Universitetet i Stavanger

DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

MASTEROPPGAVE

Studieprogram/spesialisering: Risikostyring – Master i teknologi Spesialisering: Offshore sikkerhet	Vårsemesteret, 2011 Åpen / ~~Konfidensiell~~
Forfatter: Marius Myrestrand	…… (signatur forfatter)
<u>Fagansvarlig:</u> Eirik Bjorheim Abrahamsen (UiS) <u>Veileder(e):</u> Eirik Bjorheim Abrahamsen (UiS) Vebjørn Moen (DNV)	
Tittel på masteroppgaven: IT-risikoanalyse av offshoreinstallasjoner	
Studiepoeng: 30	
Emneord: - Informasjonssikkerhet - Prosesskontrollsystem - IT-risikoanalyse	Sidetall: 71 Stavanger, 15.06.2011

IT-risikoanalyse av offshoreinstallasjoner

Marius Myrestrand

15.06.2011

Forord

Denne oppgaven er resultat av den avsluttende prosjektoppgaven for masterstudiet i risikostyring, spesialisering i offshore sikkerhet ved Universitetet i Stavanger. Oppgaven ble gjennomført våren 2011 i samarbeid med Det Norske Veritas. Tema for oppgaven ble utformet i samarbeid med min veileder Vebjørn Moen i DNV. Etter flere samtaler falt valget på temaet; "IT-risikoanalyse av offshoreinstallasjoner". Et relativt uutforsket fagfelt som falt i smak hos begge parter. Min bakgrunn fra Bachelor i Data og Mastergrad i Risikostyring var et godt utgangspunkt for den tverrfaglige kunnskapen som oppgaven krevde.

Jeg vil gjerne takke veileder Vebjørn Moen (DNV) og faglig ansvarlig Eirik Abrahamsen (UiS) for grundige veiledninger og engasjement i forbindelse med skrivingen.

Sammendrag

Denne oppgaven vil kartlegge hvorvidt det er et behov for bedre risikoanalyser og rutiner ettersom offshoreinstallasjonene på norsk sokkel får stadig økt innføring av digitaliserte styrings- og sikkerhetssystemer. Oppsiden av denne utviklingen er stor, der reserveøkning og produksjonsoptimalisering representerer et potensiale på 250 milliarder norske kroner. Oppgaven har belyst hvilke eksisterende rutiner og krav som er iverksatt for å sørge for sikkerheten til disse systemene. Den har kommet fram til at selv om det finnes styrende dokumenter som anbefaler utførelse av risikoanalyser for IT-systemene, finnes det ingen konsensus i bransjen på hvordan de skal gjennomføres.

Oppgaven har undersøkt hvilke trusler som er med å utgjøre en risiko på offshoreinstallasjoner, og samlet relevante hendelser som er med å bygge opp om argumentasjonen for grundigere analyser. Det identifiseres en mangel på dokumentasjon av uavhengighet mellom systemer, samt en manglende forståelse for hvilke konsekvenser et angrep eller svikt i IT-systemene kan forårsake.

Med utgangspunkt i en tradisjonell risikoanalyse for offshoreinstallasjoner har oppgaven undersøkt hvilke metoder og verktøy som er mest hensiktsmessig å inkludere i en IT-risikoanalyse. Forutsetningene for å analysere tradisjonell risiko er annerledes enn for IT-risiko, der en har en kontinuerlig innføring av ny teknologi og arbeidsrutiner. Det er stor usikkerhet involvert i kartlegging og analysering av IT-risiko, og det er behov for en metode som tar høyde for den usikkerheten gjennom å belyse faktorene som kan produsere avvik mellom prediksjonene og de faktiske konsekvensene av en hendelse.

En økonomisk modell som baserer seg på forventet nytteteori er konstruert for å vise hva som skjer hvis en operatør ikke har mulighet til å vurdere eventuell IT-risiko når de skal investere i sikkerhetstiltak. Denne demonstrerer at vi får en overinvestering i eventuelle sikkerhetstiltak dersom IT ikke betraktes som et alternativ.

Innhold

1 Introduksjon **5**
- 1.1 Bakgrunn . . . 6
- 1.2 Formål . . . 6
- 1.3 Krav . . . 6
- 1.4 Disposisjon . . . 7
- 1.5 Terminologi . . . 7

2 Risikobildet **9**
- 2.1 Trusler . . . 9
  - 2.1.1 Tjenestenekstangrep . . . 10
  - 2.1.2 Inntrengning og kompromittering . . . 11
  - 2.1.3 Ondsinnet programvare . . . 12
  - 2.1.4 Systemsvikt . . . 13
  - 2.1.5 Rutine -og vedlikeholdssvikt . . . 14
- 2.2 Erfaringer . . . 15
  - 2.2.1 Deepwater Horizon . . . 16
  - 2.2.2 Stuxnet . . . 17
  - 2.2.3 Slammer . . . 19
  - 2.2.4 Vitek Boden . . . 19
  - 2.2.5 SINTEF-rapport angående IT-rutiner på norsk sokkel . . . 20

3 Analyse **21**
- 3.1 Hvorfor gjøre en IT-risikoanalyse? . . . 21
- 3.2 Risikodefinisjon . . . 22
- 3.3 Metode . . . 22
- 3.4 Forslag til analysemetode . . . 25
  - 3.4.1 Samle og vurdere data . . . 25
  - 3.4.2 Risikoidentifisering . . . 26
  - 3.4.3 Predikere frekvens og konsekvens . . . 27
  - 3.4.4 Vurdere risiko og usikkerhet . . . 30
  - 3.4.5 Konklusjon og anbefalinger . . . 42
- 3.5 Andre verktøy . . . 42
  - 3.5.1 FMEA . . . 43
  - 3.5.2 Bowtie . . . 43

4 Investering i informasjonssikkerhet **46**
4.1 Alternativkostnad 47
4.2 Mangler petroleumsbransjen incentiv til å utvikle analyser og sikkerhetstiltak? 49
4.3 Verdien av informasjonssikkerhetstiltak 51
4.3.1 Investerer ikke i informasjonssikkerhetstiltak 52
4.3.2 Tar hensyn til alternativ investering i informasjonssikkerhetstiltak 54

5 Drøfting **57**
5.1 Behov for risikoanalyser 57
5.2 Metode 58
5.3 Økonomisk modell 59

6 Konklusjon **61**

Bibliografi **62**

Forkortelser

ALARP - Prinsippet innebærer at risikoen skal reduseres så langt praktisk mulig (As Low As Reasonable Practicable)

BSOD - Blue screen of death

CHAZOP - Computer Hazard and Operability studies

DDoS - Distribuert tjenestenektangrep (Distributed denial of service)

DP - Dynamisk Posisjonering

FMEA - Failure Mode and Effect Analysis

HAZOP - Hazard and Operability studies

HSE - Health and Safety Executive

IMCA - International Marine Contractors Association

IO - Integrerte operasjoner

ISA - Instrumentation, Systems and Automation Society

PLS - Programmerbar logisk styring

PLC - Programmable logic controller

SAS - Safety and automation systems

PCS - Process Control System

Ptil - Petroleumstilsynet

MODU - Mobile offshore drilling unit

NPV - Netto nåverdi

SCADA - Supervisory Controls and Data Acquisition

TCP/IP - Transfer Control Protocol / Internet Protocol

VPN - Virtual Private Nettwork

DMZ - Demilitarized Zone er et fysisk eller logisk subnett som innkapsler og blottlegger en organisasjons eksterne tjenester til et større usikkert nettverk, vanligvis Internett. Formålet med en DMZ er å legge et ekstra lag med sikkerhet til en organisasjons intranett. En ekstern trussel har bare tilgang til utstyr som eksisterer i DMZ.

