusener av nordmenns passord blottstilt på nett, 11. okt. 2019. adresse: https://e24.no/teknologi/i/dOzrP1/hundretusener-av-nordmenns-passord-blottstilt-paa-nett (sjekket 4. apr. 2022).

[FBI22] Ransomware, 28. mar. 2022. adresse: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware (sjekket 30. mar. 2022).

[Gil21] A. S. Gillis, spyware, jul. 2021. adresse: https://www.techtarget.com/searchsecurity/definition/spyware (sjekket 29. mar. 2022).

[Gin20] A. Ginter, «The Top 20 Cyber Attacks on Industrial Control Systems», Waterfall Security Solutions, tekn. rapp., 2020.

[GPMH] T. O. Grøtan, S. Petersen mfl., «SecureSafety; state-of-the-art and remaining challenges», i *e-proceedings of the 30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference*.

[Gri22] F. Grindland, Det er mulig å oppdage digitale angrep før de får konsekvenser, 9. feb. 2022. adresse: https://www.bouvet.no/bouvet-deler/det-er-mulig-a-oppdage-digitale-angrep-for-de-far-konsekvenser (sjekket 4. apr. 2022).

[Gro] T. N. Group, «Industrial Security based on IEC 62443 [Whitepaper]», Tüv Nord Group, tekn. rapp.

[H20] Cyber-attack on Hydro, 14. okt. 2020. adresse: https://www.hydro.com/en-NO/media/on-the-agenda/cyber-attack (sjekket 24. mar. 2022).

[HOJ+21] G. K. Hanssen, T. Onshus mfl., «Premisser for digitalisering og integrasjon IT-OT», SINTEF, tekn. rapp., 2021.

[HØ16] S. Hauge og K. Øien, «Guidance for barrier management in the petroleum industry», SINTEF, tekn. rapp., 2016.

[HØST15] S. Hauge, K. Øien mfl., «Towards a holistic approach for barrier management in the petroleum industry», SINTEF, tekn. rapp., 2015.

[IEC10] «Industrial communication networks - Network and system security - Part 2-1: establishing an industrial automation and control system security program», IEC, 2010.

[ISA20] «Information Technology and Operations Technology: Beyond Convergence [Whitepaper]», International Society of Automation, tekn. rapp., 2020.

[ISA21] «Security for industrial automation and control systems - Part 2-1: Security program requirements for IACS asset owners [Draft 3, Edit 10]», ISA, 62443-2-1, sep. 2021.

[ISA22] «Security for industrial automation and control systems - Models and Concepts [Draft 9, Edit 5]», ISA, 62443-1-1, jan. 2022.

[ISO27] «Information technology - Security techniques - Information security management systems - Overview and vocabulary», ISO/IEC JTC 1, Information technology, SC 27, IT Security techniques, ISO/IEC 27000:2018.

[Jac15] D. I. Jacobsen, *Hvordan gjennomføre undersøkelser?*, 3. utg. Cappelen Damm Akademisk, 2015.

[JWBK21] M. G. Jaatun, E. Wille mfl., «Grunnprinsipper for IKT-sikkerhet i industrielle IKT-systemer», SINTEF, tekn. rapp., 2021.

[KL15] «Chapter 3 - Industrial Cyber Security History and Trends», i *Industrial Network Security (Second Edition)*, E. D. Knapp og J. T. Langill, red., Second Edition, Boston: Syngress, 2015, s. 41–57.

[KO20] P. B. Kristoffersen og K. Omberg, «Cyber security SIS og egensikre komponenter, kommuniksjonsprotokoller», DNV GL AS, tekn. rapp., 2020.

[Kob22] P. Kobes, *Cybersecurity needs a holistic approach: Deep dive in ISA/IEC 62443-2-1*, Intern presentasjon, SINTEF, feb. 2022.

[KR21] S. Kelly og J. Resnick-Ault, One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators, 9. jun. 2021. adresse: https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08 (sjekket 26. apr. 2022).

[Kum16] D. K. Kumar, Colonial may open key U.S. gasoline line by Saturday after fatal blast, 31. okt. 2016. adresse: https://www.reuters.com/article/us-pipeline-blast-alabama-idUSKBN12V2FC (sjekket 26. apr. 2022).

[KV21] A. H. Kierulf og N. Vågsdal, *Prosjektoppgave: Barrierestyring for cybersikkerhet i OT-systemer*, Norges teknisk-naturvitenskapelige universitet, 2021.

[Liu20] Y. Liu, «Safety barriers: Research advances and new thoughts on theory, engineering and management», *Journal of Loss Prevention in the Process Industries*, årg. 67, nr. 104260, sep. 2020.

[LRNT06] M. B. Line, L. Røstad mfl., «Safety vs. security?», i *Proceedings of the 8th International Conference on Probabilistic Safety Assessment and Management*, mai 2006.

[mAS21] mnemonic AS, «2021 SECURITY REPORT», mnemonic AS, tekn. rapp., 2021.

[MB] Stuxnet. adresse: https://www.malwarebytes.com/stuxnet (sjekket 28. apr. 2022).

[McL17] R. W. McLeod, «Human factors in barrier management: Hard truths and challenges», *Process Safety and Environmental Protection*, årg. 110, s. 31–42, 2017.

[MOL+21] T. Myklebust, T. Onshus mfl., «Datakvalitet ved digitalisering i petroleumssektoren», Sintef, tekn. rapp., 2021.

[MS22] Beskyttelse mot phishing, 18. mar. 2022. adresse: https://support.microsoft.com/nb-no/windows/beskyttelse-mot-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44 (sjekket 4. apr. 2022).

[MTa] Corporate Overview. adresse: https://www.mitre.org/about/corporate-overview (sjekket 14. mar. 2022).

[MTb] Enterprise tactics. adresse: https://attack.mitre.org/tactics/enterprise (sjekket 14. mar. 2022).

[MTc] Frequently Asked Questions. adresse: https://attack.mitre.org/resources/faq (sjekket 14. mar. 2022).

[NP21] Arbeidsplasser, 8. jul. 2021. adresse: https://www.norskpetroleum.no/okonomi/arbeidsplasser (sjekket 28. okt. 2021).

[NS21] Cyberangrepsforsøk mot norske virksomheter økte kraftig i april, 20. mai 2021. adresse: https://norsis.no/cyberangrepsforsok-mot-norske-virksomheter-okte-kraftig-i-april (sjekket 4. apr. 2022).

[NSM15] «Sikkerhetsfaglig råd», Nasjonal sikkerhetsmyndighet, 2015.

[NSM19a] «Helhetlig digitalt risikobilde 2019», Nasjonal sikkerhetsmyndighet, tekn. rapp., 2019.

[NSM19b] Råd og anbefalinger om passord, 10. okt. 2019. adresse: https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/rad-og-anbefalinger-om-passord (sjekket 4. apr. 2022).

[NSM20a] Grunnprinsipper for sikkerhetsstyring, 31. aug. 2020. adresse: https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-sikkerhetsstyring/identifisere-og-kartlegge/identifiser-trusler (sjekket 26. apr. 2022).

[NSM20b] «Temarapport Innsiderisiko», Nasjonal sikkerhetsmyndighet, tekn. rapp., 2020.

[NSM21a] «Nasjonalt digitalt risikobilde 2021», Nasjonal sikkerhetsmyndighet, tekn. rapp., 2021.

[NSM21b] Sikkerhetstiltak mot digital utpressing og andre angrep, 30. jun. 2021. adresse: https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/digital-utpressing/sikkerhetstiltak-mot-digital-utpressing-og-andre-angrep (sjekket 4. apr. 2022).

[NSM22] «Risiko 2022», Nasjonal sikkerhetsmyndighet, tekn. rapp., 2022.

[NTB19] Ikke la deg lure: -Datasnokene blir stadig smartere, 31. mar. 2019. adresse: https://kommunikasjon.ntb.no/pressemelding/ikke-la-deg-lure---datasnokene-blir-stadig-smartere?publisherId=1726411&releaseId=17862438 (sjekket 4. apr. 2022).

[NTNU] Rapportering av mistenkelig e-post. adresse: https://i.ntnu.no/wiki/-/wiki/Norsk/Rapportering+av+mistenkelig+e-post (sjekket 4. apr. 2022).

[NV19a] Phishing, 3. sep. 2019. adresse: https://nettvett.no/phishing (sjekket 26. apr. 2022).

[NV19b] Slik lager du sterke passord, 7. feb. 2019. adresse: https://nettvett.no/passord (sjekket 4. apr. 2022).

[NV20] Håndbok for informasjonssikkerhet, 2. mai 2020. adresse: https://nettvett.no/handbok-for-informasjonssikkerhet (sjekket 4. apr. 2022).

[Nät19] T. H. Nätt, skadevare, 28. nov. 2019. adresse: https://snl.no/skadevare (sjekket 25. mar. 2022).