Kapittel 1

Introduksjon

Knapphet på de store og lett tilgjengelige oljefeltene gjør at petroleumsindustrien i dag formes av en hurtig teknologisk utvikling for å operere på krevende forhold i de store havdypene. Bruken av industrielle automasjons- og kontrollsystemer på offshoreinstallasjoner har eksplodert de siste 10 årene. Paralleller kan trekkes til romfartsindustrien når det gjelder teknologi og de ekstreme arbeidsforhold som det opereres på. Industrielle kontrollsystemer er av vesentlig betydning for sikkerhet, pålitelighet og utførelsen til offshoreoperasjoner. Eksempler på slike systemer er Dynamisk Posisjonering (DP), strømstyring, borekontroll, utblåsningsventil (BOP), kranstyring og ballastsystem. Disse kontrollsystemene på offshoreinstallasjoner består i økende grad av instrumenter som knyttes til IT-systemer via nettverk. Vedlikehold, konfigurasjon og bruk av systemene gjøres via arbeidsstasjoner og bærbare datamaskiner.

Integrerte operasjoner er et konsept som trer frem som den foretrukne måten å operere offshore olje- og gassanlegg. Samarbeid i sanntid mellom on- og offshoreansatte gjør det mye lettere å optimalisere produksjon, og baner vei for nye arbeidsprosesser og teknologi. Hyllevare IT komponenter og Internettilgang er noen av de nye teknologiene som blir tatt i bruk, der "nye" betyr at de ikke har blitt brukt til prosesskontroll tidligere. Integrerte operasjoner gjør det mulig for onshoreansatte å logge inn og utføre operasjoner på prosesskontrollsystemer og sikkerhets og automasjonssystemer som befinner seg offshore. Dette åpner også for en helt ny form for trussel relatert til informasjonssikkerhet.

Norsk petroleumsindustri er svært risikobevisst og det stilles mange krav i form av retningslinjer og grundige analyser for å operere på norsk sokkel. Risikoanalyser, tredjepartstesting, verifisering og klassifisering av strukturer og mekaniske systemer er veletablert praksis i maritim- og offshoreindustrien, men bruken av datastyrte kontrollsystem har enda ikke måtte tåle de samme kravene. Dette er et paradoks hvis en tenker på at et enslig kontrollsystem kan være mer kompleks enn alle mekaniske systemene ombord. Tradisjonelle risikoanalyser tar ikke høyde for risikoen som oppstår når kontrollsystemene bygger på IT-hyllevare og er sårbare for IT angrep og virus. Eksisterende metoder skal vurderes i forhold til det nye risikobildet for en moderne, fjernstyrt plattform.

1.1 Bakgrunn

Risikoanalyser av offshoreinstallasjoner har lenge vært påkrevd på norsk sokkel og er i dag et viktig verktøy for å minimere risikoen forbundet med farer og storulykker. Med undertegnede sin bakgrunn fra både Data og Risikostyring - Offshoresikkerhet var det ønskelig å kombinere fagene og produsere en tverrfaglig masteroppgave. Etter samtaler med Vebjørn Moen fra DNV, Terje Aven (UiS) og Jan Erik Vinnem (UiS), var det åpenbart at det var lite fokus på risiko forbundet med informasjonsteknologi og integrerte operasjoner (IO) i de tradisjonelle offshore-risikoanalysene. Det var heller ikke mulig å oppdrive litteratur eller andre kilder på dette området. Det er et faktum at de nye driftsformene og integreringen av ny teknologi skaper både nye risikomomenter og muligheter for å bli bedre på risikostyring. I en rapport om HMS og IO fra 2007 [1] nevner Petroleumstilsynet (Ptil) at petroleumsvirksomheten i økende grad blir mer kompleks og vil kreve en utvikling av risikoforståelsen, og at mange av risikodriverne som er knyttet til IO i liten grad fanges opp av tradisjonelle risikoanalyser som er brukt i næringen så langt.

1.2 Formål

Formålet med denne oppgaven er gjøre en vurdering på hvilke risikomomenter en offshoreinstallasjon i dag står ovenfor, samt undersøke hvilken risikoanalytisk metode som mest hensiktsmessig kan benyttes. Oppgaven vil med dette teste om det er praktisk gjennomførbart og om det finnes en forretningsmessig verdi i denne typen analyser. Hvor viktig er det med fokus på sikkerhet fra operatørene og leverandørenes side når et IT-system skal prosjekteres og installeres på en offshoreinstallasjon, og hva er grunnen til at IT ikke inngår i de tradisjonelle risikoanalysene? Må vi vente til det skjer en storulykke eller alvorlig hendelse før bransjen reagerer? En bred innføring av informasjonsteknologi og IO forutsetter, i følge Ptil [1], at næringen utvikler metoder og verktøy som er egnet for å styre og overvåke risiko i de nye driftskonseptene. Forhåpentligvis vil denne oppgaven avdekke et behov for denne typen analyser, samt gi et bidrag til den naturlige utviklingen av risikoanalysefaget når det gjelder å inkludere tverrfaglige disipliner etterhvert som teknologien og bransjen utvikler seg.

1.3 Krav

Det finnes per dags dato retningslinjer for operatørene som retter seg mot informasjonssikkerheten på offshoreinstallasjoner. I Norge benyttes retningslinje Nr. 104 - Krav til informasjonssikkerhetsnivå i IKT-baserte prosesskontroll-, sikkerhets- og støttesystemer (2007) [2], som er utformet av OLF, Oljedirektoratet og Petroleumstilsynet. Denne har som mål å forbedre informasjonssikkerheten i petroleumsindustrien og derigjennom forbedre driftssikkerhet og regularitet på norsk sokkel. Tore Langeland fra OLF sier i dialog med undertegnede, at han har inntrykk av at retningslinje 104 brukes av operatørene i drift og i prosjekter. Statoil har kopiert den inn i et internt styrende dokument og Petroleumstilsynet forholder seg til retningslinjen i sine revisjoner. Retningslinje 104, som er den grunnleggende retningslinjen for informasjonssikkerhet, har mottatt

Rosing-prisen av Dataforeningen som banebrytende arbeid innen industrien [3]. I OLF 104 på punkt nummer 2 finner vi følgende:

> *"Risikovurderinger skal gjennomføres for IKT-basert prosesskontroll, sikkerhet, støttesystemer og produksjonsnettverk. Risikovurderinger skal identifisere sannsynlighetene og konsekvensene av brudd på informasjonssikkerheten, tatt i betraktning de sikringstiltak og aktiviteter som har blitt gjennomført for å redusere potensielle risikoer."*

Det er foreløpig opp til hver enkelt operatør hvordan de vil utføre en slik risikovurdering, og det finnes ingen bred enighet om hva som er beste praksis for å analysere risiko forbundet med informasjonssikkerhet. Det er tilstrekkelig at operatøren kan vise til at det blitt gjennomført en slik vurdering.

1.4 Disposisjon

- Kapittel 1 omhandler generell introduksjon til oppgaven, hvilke krav som stilles til bransjen i dag, samt terminologi for de viktigste begrepene.
- Kapittel 2 presenterer dagens risikobilde med tilhørende trusler og aktuelle hendelser som er med å bygge opp om behovet for bedre risikoanalyser.
- Kapittel 3 presenterer forutsetningene som settes til grunn for å gjennomføre en IT-risikoanalyse, samt et forslag til hvordan aktuelle metoder kan benyttes i denne sammenhengen.
- Kapittel 4 forklarer hvilke økonomiske drivkrefter som ligger til grunn for å innføre nye IT-systemer og analyser på en offshoreinstallasjon. Her presenteres også en økonomisk modell som undersøker hvorvidt investeringer i sikkerhetstiltak påvirkes når informasjonssikkerhet kommer inn i bildet.
- Kapittel 5 diskuterer og oppsummerer de øvrige kapitlene
- Kapittel 6 Gir en konklusjon med de viktigste funnene

1.5 Terminologi

Prosesskontrollsystem Det finnes mange forskjellige definisjoner, forkortelser og ord for å beskrive de datastyrte automasjonssystemene i industrien. For å nevne noen:

- SAS: Sikkerhets- og automasjonssystemer (omfatter prosesstyring og sikkerhetssystemer)
- PCS: Process Control Systems (Prosesskontrollsystem er betegnelse på store datasystemer som benyttes for styring og prosesskontroll innenfor mange virksomheter som leverer varer og tjenester, f.eks industrien, kraftproduksjon og distribusjon, olje- og gasssektoren, transportsektoren)
- PLS: Programmerbar logisk styring
- ICS: Industrial control system

- SCADA: Supervisory Control and Data Acquisition Systems (SCADA-system refererer til et system som koordinerer prosesser, og kan bestå av flere PLCer. I praksis det samme som PCS og SAS)

Hvis oppgaven ikke går spesifikt inn på detaljer i PLC eller SCADA, forholder den seg til samlebegrepet *prosesskontrollsystem*

Informasjonssikkerhet IT-sikkerhet, datasikkerhet, og informasjonssikkerhet er alle begreper som blir brukt til å beskrive sikkerheten til et datasystem. Disse begrepene kan brukes for å beskrive sikkerhet i forskjellige nivåer:

- Informasjonssikkerhet: Handler om hvor sikker håndteringen av informasjon er med hensyn på ønsket tilgjengelighet, konfidensialitet, kvalitet og sporbarhet
- IT-sikkerhet: Med IT-sikkerhet menes hvordan informasjonen beskyttes og behandles i selve det tekniske IT-systemet
- Datasikkerhet: Beskyttelse av data og datasystem mot uautorisert tilgang, forandring eller forstyrrelse av databehandlingen. Med dette menes at datamaskinenes interne lagrede data og behandlingen av disse skal skje på en sikker måte.

IT må ses på i en kontekstuel sammenheng, der mennesker og bedriften, sammen med teknikken, har en sentral plass. Informasjonssikkerhet er den mest anvendbare terminologien i de fleste sammenhenger [4], og er det begrepet som benyttes i oppgaven.

Kapittel 2

Risikobildet

De siste årene har prosesskontrollere, Supervisory Controls and Data Acquisition (SCADA) og industrielle produksjonssystemer ombord på offshoreinstallasjoner blitt stadig mer avhengig av kommersiell IT-teknologi som nettverk, LAN/WAN, brannvegger og Microsoft Windows for både kritiske og ikke-kritiske prosessystemer. Bruken av hyllevare programvare, protokoller og operativsystem har resultert i betraktelig mindre isolasjon fra omverdenen for sikkerkritiske SCADA og prosesskontrollnettverk (PCN). Prosesskontrollsystemene er nå utsatt for en rekke nye trusler. Sikkerhetsproblemer fra bedriftsnettverket og Internett kan overføres til SCADA og prosesskontrollnettverket, noe som gir økt risiko for produksjonen og menneskelig sikkerhet [5]. Mennesker rundt hele verden har i dag tilgang til Internett, og i teorien er de da koblet opp mot utallige nettverk som inneholder kritiske funksjoner. Angrep på slike nettverk skjer regelmessig og kan forårsake alvorlige konsekvenser hvis de påvirker PCN eller SCADA systemer [6].

Olje -og gassoperasjoner på den norske kontinentalsokkelen foregår i økende grad ved hjelp av integrerte operasjoner [7]. Integrerte operasjoner er med på å skape nye arbeidsprosesser som resulterer i forbedret og mer effektiv produksjon samt utnyttelse av ressursene. Den nye måten å organisere arbeidet på muliggjør fjernstyring, support og lett tilgang på ekspertise på tvers av fagområder. Introduksjonen av denne teknologien innebærer risiko, med både negativ og positiv innvirkning [8].

Viktigheten med å beskytte disse systemene erkjennes, men det tas per dags dato lite hensyn til IT-systemene når en skal analysere risiko på en offshore plattform. Det eksisterer retningslinjer og standarder som kan tilby god veiledning, men det er også viktig å ta hensyn til hvordan disse skal praktiseres. Målene til en IT-avdeling kan være fundamentalt forskjellige fra de som har ansvaret for prosesskontroller i samme selskap. I IT fokuseres det mye på ytelse og dataintegritet, mens den industrielle verdenen ser på personell- og anleggssikkerhet som det viktigste [5].

2.1 Trusler

I følge sikkerhetsselskapet McAfees rapport fra 2009 “Critical Infrastructure in the Age of Cyber War” [9] er det i dag over 120 land som har, eller utvikler

mulighet for elektronisk krigføring. Det rapporteres at USA, Russland, Frankrike Israel og Kina allerede har supplert sine offensive arsenaler med Internettvåpen i form av store datanettverk kalt botnett og dataormer som kan skade fiendens infrastruktur og økonomi. Norge opprettet den 1.Februar 2009 en organisasjon kalt Forsvarets Informasjonsinfrastruktur (INI) som i dag har 1200 ansatte. INI har ansvaret for å drifte, utvikle og beskytte forsvarets nettverk og IKT-løsninger i inn- og utland [10]. I en årsmelding fra 2010 slår Nasjonal sikkerhetsmyndighet (NSM) fast at datasikkerheten i Norge ikke er god nok. NSM's direktør Kjetil Nilsen kommer med krass kritikk av sprikende regler og mangelfull lederkultur i det norske samfunnet, og retter spesielt fokus mot systemene som kontrollerer viktige prosesser i landets industri og infrastruktur.

> *"Fremveksten av skadelig programvare som angriper prosesskontrollsystemer kan i fremtiden bli en av de største sikkerhetsutfordringene som det moderne samfunnet står overfor."*
>
> *Kjetil Nilsen NSM[11]*

Det stadig økende fokuset på informasjonssikkerhet og IT-Risiko verden rundt indikerer at trusselbildet er i forandring. Krig og terror kan allerede i dag utkjempes uten bombefly, stridsvogner eller soldater. Det kan gjennomføres på Internett, gjennom tunge hackeragrep og skjult cyberspionasje. Er det naivt å tro at oljebransjen ikke vil være utsatt for slike angrep? Et whitepaper fra 2011 som heter "Global Energy Cyberattacks" [12] rapporterer at det er utført flere hemmelige angrep på globale olje- og energiselskaper. Disse angrepene har involvert sosial manipulering, phishing, utnyttelse av sårbarhet i systemet, og bruk av fjernstyrte administratorverktøy for å samle sensitiv informasjon om prosjekter og finansiering av olje- og gassoperasjoner.

SINTEF, som er en uavhengig forskningsorganisasjon i Skandinavia, har dybdeintervjuet en rekke nøkkelpersoner i oljebransjen for å undersøke hvordan det står til på feltet. Intervjuene stadfester at det har vært et økende antall såkalte "sikkerhetshendelser" ved produksjonssystemene de siste årene [13]. Oljeselskapene og leverandørindustrien har gjort mye godt arbeid rundt helse, miljø og sikkerhet offshore, men de har ikke har vært like flinke når det gjelder informasjonssikkerhet. Med dagens satsing på integrerte operasjoner og digitalisering av arbeidsprosessene på offshoreinstallasjoner, oppstår det nye trusler og farer som må identifiseres og synliggjøres. Når nye arbeidsmetoder og teknologi innføres i en så risikobevisst bransje som norsk olje -og gassproduksjon, må analyseverktøyene utvikle seg i samme takt.

De følgende truslene granskes for å se hvilken risiko og konsekvens de utgjør på en offshoreinstallasjon:

-Tjenestenektsangrep
-Inntrengning og kompromittering
-Ondsinnet programvare
-Systemsvikt
-Rutine- og vedlikeholdssvikt

2.1.1 Tjenestenekstangrep

Mediebildet har den siste tiden indikert et økende antall nettangrep på organisasjoner, selskaper og myndigheter i form av hacking og angrep på dataservere.

Enkle verktøy for å lage virus og internettangrep har i dag gjort det mulig for selv "ufaglærte" hackere å kjøre angrep over nettet [14]. Angrepene som har fått mest publisitet den siste tiden har en tendens til å være politisk motiverte, men flere tilfeller av sabotasje og militære operasjoner er også rapportert. Virusselskapet McAfee har gitt ut en rapport som beskriver flere slike hendelser mot internasjonale selskaper og organisasjoner i 2010 [15]. Hendelser blir rapportert gjennom deteksjonssystemer, brannmurer og nettverkslogger, men organisasjoner kan få problemer med å forstå de dataene som oppdages, ikke minst å forstå karakteren og alvorligheten av forskjellige typer hendelser.