[PNR+21] I. Progoulakis, N. Nikitakos mfl., «Perspectives on Cyber Security for Offshore Oil and Gas Assets», *Journal of Marine Science and Engineering*, årg. 9, nr. 2, 2021.

[PSA17] «Principles for Barrier Management in the Petroleum Industry, Barrier Memorandum 2017», Petroleum Safety Authority Norway, tekn. rapp., 2017.

[PST20] «Etterretningstrusselen mot norsk petroleumssektor», Politiets Sikkerhetstjeneste, 2020.

[PST21] «Nasjonal trusselvurdering 2021», Politiets Sikkerhetstjeneste, 2021.

[PST22a] «Nasjonal trusselvurdering 2022», Politiets Sikkerhetstjeneste, 2022.

[PST22b] PST vurderer etterretningstrusselen fra Russland i Norge som økt, 18. mar. 2022. adresse: https://www.pst.no/alle-artikler/pressemeldinger/oppdatert-trusselvurdering-pst-ser-en-okt-etterretningstrussel-fra-russland-i-norge (sjekket 27. apr. 2022).

[Rau14] M. Rausand, *Reliability of safety-critical systems : theory and applications*. Wiley, 2014.

[Rob11] C. Robson, *Real World Research*, 3. utg. WILEY, 2011.

[SB21] Statsbudsjettet 2022: Statens inntekter og utgifter, 12. okt. 2021. adresse: https://www.regjeringen.no/no/statsbudsjett/2022/statsbudsjettet-2022-statens-inntekter-og-utgifter/id2873448 (sjekket 22. apr. 2022).

[SF5] Styringsforskriften §5. adresse: https://lovdata.no/dokument/SF/forskrift/2010-04-29-611#KAPITTEL_2.

[SGBC22] R. Shandler, M. L. Gross mfl., «Cyber Terrorism and Public Support for Retaliation – A Multi-Country Survey Experiment», *British Journal of Political Science*, årg. 52, s. 850–868, 2022.

[SH21] A. N. Skytterholm og G. Hotvedt, «Preparedness Exercises for Cyber Attacks Against Industrial Control Systems in the Petroleum Industry», masteroppg., Norges teknisk-naturvitenskapelige universitet, jun. 2021.

[Sil06] D. Silverman, *Interpreting Qualitative Data*, 3. utg. Sage, 2006.

[STA] Standardisering. adresse: https://www.standard.no/standardisering (sjekket 14. mar. 2022).

[Stø19] K. Stølen, *Teknologivitenskap, Forskningsmetode for teknologer*. Universitetsforlaget, 2019.

[TBH+21] O. Tor, L. Bodsberg mfl., «IKT-sikkerhet og uavhengighet», Petroleumstilsynet, tekn. rapp., 2021.

[Tjo20] A. Tjora, *Kvalitative forskningsmetoder i praksis*, 3. utg. Gyldendal, 2020.

[TL21] L. S. Tinnel og U. Lindqvist, «Project 12 Safety Instrumentation Final Report», SRI International, tekn. rapp., 2021.

[TM21] W. Turton og K. Mehrotra, Hackers Breached Colonial Pipeline Using Compromised Password, 4. jun. 2021. adresse: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password (sjekket 27. apr. 2022).

[TN] Lær mer om cybersikkerhet. adresse: https://www.telenor.no/bedrift/sikkerhet/cybersikkerhet (sjekket 5. mai 2022).

[TN21] «Valgene vi tar - Digital sikkerhet 2021», Telenor, tekn. rapp., 2021.

[TWNS07] A. Thuv, R. Windvik mfl., «Sårbarheter i Internett», Forsvarets forskningsinstitutt, tekn. rapp., 2007.

[WF] The Story of Waterfall Security & Unidirectional Gateway Technology. adresse: https://waterfall-security.com/company/about-us (sjekket 27. apr. 2022).

[Woo] R. Wood, Fundamentals of deploying secure industrial networks. adresse: https://www.isa.org/intech-home/2017/november-december/features/three-keys-designing-configuring-secure-networks (sjekket 24. mar. 2022).

[Zur21] R. Zurfluh, OT-security, because it´s all about all of our safety and security, 6. aug. 2021. adresse: https://www.infoguard.ch/en/blog/ot-security-because-its-all-about-all-of-our-safety-and-security (sjekket 21. apr. 2022).

[ØWFR14] S. Øie, A. Wahlstrøm mfl., «Barrier Management in Operation for the Rig Industry; "Good practices"», DNV GL, NSA, tekn. rapp., 2014.

Tillegg

A Angrepsscenarioer

Angrepsscenarioene er hentet fra "Preparedness Exercises for Cyber Attacks Against Industrial Control Systems in the Petroleum Industry" [SH21]. De opprinnelige scenarioene er skrevet på engelsk, men er oversatt til norsk for denne oppgaven.

A.1 Scenario 1: Ransomware

Bakgrunn:
En ansatt mottar en e-post fra det som tilsynelatende er en medarbeider. E-posten inneholder et vedlegg med relevant informasjon. Den ansatte har høyt priviligert tilgang til viktige deler av systemet. Vedlegget blir åpnet og ser legitimt ut.

Beskrivelse av Scenario 1:
Del 1: En kontrollromsoperatør jobber nattskift i offshore-kontrollrommet. Plutselig oppdager operatøren en melding i et av tekstfeltene i alarmlistene. Meldingen krever 20 millioner kroner i løsepenger som skal betales til en gitt Bitcoin-adresse. Når de ansatte i kontrollrommet tar en nærmere titt på systemene deres ser de at alt er kryptert.

Del 2: Etter tre dager kommer angriperne med en ny melding. Meldingen forteller at de har kontroll på hovedgeneratoren til platformen. Hvis løsepengene ikke blir betalt, vil de stoppe generatoren, samt produksjonen inntil de mottar betalingen.

A.2 Scenario 2: Angrep med USB som aktiverer 4G

Beskrivelse av Scenario 2:
Del 1: En kontrollromoperatør oppdager en drastisk endring i trykkmålingen på et av operatørpanelene.

Del 2: Etter seks timer oppdager en tekniker som jobber i telekommunikasjon-utstyrsrommet en ukjent 4G-dongel USB-pinne som er festet til en av svitsjene. Nå viser flere trykkmålinger en drastisk endring.

Del 3: En tekniker som jobber på den spesifikke svitsjen hadde utført en kontroll av svitsjene en uke tidligere, da så alt normalt ut og ingen USB var tilkoblet. Det har ikke vært noen andre enn teknikere eller leverandører på plattformen i løpet av den siste måneden. Det er derfor mistenkelig at USB dongelen ble plugget inn i løpet av den siste uken.

A.3 Scenario 5: IACS innsideangrep

Beskrivelse av Scenario 5:
Del 1: En av de SOC-ansatte oppdager uvanlig nettverkstrafikk i en del av IACS-nettverket. Det virker som informasjon har blitt sendt gjennom porter som ikke vanligvis brukes.

Del 2: Etter å ha lukket portene starter teknikere å undersøke trafikken og oppdager at spyware er ansvarlig for uvanlig trafikk.

Del 3: Etter å sjekke logger ble det oppdaget at de spesifikke portene ble aktivert forrige torsdag kl 03.41. Når man sjekker listen over ansatte som var på jobb den dagen er det grunn til å tro at en ansatt fra et høyrisikoland, som jobber med teknisk vedlikehold av IACS, er ansvarlig. Selskapet er klar over at hjemlandet kan presse innbyggere til å gjøre slike handlinger, noe som øker mistanken.

Del 4: Den ansatte innrømmer å ha installert spywaren og aktivert de spesifikke portene. Den ansatte forsvarer handlingen ved å fortelle ledelsen at familien hans ble truet i hjemlandet.

Tillegg B
Intervjuspørsmål

1. I hvilken grad opplever du at metoden fanger opp ikke-tekniske barrierer?
2. I hvilken grad opplever du at metoden vil bidra til å dekke krav fra ISA/IEC 62443?
3. Opplever du at et ransomware-angrep er et relevant angreps-scenario for petroleumsindustrien?
4. Hva tenker du om bruken av MITRE-rammeverket som en del av metoden?
   - Er du kjent med MITRE-rammeverket?
5. Forstår du alle stegene i metoden?
   - Hvis nei, hva er uklart?
6. Ser du noen åpenbare svakheter/utfordringer med metoden?
   - Hvis ja, har du forslag til løsning?
7. Hva synes du er bra med metoden?
8. Hva mangler for at vår metode skal kunne brukes i praksis?
   - Er den mulig å gjennomføre eller vil det for eksempel kreve for mye ressurser?
9. Har du/dere noen andre kommentarer?