Wikileaks er en nettside som publiserer lekkende dokumenter fra styresmakter og andre organisasjoner, og var i 2010 ansvarlig for publisering av sensitiv informasjon om Krigen i Irak. Dette utløste store protestaksjoner [16]. Kort tid etter lekkasjen ble nettstedet offer for distribuert tjenestenektsangrep av nasjonalister i USA. Tilhengere av Wikileaks utførte distribuert tjenestenektsangrep på nettsidene til store selskap som VISA, Paypal og Mastercard etter at de stoppet mulighetene for å gi donasjoner til Wikileaks. Konsekvensene av distribuerte tjenestenektsangrep varierer med motivet til de som angriper. I mange av tilfellene dreier det seg om noen timer med nedetid før nettsidene er operative igjen.

Et distribuert tjenestenektsangrep, eller Distributed Denial of Service (DDoS) kan foregå på følgende måte:

1. Angriperen forbereder seg ved å samle et stort nettverk av datamaskiner i et såkalt botnett som står sentralt i angrepet. Dette er ofte tilfeldige PC-er hjemme hos helt vanlige databrukere. De er fra før hacket og infisert med programmer som lar angriperen ta kontrollen over dem anonymt.

2. Hoveddatamaskinen gir en kommando til botnettet om å sende datapakker til en bestemt mottaker.

3. Det store antallet tunge datapakker overbelaster offerets IT-system. Angrepet ødelegger ikke offerets system, men lammer det i en periode.

Maria Kjærland har skrevet en doktoravhandling [17] som argumenterer mot myten om at hacking bare utføres på bakgrunn av status og utfordringer. Den konkluderer med at motivet for slike angrep ofte er relatert til finansiell eller politisk fortjeneste eller et ønske om å forårsake ødeleggelse. Det at organisasjoner vanligvis benytter hacking for finansiell vinning og ødeleggelse av virksomhetsfunksjoner bygger opp om behovet for en mer integrert informasjonssikkerhet og risikostyring. Imidlertid, må ikke et tjenestenektsangrep være en forsettlig handling utført av individer. Komponentfeil kan også generere mye datatrafikk som systemene ikke takler og bukker under for. Hvis et distribuert tjenestenektsangrep rettes mot et SCADA-system på en offshoreinstallasjon kan konsekvensene bli alvorlige. En test utført av CERN [18] viste at 30% av SCADA-komponentene stoppet opp hvis de ble utsatt for et tjenestenektsangrep.

2.1.2 Inntrengning og kompromittering

Mange leverandører og operatører har en formening om at SCADA-systemer og prosesskontrollsystemer er utradisjonelle og vanskelige for utenforstående å få tak i informasjon om, såkalt sikkerhet gjennom obskuritet. Imidlertid er informasjon om slike systemer ofte lett tilgjengelig på leverandørenes nettsider,

det finnes også ganske detaljerte beskrivelser av referanseprosjekter som leverandørene bruker til markedsføring av sine tjenester. Det antas at informasjon også kan skaffes gjennom insidere, sosial manipulering, phishing, harddisker fra vraket pc-utstyr og andre kreative metoder.

På papiret kan det virke som om prosesskontrollere står for seg selv og er ikke tilkoblet andre nettverk, men realiteten er en annen. Tidligere var det arbeidere som manuelt verifiserte målinger på ventiler og instrumenter. Disse målingene ble så brukt til å ta avgjørelser om justeringer og tilpasninger. Med IO har industrien gjort det enklere å kontrollere tilstanden fra en sentralisert lokasjon ved hjelp av SCADA og PLS. Disse systemene kan være sammenkoblet med bedriftsnettverket ved flere punkt, og som regel er det logiske, ikke fysiske barrierer som hindrer uautorisert tilgang. Med logiske barrierer menes brannvegger, Demilitarized zones (DMZ) og Network adress translator (NAT). Disse logiske barrierene sørger for tilsynelatende god sikkerhet og integrasjon, men isolerte fra omverdenen er de ikke. Datamaskiner som prosesserer informasjon fra oljepumping for å optimere produksjonen, er på kontornettverket. De henter data fra produksjonsnettverket og sender konfigurasjonskommandoer tilbake til produksjonsnettverket. Dermed må de to nettverkene være sammenkoblet på et punkt.

2.1.3 Ondsinnet programvare

Moderne oljeriggsystemer tenderer mot å være mer og mer fjernstyrte og overvåket fra kontrollrom på land, så muligheten for å kompromittere et system fra land er tilstede. Hvis et prosessystem står for seg selv og ikke er koblet til andre systemer, er virusinfisering fra land lite sannsynlig. Imidlertid, om man ikke skulle hatt en direkte link mellom land og styringssystemene på plattformen, finnes det alternative angrepsvektorer, som å plante en USB-minnepinne med ondsinnet programvare på en oljearbeider, infisere leverandørers utstyr og bruk av fjerntilgang, selv for systemer som er frittstående. Det er med andre ord bare snakk om å være kreativ. Det kan også være virus tilstede i den originale programvaren. Virus kan overføres til operatører fra leverandører ved at en leverandør kobler datamaskinen sin til produksjonsnettverket. Basert på diskusjoner med oljeindustrien er dette den vanligste årsaken til virusinfeksjoner på norsk sokkel [13].

Sett i lys av Stuxnet-ormen som angrep Iranske atomkraftverk i 2010 [19], utgjør virus og trojanere en trussel mot offshoreinstallasjoner i dag. Stuxnet er kjent som den første dataormen som spionerer på og omprogrammerer SCADA-systemer. Ormen forårsaket ødeleggelse av 1000 uraniumsentrifuger, og satte bremser på Irans atomprogram. Kapittel 2.2.4 forklarer Stuxnet i større detalj. Det er svært trolig at en orm med tilsvarende kompleksitet og ikke minst produksjonskostnader kan forårsake store konsekvenser på en offshoreinstallasjon i form av produksjonsstans, full nedstengning, evakuering eller tap av liv.

I midten av August 2005, angrep ormen Zotob.E et stort norsk oljeselskap. I løpet av en måned var 157 maskiner på land og offshore infisert med viruset. IT-personell brukte lang tid på å forklare konsekvensene og overbevise operasjonsansvarlige om faren før mottiltak ble satt i gang. Heldigvis resulterte det ikke i en ulykke [20].

SCADA-systemene har andre behov enn tradisjonelle IT-systemer. Mange utfordringer oppstår når disse skal integreres. Tilgjengelighet er ekstremt viktig

for SCADA-systemer, mens integritet og konfidensialitet er viktigere for IT-systemer. SCADA-systemer har vanskelig for å ta i bruk antivirus-program som i tillegg må oppdateres manuelt [13]. For mange SCADA-systemer prioriteres det ikke å rulle ut sikkerhetsoppdateringer, da det blant annet kan være driftsmessige utfordringer ved å oppdatere disse systemene [11]. En del systemer i lukkede produksjonsnett oppdateres gjerne aldri, da man ikke har anledning til å ta ned systemene. Disse vil være utsatt for spesielt høy risiko.

Det har vært en økning i hendelser som inkluderer SCADA-systemer, noen av dem har fått alvorlige konsekvenser på operasjoner offshore. Disse hendelsene og angrepene blir sjelden rapportert [21]. Intervjuer har avslørt at det er en vanlig oppfattelse blant ansatte i Nordsjøen at SCADA-systemene som brukes offshore er skjermet fra offentlige nettverk som Internett [13], mens realiteten er at i de siste 10 årene har disse systemene i økende grad blitt koblet mot Internett og andre nettverk [22] som en naturlig konsekvens av utbredelsen til IO.

Oppgaven med å konstruere et virus eller ormer som kan ta over vitale prosesser på en offshoreinstallasjon, er en avansert prosess. I tilfellet med Stuxnet hevder antivirusselskaper og eksperter at det digitale våpenet ikke kunne blitt konstruert uten medvirkning fra et lands myndigheter [19]. Det krever mye resurser og kunnskap, ikke minst at man har hatt mulighet til å teste ut det man skal gjøre i forkant.