Tillegg C

Ikke-tekniske krav i ISA/IEC 62443-2-1

Beskrivelse	Krav
SPE 1: Organizational security measures	
ORG 1: Security related organization policies	
ORG 1.1: Information security management system (ISMS)	The asset owner shall ensure that, if it has a formal ISMS, the SP of the IACS is coordinated with it.
ORG 1.2: Background checks	The asset owner shall ensure that background checks are performed on all personnel who have access to the IACS, including employees, contractors, subcontractors, consultants and vendors to the extent allowed by applicable law prior to granting them access to the IACS.
ORG 1.3: Security roles and responsibilities	The asset owner shall ensure that security roles and responsibilities are assigned to qualified personnel, including employees, contractors, subcontractors and consultants.
ORG 1.4: Security awareness training	The asset owner shall ensure that all personnel, including employees, contractors, subcontractors, consultants and vendors, who interact with the IACS receive formal cyber security awareness training that is updated on a regular basis.
ORG 1.5: Security responsibilities training	The asset owner shall ensure that all personnel, including employees, contractors, subcontractors, consultants and vendors who interact with the IACS receive formal cybersecurity training that is relevant to their IACS cyber security responsibilities.
ORG 1.6: Supply chain security	The asset owner shall ensure that a formal security supply chain process is in place that specifies requirements for suppliers of products and services that address cyber security risks of the IACS. Each of these suppliers shall enforce this requirement recursively on its suppliers.

ORG 2: Security assessments and reviews	
ORG 2.1: Security risk mitigation	The asset owner shall ensure that IACS cyber security risks are identified, documented and mitigated or otherwise managed.
ORG 2.2: Processes for discovery of security anomalies	The asset owner shall ensure that the organization periodically uses manual or automated processes to discover and address: a) undocumented and unauthorized devices/software connected to or communicating within the IACS, b) undocumented and/or unauthorized network traffic, c) undocumented vulnerabilities in the IACS, and d) other security anomalies and non-conformities.
ORG 2.3: Secure development and support	The asset owner shall ensure that systems and components used in the IACS are developed and supported using formally defined secure development lifecycle processes.
ORG 2.4: SP reviews	The asset owner shall ensure that the SP is viewed to verify that it is being properly applied and to address changes in the organization and its processes, technical changes in the Automation Solution and changes in the threat environment.
ORG 3: Security of physical access	
ORG 3.1: Physical access control	The asset owner shall ensure that physical access to the IACS, including access to facilities, equipment and cabling, is controlled to meet risk targets.
SPE 2: Configuration management	
CM 1: Inventory management of IACS HW/SW components and network communication	
CM 1.1: Asset inventory baseline	The asset owner shall ensure that the current baseline of all devices, hardware components, software components and communications protocols/-ports used in the IACS is verified, documented and maintained to include: a) organizational responsibilities, b) manufacturer, c) model, d) version numbers, e) serial numbers, f) revision/patch levels, and g) history.
CM 1.2: Infrastructure drawings / documentation	The asset owner shall ensure that the current baseline of drawings/documentation showing the physical and logical connectivity of all IACS devices and software components is verified and maintained.
CM 1.3: Configuration settings	The asset owner shall ensure that the configuration settings of all IACS devices and software applications are documented and that their operational compliance with the documented configuration is verified.

CM 1.4: Change control	The asset owner shall ensure that all changes to the current configuration baseline and infrastructure drawings/documentation, including revision and patch levels, are authorized, validated and approved.
SPE 3: Network and communications security	
NET 1: System segregation	
NET 1.1: Segmentation from non-IACS networks	The asset owner shall ensure that segmentation and communications policies for interconnection between IACS and non-IACS networks are defined and enforced.
NET 1.2: Documentation of network segment interconnections	The asset owner shall ensure that a current baseline of all IACS network segment interconnections, the security risks associated with each and their designation as trusted or untrusted are documented and maintained.
NET 1.4: Network autonomy	The asset owner shall ensure that the IACS is able to operate as designed when disconnected from external networks (for example, fail-safe operation, safe shut down, restricted operation and normal operation).
NET 1.5: Network disconnection from external networks	The asset owner shall ensure that the IACS is able to be disconnected from external networks to protect itself from actual or suspected threats.
NET 1.6: Internal network access control	The asset owner shall ensure that security risks associated with communications between internal IACS network segments are mitigated, or otherwise managed.
NET 1.7: Device connections	The asset owner shall ensure that all devices connected to the IACS are identified and authenticated.
NET 2: Secure wireless access	
NET 2.1: Wireless protocols	If wireless communications are authorized for use in the IACS, the asset owner shall ensure that wireless protocols used in the IACS are commonly accepted for use in IACS by the industrial and security communities. They shall be documented, and this documentation maintained to include: a) a current baseline configuration of each, b) data exchanges with other network segments, and c) security capabilities and features employed by each wireless network.
NET 2.3: Wireless properties and addresses	If wireless communications are authorized for use in the IACS, the asset owner shall ensure that wireless networks are configured with properties and network addresses that minimize information useful to attackers.