2.1.4 Systemsvikt

I høringer etter Deepwater Horizon-ulykken har det kommet fram at feil i enkelte av systemene på riggen har vært kjent i lengre tid. Feil på software i sikkerhetskritisk utstyr var en kjent problemstilling for mannskapet ombord. I kapittel 2.2.1 står det mer inngående om dette. I mange tilfeller ufarliggjøres denne type systemer med at de er sviktsikre, altså at hvis de feiler så skal de gå til trygg tilstand, for eksempel at en ventil stenges. BOP-en på Deepwater Horizon var såkalt sviktsikker. For flere av systemene, for eksempel; brønnkontroll, DP og kraftforsyning, er sviktsikre systemer en myte [23]: Enten fungerer systemene etter hensikten, eller så oppstår det en kritisk situasjon. De moderne databaserte systemene har gjort det mulig å utføre boring på store havdyp, men de innfører også nye farer. Opplæringen som blir gitt i de nye systemene er gjerne av noen dagers varighet, og deretter med videre praktisk trening om bord på rigg.

En undersøkelse som analyseselskapet Coleman Parkes har gjennomført for IT-selskapet CA Technologies i 2011 [24], viser at norske bedrifter med minst 50 ansatte taper 600.000 arbeidstimer hvert år som følge av nedgang i de ansattes produktivitet når IT-systemene stopper opp. Når de ansatte ikke har tilgang til sine IT-systemer, faller produktiviteten til 58 prosent av den normale. Det kommer også frem at hver ansatt opplever i gjennomsnitt ni timer med nede- og gjenopprettingstid hvert år. CA Technologies mener mye av nedetiden kunne vært unngått med forholdsvis enkle tiltak for å gjøre IT-infrastrukturen mer robust. Et tiltak kan være å identifisere de mest kritiske systemene og dataene. Alt for ofte velger organisasjoner en generisk tilnærming til datasikkerhet, og de samme prinsippene og prosessene blir gjort på alle systemer [24].

Den vanligste fremgangsmåten for å sørge for sikkerheten til et system som inkluderer programvare, er å gjøre programvaren mest mulig pålitelig. Fordelene med å digitalisere prosessene om bord på en rigg er mange, og implementerin-

gen av datamaskiner med spesielle formål vil fortsette å øke drastisk, også i sikkerhetskritiske systemer. En utfordring med utvikling og bruk av de fleste systemene er at designet vanligvis utføres av folk uten ekspertise på det aktuelle området. Ekspertene bestemmer hvordan den skal fungere og spesifiserer informasjonen til en programutvikler, som igjen lager det detaljerte designet. Det ekstra kommunikasjonsleddet mellom ingeniør og programutvikler er kilden til de alvorligste problemene med operasjonell programvare i dag. Nesten alle alvorlige ulykker forbundet med programvarefeil de siste 20 årene kan spores til feilspesifisering, ikke feil i kildekoden [25]. Problemene kan også stamme fra uforutsette systemtilstander og miljøforhold. Et amerikansk F-18 styrtet da en mekanisk feil i flyet førte til at inndata ankom raskere enn forventet, som igjen overbelastet systemet. Et annet F-18 gikk tapt på grunn av at det kom opp i en høyde som ingeniørene hadde ansett som umulig og som programvaren derfor ikke var i stand til å takle [25]. Når programvaren gjør det som utvikleren trodde den skulle gjøre og det ikke er hva oppdragsgiver ønsket, ser vi et klart behov for bedre teknikker og risikoanalyser for å fastslå spesifikasjonskravene, og sørge for at oppdragsgiver får det han trenger.

Det kan virke som om svikt i IT-systemene på Deepwater Horizon ikke ble prioritert og ikke fikk den samme oppmerksomheten og responsen som mekaniske feil. Nå som de mekaniske prosessene i stor grad blir styrt og overvåket av kontrollsystemer, bør fokuset på pålitelighet i styringssystemene få en mye høyere prioritering enn før. Imidlertid bør også anlegg og offshoreinstallasjoner i den grad det er mulig, designes slik at de er sikre selv om systemene svikter.

Historisk sett, har ikke uavhengig testing av datasystemene ombord på rigger vært en del av kommisjoneringsprosessen. Verftet, som burde hatt rollen som systemintegrator, fokuserer vanligvis på mekanisk ferdigstillelse, og overlater programvareintegrering og testing til leverandørene. I tillegg finnes det ikke noen spesifikke regler for klassifisering på testing og verifisering av programvare. Resultatet er at verifisering av programvarefunksjonalitet, feilhåndteringsegenskaper og sikkerhetsbarrierer ikke har fått nok oppmerksomhet i kommisjoneringsprosessen.

2.1.5 Rutine -og vedlikeholdssvikt

Offshoreinstallasjoner har mangfoldige rutiner på behandling av data og kontrollsystemer. Tilgang til sikkerkritiske systemer kan avgrenses i form av sperringer og klareringer. Slike sperrer på datastyrte prosesser kan overstyres ved å få tilgang til rett programvare. Trevor Kletz [26] beskriver et anlegg der var det nødvendig med passord og koder for å få tilgang til et tilsvarende program. De ble oppbevart med lås og nøkler og adgang ble kun gitt til noen få elektrikere og ingeniører. På tross av dette hadde 40 personer tilgang til dem. I dag er det kritisk at slik informasjon ikke kommer i gale hender. Det er viktig med gode rutiner på passord og adgangskontroll på kritiske systemer. Ofte kommer de største truslene fra innsiden. Ansatte med inngående kunnskap om systemer og hvordan de kontrolleres, er noen ganger like farlig som eksterne trusler. I noen tilfeller er det ikke mulig å forandre passord på gamle SCADA-systemer, så tidligere ansatte har fortsatt passord til å aksessere disse enhetene.

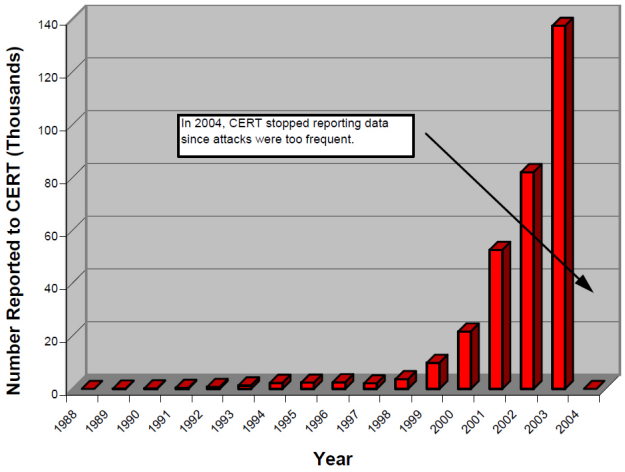
I Australia i 2001 åpnet en misfornøyd ansatt flere kloakksluser med hjelp av fjerntilgang, og forårsaket et kloakkutslipp på millioner av liter [27]. Se kapittel 2.2.6 for mer informasjon om denne hendelsen. Rutinene for oppdatering

og vedlikehold av systemene på et anlegg er kritiske og sårbare. Maskinene som styrer DP ombord en Mobile offshore drilling unit (MODU) kjøres ofte på gamle Windows NT-systemer, og oppdateres ved fysisk tilkobling av lagringsmedier. Det er viktig å kontrollere disse enhetene for virus og lignende før de settes inn. På en ikke-navngitt oljeplattform måtte produksjonen stanses på grunn av dataormen Blaster, som hadde kommet inn i produksjonsnettverket. Årsaken var at noen hadde plugget inn en bærbar datamaskin når de skulle diagnostisere et problem på oljeplattformen [22]. Ormen spredte seg hurtig og den tapte produksjonen forårsaket et tap på millioner av dollar.