NET 3: Secure remote access	
NET 3.1: Remote access applications	If remote access is authorized for use in the IACS, the asset owner shall ensure that all remote access applications used in the IACS are commonly accepted by both the industrial and security and communities.
NET 3.2: Remote access connections	If remote access is authorized for use in the IACS, the asset owner shall ensure that all interactive remote access connections are authorized, authenticated, encrypted and documented. Documentation for each connection shall include, but not be limited to: a) its purpose, b) the remote access application to be used, c) encryption and authentication technologies used, d) how the connection will be established (for example, via the Internet through a virtual private network (VPN) through a DMZ) with instructions as necessary, e) the circumstances requiring the connection, f) the length of time the connection needs to be open, including expected inactivity periods, and g) the location and identity of the remote client device, application and user.
SPE 4: Component security	
COMP 1: Devices and media	
COMP 1.2: Dedicated portable media	If portable media is authorized for use in the IACS, the asset owner shall ensure that portable media used within the IACS is dedicated to that use.
COMP 2: Malware protection	
COMP 2.1: Malware free	The asset owner shall ensure that all devices and portable media (if portable media is authorized for use in the IACS) are verified to be free of known malware before being used in the IACS.
COMP 2.3: Malware protection software validation and installation	The asset owner shall ensure that malware protection software and its malware definition files are tested for compatibility with the IACS prior to installation, approved for installation and installed in a timely manner after their release.
COMP 3: Patch management	
COMP 3.1: Security patch authenticity/integrity	The asset owner shall ensure that all installed security patches are verified for authenticity and integrity.
COMP 3.2: Security patch validation and installation	The asset owner shall ensure that security patches applicable to device software are tested for compatibility with the IACS, approved for installation and installed in a timely manner after their release.

COMP 3.3: Security patch status	The asset owner shall ensure that the security patch status of all devices is documented and maintained to be current.
COMP 3.4: Security patching retention of security	The asset owner shall ensure that security patch installation does not cause a reduction in the security of the device.
COMP 3.5: Security patch mitigation	The asset owner shall ensure that applicable security patches that are not installed are assessed for risk, and if the risk is not tolerable, address the risk and document the resolution.
SPE 5: Data	
DATA 1: Protection of data	
DATA 1.1: Data classification	The asset owner shall ensure that all IACS data requiring safeguarding are identified and classified according to their protection requirements.
DATA 1.2: Protection of data	The asset owner shall ensure that all data requiring safeguarding, whether at rest or in motion (electronically or physically), shall be protected from compromise according to their classification.
DATA 1.5: Data retention	The asset owner shall ensure that data retention policies and capabilities support security operations before, during and after a cyber event.
DATA 1.6: Data purging	The asset owner shall ensure that all data requiring safeguarding are purged when the device is decommissioned or otherwise removed from the IACS.
DATA 1.7: Cryptographic mechanisms	The asset owner shall ensure that cryptographic mechanisms used in the IACS shall be commonly accepted by both the industrial and security communities.
DATA 1.8: Key management	If cryptographic mechanisms utilizing keys are approved for use in the IACS, the asset owner shall ensure that the use, protection and enforcement of the lifetime of cryptographic keys follow practices and recommendations commonly accepted by both the industrial and security communities.
DATA 1.9: Public key infrastructure (PKI)	If PKI is approved for use in the IACS, the asset owner shall ensure that the use of PKI follows practices commonly accepted by both the industrial and security communities, and shall ensure that: a) all certificates are validated, b) all certificates are generated by a trusted certificate authority, and c) all access to certificates and the certificate revocation list is controlled.
SPE 6: User Access Control	
USER 1: Identification and authentication	