Genuine feilgrep kan også utgjøre en stor trussel som et resultat av mangel på riktig opplæring, skjødesløshet eller overseelse. Da er det viktig å sørge for at systemene er kalibrerte og konstruert slik at en tastefeil ikke kan sende enorme mengder med råolje ut i havet.

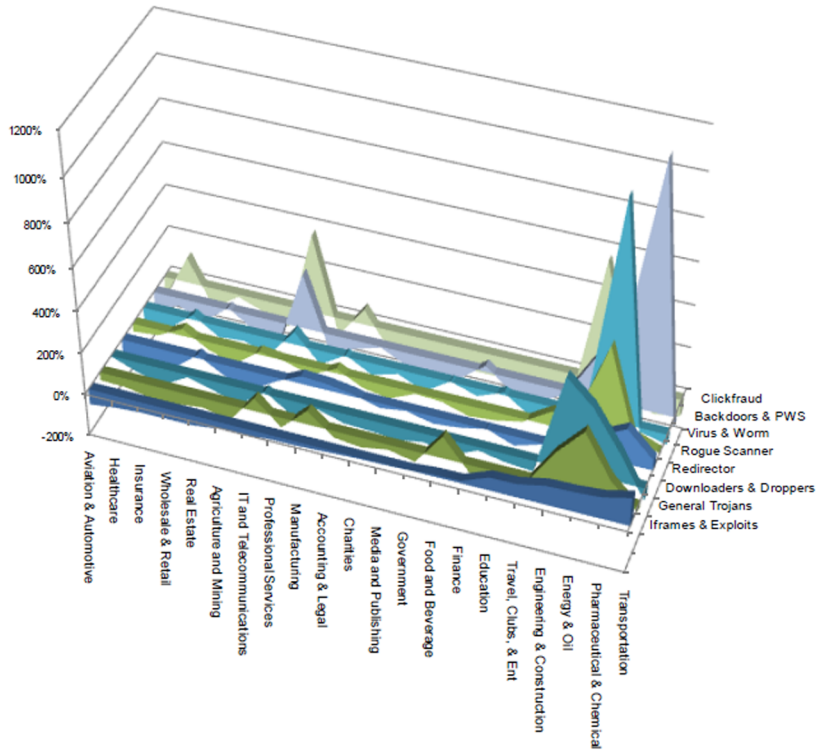
2.2 Erfaringer

Dette kapittelet inneholder beskrivelse av konkrete hendelser hvor informasjonssikkerhet spiller en viktig rolle for utfallet. Det er viktig å dra lærdom av aktuelle hendelser for å vurdere kritikalitet og implementasjon av mottiltak. Dessverre er det svært vanskelig å få tak i informasjon om hendelser angående sikkerhetsbrudd og virusangrep hos operatører. Flere saker har kommet undertegnede for øret, men operatørene ønsker at disse hendelsene forblir konfidensielle og ikke offentliggjort. Organisasjonen CERT som står for Computer Emergency Response Team, er et forsknings og utviklingssenter i USA som har overvåket og etterforsket antall Internettangrep siden 1988. Om de rapporterte tilfellene innbefatter hendelser for kontrollsystemer vites ikke, men siden 2004 har de sluttet med overvåkningen fordi det store antallet automatiserte angrepsverktøy har ført til en eksponentiell økning i antall angrep. Det store antallet rapporterte hendelser ga lite informasjon om omfanget og påvirkningen til angrepene. Figur 2.1 viser en graf over antall angrep, og demonstrerer den dramatiske økningen som har funnet sted de siste 15 årene.



Figur 2.1: Rapporterte angrep på datasystemer frem til 2004 [28]

ScanSafe har gjennomført en analyse [29] som tar for seg spredningen av ondsinnet programvare fordelt på 21 forskjellige typer industrier. Data til analysen er hentet fra de tre første kvartalene i 2008. Som en kan se fra figur 2.2 er energi -og oljebransjen den klart mest utsatte for slike trusler, men det oppsiktsvekkende er at eksponeringen for nye varianter av informasjonssøkende trojanere er fire ganger større enn gjennomsnittet for alle. Denne trenden fortsatte videre gjennom 2009. Energi og olje opplevde en eksponeringsrate som er 356% høyere enn alle andre samlet. De industriene som er mest utsatt for ondsinnet programvare er; energi og olje, farmasøytiske og kjemiske, ingeniør- og byggebransjen. Årsaken til dette nevnes ikke i rapporten, men fellesnevner for disse er at de har en kritisk innvirkning på infrastruktur, og sitter på intellektuell eierskap.



Figur 2.2: Prosentvis varians av skadevare fordelt på industrisektor og ondsinnet programvare [29]

2.2.1 Deepwater Horizon

Femtegenerasjonsriggen fra Transocean hadde en rekke moderne datasystemer, som skulle sikre automatisering og operasjoner. Deepwater Horizon var utstyrt med de mest moderne databaserte sikkerhetssystemer relatert til overvåking av brønn, avstenging av brønn, frakobling av rigg, kraftforsyning, deteksjon og varsling av mannskap. Under ulykken sviktet alle disse systemene helt eller delvis [30]. Granskningen av ulykken på Deepwater Horizon har også avslørt store IT-problemer i forkant av ulykken. Sjefsteknikker ved Deepwater Horizon,

Michael Williams vitnet foran granskningskomitéen om flere feil i systemet som skulle sikre boringen [31]. Boreoperatørenes systemer som overvåker og styrer boreprosessen opplevde datafrys og blåskjermer i flere måneder før ulykken, såkalte Blue Screen of Death (BSOD). Disse hendelsene er i mange tilfeller kortvarige, og i utgangspunktet ikke kritiske i seg selv, men konsekvensene av at dette skjer midt under boreprosessen kan bli betydelige. Boreprosessen stiller store krav til pålitelighet på alt av data som kommer fra brønnen, og bare noen få sekunder uten innsyn i hva som foregår kan skjule et varsel om at det er noe alvorlig galt.

> *"The A-chair is located in the dog house. That is the main operating point for the driller to control all drilling functions. It controls everything from mud pumps to top drive, hydraulics. It controls everything. For three to four months we've had problems with this computer simply locking up. We even coined a term, the blue screen of death, because it would just turn to a blue screen. You would have no data coming through."*
>
> Michael Williams,Transocean chief electronics technician [31]

I høringene kom det frem at de sikkerhetskritiske systemene er ustabile, upålitelige og med ukjente fellesfeil. Mannskapet på riggen skal også ved et tilfelle ha opplevd brønnspark på grunn av datasvikt. Brønnspark er en situasjon som oppstår når formasjonstrykket i en petroleumsbrønn overskrider det hydrostatiske trykket og brønnvæske strømmer ut. Dette er en innledende årsak til utblåsninger. Situasjonen var kjent for mannskapet som hadde meldt inn feilen mange måneder i forveien av hendelsen. Arbeid med å bytte ut komponenter og software på systemet var ikke fullført frem til ulykkesdagen.

Etter sammenslåingen mellom Transocean og Santa Fe International Corporation i 2007 ble vedlikeholdsprogramvaren ombord på Deepwater Horizon byttet ut [31]. Den nye programvaren inneholdt mye feildata og manglende integritet, noe som førte til problemer for mannskapet med å utføre vedlikeholdsarbeid og loggføre arbeidet ombord på riggen. Mannskapet skal også hatt manglende kontroll med utkoblinger av brann og gassvarslingssystemet. Kunne ulykken vært unngått/redusert ved mer fokus på risikoene med systemsvikt?

En ekspertgruppe på risikohåndtering ledet av University of California, Berkeley har konkludert med at omfattende feil og mangler med de sikkerkritiske IT-systemene kan ha bidratt til ulykken [23]. Antakelig ble mange av feilene aldri rapportert fordi de ikke ble forstått. Samhandlingen mellom systemene kan være så komplekse at selv de få som har detaljkunnskap, kan få problemer med å forutse mulige hendelser. Dette fører til mangel på kompetanse til å ta avgjørelser når det oppstår feil.

2.2.2 Stuxnet

Felles for de fleste virus og ormer er at de er ute etter å innhente sensitiv informasjon eller å bruke maskinen til spesifikke formål. Eksempel på det første er å stjele brukernavn og passord, kredittkortinformasjon og sensitiv data. Det andre kan være å kjøre maskinen din inn i ett botnet, for å så bruke datakraft til for eksempel utsending av spam, eller tjenestenektsangrep. Stuxnet er svært annerledes. Formålet er spionasje og sabotasje, og den har siktet rettet

mot kontrollsystemer som brukes i automatisere prosesser, som for eksempel i boreutstyr. Det er to prosesskontrollsystemer Stuxnet angriper: Siemens Simatic S7-300 og S7-400. Disse er 2 av de mest brukte PLC (Programmable logic controller) på verdensbasis, og brukes av flere norske oljeleverandører i følge en artikkel fra PETROmedia [32].

Hva gjør Stuxnet? Stuxnet er en spesialisert orm som angriper Windows-baserte SCADA-systemer. Den sprer seg hovedsakelig via USB-pinner, og ikke via Internett. På den måten kommer ormen seg inn på maskiner som ikke er koblet mot Internett. Symantec har analysert kildekoden til ormen, og har konkludert med at skaperne av Stuxnet har stjålet og benyttet seg av to sertifikater, som tilhører to ulike leverandører. Disse sertifikatene er brukt til å signere deler av skadevaren. En konsekvens av dette er at Windows stoler på skadevaren og lar den legge seg til uten manuell godkjenning når maskinen kompromitteres. Den benytter også fire ukjente sikkerhetshull for å komme seg inn på maskinen og opprette et såkalt rootkit som skjuler at systemet er under kontroll av andre. Når den er inne, krysser den nettverket for å installere seg på andre tilkoblede maskiner. Programmet oppdaterer seg automatisk mot kontrollservere i Danmark og Malaysia, samt med et peer-to-peer system [33]. Ukjente sikkerhetshull kalles også for 0-dags-sårbarheter, som er et hull som ikke er offentlig kjent. Dermed er det ikke opprettet virussignatur og skadevare som utnytter dette hullet er resistent mot alle antivirusløsninger. Å bruke fire slike sikkerhetshull er svært uvanlig, siden den økonomiske verdien til disse hullene er svært høy.

På de fleste maskiner gjør Stuxnet ingen verdens ting. Den bare propagerer videre, enten via nettverket eller så kopierer den seg til USB-pinner hver gang det settes inn imaskinen. For et eksklusivt mindretall kan den ha fatale konsekvenser. Hvis den infiserte maskinen innehar styringsprogrammvare for Siemens sine prosesskontrollsystem, setter ormen i gang med å forandre kildekoden. Disse systemene er mye brukt i industriarbeid, som for eksempel i oljeindustrien og på kjernekraftverk. Ormen har teoretisk sett potensialet til å skape både økonomisk kaos og massiv fysisk ødelegging. Den kan modifisere verdier på prosesser som i verste fall kan føre til eksplosjoner og masseødeleggelse..

Iran Selv om Stuxnet har spredt seg globalt er det kun ett kjent tilfelle der viruset har forårsaket store konsekvenser. Det er en økende aksept for teorien om at Stuxnet i slutten av 2009 var ansvarlig for ødeleggelsen av 1000 uraniumsentrifuger på anlegget Natanz i Iran [19], og at formålet med Stuxnet var nettopp å sabotere Iran sitt atomprogram. For å klare dette må en ha tilgang til detlajerte plategninger og informasjon om anlegget. På et vis fikk noen tak i svært detaljerte beskrivelser av hva som foregikk i Irans atomprogram. Den angripende koden av Stuxnet settes kun i gang når den gjenkjenner en spesifikk konfigurasjon av frekvensomformere som en finner igjen i prosesskontrollerene i Iran. Stuxnet infiserte betydelige mengder med prosesskontrollere rundt omkring i verden, men fordi de ikke tilsvarte konfigurasjonen som vi finner i Iran, ble heldigvis ikke styringsprogrammene på andre anlegg forrandret.

Ny publisering av sikkerhetshull i Siemens SCADA-systemer En sikkerhetsforsker fra NSS Labs som har identifisert flere alvorlige problemer med Siemens prosesskontrollsystemer, har planlagt å publisere resultatene på Black

Hat sikkerhetskonferanse i sommeren 2011 [34] . I mai 2011 trakk den samme forskeren seg fra å publisere de samme detaljene fordi Siemens ikke hadde rukket å utrede feilene [35]. Siemens og myndighetene i USA ble enige med NSS Labs at det var for risikabelt å gå ut med informasjonen før en løsning på problemet var på plass. I følge NSS Labs skal Siemens ha på plass en løsning på problemene før konferansen går av stabelen.

Systemene som forskeren hadde hacket er de samme Siemens-systemene som var målet for Stuxnet, og som er i bruk på kjemiske anlegg, kraftanlegg og ikke minst i oljebransjen. Det er oppdaget hele seks nye sårbarheter som tillater en angriper å ta kontroll på enheten. Imidlertid må en angriper være på samme nettverk som Siemens-systemet, men utilstrekkelig uavhengighet i nettverkene, samt infisering via USB-minnepinner (slik som i Stuxnet sitt tilfelle) gjør det mulig å nå de bestemte systemene.

2.2.3 Slammer

I januar 2003, spredte dataormen SQL Slammer seg rundt på Internett og private nettverk[28]. Den kom seg inn på et nettverk hos atomkraftverket Davis-Besse i USA der det deaktiverte overvåkningssystemet i nesten fem timer. Dette skjedde på tross av at personell på anlegget trodde de var beskyttet av en brannmur. Årsaken til at det kom inn på nettverket var en ubeskyttet sammenkobling mellom anleggs- og kontornettverket. SQL Slammer tok også ned et kritisk SCADA-nettverk i et annet anlegg etter at det forflyttet seg fra kontornettverket til lokalnettverket i kontrollrommet. Et annet anlegg mistet sitt "Frame Relay Network" som ble brukt til kommunikasjon, og noen petrokjemiske anlegg mistet human-machine interfaces (HMIs) og datahistorikk. En nødsentral ble fullstendig frakoblet, fly ble forsinket og kansellert, og minibanker ble deaktivert.

2.2.4 Vitek Boden

En artikkel fra 2008 som heter: "Malicious Control System Cyber Security Attack Case Study" [27] beskriver en hendelse som involverer angrep på SCADA-systemer. Vitek Boden er en mann i 40 årene som jobbet for Hunter Watertech, et Australsk firma som installerte SCADA-basert kloakkutstyr i Queensland, Australia [27]. Boden hadde visstnok et anstrengt forhold til arbeidsgiveren Hunter Watertech, og søkte derfor på en jobb i den samme kommunen han hadde installert et radiobasert SCADA-system for kloakkstyring. Kommunen valgte å ikke ansette han. Boden hevnet seg i April 2000 ved å kjøre rundt med laptop tilknyttet radioutstyr og sende kommandoer til kloakkanlegget som han hadde vært delaktig i å installere. Han fikk tilgang til datamaskinene som kontrollerte kloakksystemet og forandret elektroniske data i pumpestasjonene som førte til funksjonsfeil. Boden greide å slå av 4 alarmer og sørget for et kloakkutslipp på 800.000 liter som fikk konsekvenser for innbyggere og miljøet i Queensland. Dette er et forsettelig målrettet angrep som demonstrerer kritiske, fysiske, administrative og nettverksbaserte sårbarheter med industrielle kontrollsystemer. Imidlertid, er kanskje sårbarheten som følger bruken av leverandører eller andre utenfor organisjasjonen undervurdert som en potensiell angrepskilde. De tekniske aspektene i artikkelen demonstrerer vanskeligheten med å forutse og identifisere et angrep på et kontrollsystem. Når en er blitt gjort oppmerksom på denne

typen angrep kan eierne og operatørene iverksette barrierer for å beskytte systemene. Men en besluttsom, kunnskapsrik motstander som Vitek Boden kunne potensielt omgått barrierene.