USER 1.1: User identity assignment	The asset owner shall ensure that a process is employed for assigning IACS-specific identifiers, authenticators and roles to users (human users, software processes and devices).
USER 1.2: User identity removal	The asset owner shall ensure that a process is implemented for removing/-disabling IACS-specific identifiers, authenticators, roles and access rights for human users, software processes and devices that do not or no longer need access.
USER 1.4: Access rights assignment	The asset owner shall ensure that a process is implemented for assigning, reviewing and removing access rights to/from IACS-specific roles and to users.
USER 1.5: Least privilege	The asset owner shall ensure that only IACS users are assigned access rights to the IACS, and they are only granted the access rights that they require to perform their assigned tasks.
USER 1.8: User authentication	The asset owner shall ensure that all human users are identified and authenticated on all IACS interfaces that can be used by human users to access the IACS. This includes, but is not limited to: a) device interactive human user login interfaces, b) application interfaces such as web servers, file transfer protocol (FTP) servers and OPC servers, and c) remote desktop interfaces that provide human users login access to IACS devices over the network.
USER 1.9: Multifactor authentication	If multifactor authentication is approved for use in the IACS, the asset owner shall ensure that multifactor authentication is used by devices that support interactive human user login and that are physically accessible by personnel who are not authorized to login to the IACS.
USER 1.11: Password protection	The asset owner shall ensure that password policies are implemented that increase the degree of difficulty to compromise passwords, including complexity, lifetime and reuse.
USER 1.12: Shared and disclosed/compromised passwords	The asset owner shall ensure that a process is implemented for managing shared and disclosed/compromised passwords.
USER 2: Authorization and access control	
USER 2.2: Administrative rights authorization	The asset owner shall ensure that IACS users who are logged onto the OS with administrative privileges are not able to access control system functions of the IACS.

USER 2.3: Multiple approvals	The asset owner shall ensure that approval by two or more users are required for actions that can result in serious impact to the industrial process, unless failure to perform the action can result in a greater impact to the industrial process.
USER 2.4: Manual elevation of privileges	The asset owner shall ensure that explicit elevation of privileges, including supervisor overrides, are required for all operations that require elevated privileges.
SPE 7: Event and incident management	
EVENT 1: Event and incident management	
EVENT 1.1: Event detection	The asset owner shall ensure that IACS events are detected to support security management activities that include reporting, logging, analysis and response (immediate or delayed).
EVENT 1.2: Event reporting	The asset owner shall ensure that IACS events are reported in a timely manner.
EVENT 1.7: Event analysis	The asset owner shall ensure that security-related events are analyzed to identify and characterize attacks, security compromises and security incidents.
EVENT 1.8: Incident handling and response	The asset owner shall ensure that a process is employed and kept current for evaluating and responding to IACS security incidents.
EVENT 1.9: Vulnerability handling	The asset owner shall ensure that existing and newly identified IACS vulnerabilities are addressed and resolved.
SPE 8: System integrity and availability	
AVAIL 1: System availability and intended functionality	
AVAIL 1.1: Continuity management	The asset owner shall ensure that a site disaster recovery plan (DRP), business continuity plan (BCP) or both, is employed and kept current that includes disaster scenarios, failure handling procedures and processes for maintaining the required level of operational continuity.
AVAIL 1.2: Resource management	The asset owner shall ensure that the IACS is protected from resource/equipment failures due to power disruptions, capacity/processing overloads and hardware failures.
AVAIL 1.3: DoS attacks	The asset owner shall ensure that the IACS is protected from DoS attacks.
AVAIL 2: Backup / restore / archive	

AVAIL 2.3: Backup verification	The asset owner shall ensure that the integrity of backup data is verified at the completion of the backup and periodically after the backup.
AVAIL 2.4: Backup media	The asset owner shall ensure that backup media is handled and stored in a safe and secure manner to ensure its integrity, authenticity and availability when needed.
AVAIL 2.5: Backup restoration	The asset owner shall ensure that the IACS is capable of being restored from a backup to a stable state in a timely manner.

Tabell C.1: Ikke-tekniske krav i ISA/IEC 62443-2-1 [Kob22].

Tillegg D

Tekniske krav i ISA/IEC 62443-2-1

Beskrivelse	**Krav**
SPE 3: Network and communications security	
NET 1: System segregation	
NET 1.3: Network segmentation from safety systems	If the IACS contains a safety system network, the asset owner shall ensure that the safety system is protected from interference by non-safety system networks and their devices.
NET 1.8: Network accessible services	The asset owner shall ensure that network accessible services are protected from unauthorized network access.
NET 1.9: User messaging	The asset owner shall ensure that user-to-user messages transferred on IACS networks are not capable of containing payloads, such as attachments and network links, that can be used to support attacks against the IACS.
NET 1.10: Network time distribution	The asset owner shall ensure that time sources used for the secure distribution and synchronization of time within the IACS are protected from tampering.
NET 2: Secure wireless access	
NET 2.2: Wireless network segmentation	If wireless communications are authorized for use in the IACS, the asset owner shall ensure that access and data transfers within and between wireless networks and with other IACS network segments is controlled.
NET 3: Secure remote access	
NET 3.3: Remote access termination	If remote access is authorized for use in the IACS, the asset owner shall ensure that all interactive remote access connections are terminated after a configured inactivity period.
SPE 4: Component security	
COMP 1: Devices and media	

COMP 1.1: Malware protection	The asset owner shall ensure that devices are hardened prior to use in the IACS to protect their software and hardware features. At a minimum, this includes: a) removing/disabling unnecessary software applications and services (for example, email, office applications and games) and their associated communication access points (for example, TCP/UDP ports), b) enabling interfaces for portable media when authorized for use and disabling them when not authorized for use, c) removing/disabling wireless communications that are not required by the IACS, d) removing/disabling network addresses that are not authorized for use, e) protecting physical and logical access to diagnostic and configuration ports from unauthorized access and use, f) configuring unused ports on network devices (for example, switches and routers) to protect against unauthorized access to the IACS network infrastructure, and g) ensuring maintenance processes maintain the hardened state of the IACS during its lifetime.
COMP 2: Malware protection	
COMP 2.2: Malware protection	The asset owner shall ensure that all devices have malware protection software installed, where feasible, that has been verified to detect and respond to known malware, and that has been tested for compatibility with the device.
SPE 5: Data	
DATA 1: Protection of data	
DATA 1.3: Safety system configuration mode	If safety systems are authorized for use in the IACS, the asset owner shall ensure that safety system configuration updates are only able to be performed when configuration mode is enabled, and configuration mode is only enabled when configuration changes are necessary.
DATA 1.4: Failure-state	The asset owner shall ensure that the IACS is set to a predetermined state if normal operation cannot be maintained as a result of a detected security breach.
SPE 6: User Access Control	
USER 1: Identification and authentication	
USER 1.3: User identity persistence	The asset owner shall ensure that IACS-specific user identifiers, authenticators, roles and their associated access rights that are used to support essential IACS operations, including operator accounts, are configured so they are not disabled automatically.
USER 1.10: Mutual authentication	The asset owner shall ensure that mutual authentication is used for access to all server applications hosted on IACS devices, including web server technology-based servers.

USER 1.13: User login display information	The asset owner shall ensure that login processes display information to the user as part of the login process to assist the user in the detection of fraudulent logins.
USER 1.14: User login failure displays	The asset owner shall ensure that information displayed following a login failure limits the information useful to attackers.
USER 1.15: Consecutive login failures	The asset owner shall ensure that user accounts are denied login access for a specified length of time or until unlocked by an authorized administrator after the configured number of consecutive unsuccessful login attempts have occurred.
USER 1.16: Session integrity	The asset owner shall ensure that sessions are protected from unauthorized access and modification.
USER 1.17: Concurrent sessions	The asset owner shall ensure that the number of concurrent sessions per interface for any given human user, software process or device is configured to a limited number.
USER 1.18: Screen lock	The asset owner shall ensure that user screens, except for operator screens, are locked upon user request or automatically after a configured period of inactivity. Re- authentication shall be required of an authorized user to unlock it.
USER 2: Authorization and access control	
USER 2.1: Authorization	The asset owner shall ensure that assigned access rights are enforced for all users.
SPE 7: Event and incident management	
EVENT 1: Event and incident management	
EVENT 1.3: Event reporting interfaces	The asset owner shall ensure that IACS events are reportable through interfaces commonly accepted by the industrial and security communities
EVENT 1.4: Logging	The asset owner shall ensure that events are written to one or more protected event/audit logs and retained for an adequate time period.
EVENT 1.5: Log entries	The asset owner shall ensure that IACS security-related audit and event log entries contain information adequate to support non-repudiation and time-correlated analysis of events.
EVENT 1.6: Log access	The asset owner shall ensure that event logs are accessible through interfaces commonly accepted by the industrial and security communities.
SPE 8: System integrity and availability	
AVAIL 2: Backup / restore / archive	

AVAIL 2.1: Backup	The asset owner shall ensure that the IACS is backed up at regular intervals to support recovery to a stable state.
AVAIL 2.2: Backup non-interference	The asset owner shall ensure that backup processes do not adversely affect normal operations of the IACS.

Tabell D.1: Tekniske krav i ISA/IEC 62443-2-1 [Kob22].

Alva Herdis Kierulf og Nora Vågsdal

Ikke-tekniske cybersikkerhetsbarrierer for OT-systemer i petroleumsindustrien

NTNU
Norwegian University of
Science and Technology