2.2.5 SINTEF-rapport angående IT-rutiner på norsk sokkel

Petroleumstilsynet (Ptil) og SINTEF har avdekket en rekke mangler ved de digitale sikkerhetssystemene ved installasjoner på norsk sokkel . Dette kommer frem i en rapport fra 2009 [36] der SINTEF ble hyret inn av Ptil for å utføre datatilsyn ved fire installasjoner tilhørende Statoil, BP og Exxon Mobil. Hovedformålet var å undersøke i hvilken grad Ptil sine krav til uavhengighet er oppfylt, og videre vurdere hvor sikkerhetskritisk eventuelle koblinger og avhengigheter egentlig er. Tilsynet skulle også sjekke om de digitale sikkerhetssystemene fungerer fullstendig uavhengig av andre funksjoner ombord.

Listen over uregelmessigheter er lang. Selskapene kan blant annet ikke dokumentere at automatiseringssystemene tåler belastning i form av nettbaserte angrep, som kan skje med økt bruk av pc-teknologi og datanettverk. Det mangler beredskap og prosedyrer for å håndtere virus og sørge for oppdateringer av Windows-baserte maskiner. Offshoreinstallasjonene bruker sentrale datasystemer på land som vil falle bort ved tap av fiberkommunikasjon til land. Dette kan være arbeidsordre-, vedlikeholds- og hendelsesrapporteringssystem samt tap av datanett, telefon og VHF. Mannskap som er intervjuet gir inntrykk av at de ikke har full oversikt over hvilke systemer som svikter hvis plattformene mister bredbåndsforbindelsen til land.

Hvis en driftsfunksjon svikter og mennesker eller materiell står i fare, skal det være mulig å avbryte operasjonen med et knappetrykk. Tradisjonelt har dette vært mekaniske systemer, der drift og sikkerhet er bygget separat. I dag leveres de digitale drifts- og sikkerhetsløsningene ofte fra samme leverandør, og de kan være bygget på samme programvareplattform. SINTEFs rapport avdekker flere tilfeller med bruk av felles nettverk og at det er forbindelse mellom drifts- og sikkerhetssystemer. Et tenkelig scenario er da at driftsfeil kan smitte over på sikkerhetsmekanismer og sette dem ut av funksjon. Det mangler akseptkriterier for hva som er ”tilstrekkelig uavhengig”, og det mangler metoder for å påvise tilstrekkelig uavhengighet. Dette stemmer overens med funn fra tidligere studier [37] som blant annet viste at selskapene i liten eller ingen grad utfører spesifikke analyser for å påvise at systemene er funksjonelt uavhengige. Det ble også avdekket at brannspjeld og brannpumper er avhengig av prosesskontrollsystemet. Dette må ses på som et avvik fra Ptil sitt generelle krav om uavhengighet mellom styre- og sikkerhetssystemer, skriver Sintef i sin rapport.

Rapporten fra 2009 avdekker mangler i risiko og sårbarhetsanalysene som er utført. Hvis de først gjøres, skjer det på delsystemnivå og ikke på et overordnet nivå. Et symptom er at det ofte er mer fokus på produksjon enn sikkerhet.

Kapittel 3

Analyse

Risikoanalyser for offshoreinstallasjoner startet som et forskningsverktøy i Norge sent på 1970-tallet. I dag er dette en viktig brikke for hvordan vi styrer sikkerhet, helse og miljø i olje- og gassindustrien. Risikoanalyse blir sett på som et redskap for å øke fleksibiliteten med tanke på å imøtekomme en akseptabel sikkerhetsstandard i offshoreoperasjoner. Disse modellene kan være svake på noen områder, men undersøkelsene blir uansett brukt effektivt i søken etter bedre konsepter og optimalisering av design og operasjoner.

Risikoanalyser er en systematisk fremgangsmåte for å beskrive og beregne risiko. Analysene utføres ved kartlegging av uønskede hendelser, og årsaker til, sannsynlighet for, og konsekvenser av disse. Verktøyene for tradisjonell risikoanalyse i offshorebransjen er mange; Hazard and operability studys (HAZOP), kvantitativ og kvalitativ risikoanalyse (QRA), Bow-tie og barriereanalyse for å nevne noen. Men hvordan kan eksisterende metoder håndtere det nye risikobildet som oppstår når vi skal ta hensyn til IT-risiko?

3.1 Hvorfor gjøre en IT-risikoanalyse?

Alle organisasjoner har en begrenset mengde resurser å bruke på sikkerhetstiltak. Ved å utføre en IT-risikoanalyse kan en ta i bruk resultatene til å prioritere de forskjellige systemene basert på mulige konsekvenser. En risikovurdering vil bidra til å identifisere sårbarheter og svakheter som kan påvirke konfidensialitet, integritet og tilgjengeligheten til systemer og data. Ved å avdekke et risikobilde for IT i offshore-sektoren kan en lettere sammenlikne risikoreduserende løsninger allerede i designfasen. Tiltak kan identifiseres og implementeres for å gjøre systemet bedre rustet til å tåle belastningene og truslene. Det er også hensiktsmessig å utføre slike analyser av eksisterende installasjoner, særlig av de som gjennomgår revitaliseringsprosjekter og utstyres med nye IT-systemer.

Oppgaven med å identifisere sårbarheter i et prosesskontrollsystem krever en annen fremgangsmåte enn tradisjonelle IT-systemer. I mange tilfeller kan et IT-system startes på nytt, gjenopprettes, eller byttes ut. Et prosesskontrollsystem kontrollerer en fysisk prosess og har derfor sanntidskonsekvenser assosiert med handlingene den skal utføre. Det er derfor vanskelig å utføre reelle tester på et slikt system når det er tatt i bruk på et anlegg [23]. Gjennomførelsen av en IT-risikoanalyse vil derfor ikke bestå av å utføre tester og sårbarhetsanalyser

på hver enkelt komponent, men heller vurdere hvilke systemer og trusler som er mest kritiske å håndtere, og danne et beslutningsgrunnlag for operatører og leverandører vedrørende implementasjon av eksisterende og nye løsninger.

3.2 Risikodefinisjon

Tradisjonelt sett er risiko definert som:

$$En\ fremtidig\ hendelse \times konsekvens$$

Dette er anvendbart når en har kvalitative datasett som inndata i beregningene. Hvilken definisjon av risiko skal brukes for å beskrive sårbarhet i IT-systemene når det er knyttet stor usikkerhet til både sannsynligheten og konsekvensene? Det er svært vanskelig å knytte sannsynlighet til fremtidige hendelser sett fra et IT-perspektiv. Det finnes svært lite historiske data å beregne fra og i tillegg er teknologien og arbeidsprosessene i stadig utvikling, noe som fører til at historiske data ikke får den samme anvendbarheten. Imidlertid er det mulig å knytte sannsynlighet til levetiden på hardware, men også her eksisterer det stor usikkerhet. Usikkerhet er viktig å ta hensyn til og beskrive, derfor brukes definisjonen om at risiko er relater til [38]:

- A en fremtidig hendelse
- C konsekvensene av hendelsen
- U usikkerhetene assosiert med både hendelsen og konsekvensene
- P sannsynlighet
- K bakgrunnskunnskap

Et relevant eksempel på denne bruken kan være:

A: En viktig server som blir brukt til å overvåke en boreprosess går ned i 24 timer

C: Ingen konsekvenser; redusert produksjon; borestans

U: Vi vet ikke om serveren noen gang vil feile og hvilke konsekvenser som følger.

P: Vi vet at serveren har feilet mange ganger tidligere. Basert på historiske data (K) kan vi knytte en sannsynlighet på 0.007 til at serveren vil gå ned innen de neste 24 timene. Erfaringsmessig har det aldri oppstått borestans som følge av at serveren går ned, men systemeksperter mener det er 3% sjanse for en borestans hvis det skjer en feil med serveren. $P(A|K) = 0.007$ og $P(borestans|A, K) = 0.03$

3.3 Metode

Tradisjonell risikoanalyse er definert i NORSOK-Z013 [39] som en analyse som inkluderer en systematisk identifikasjon og beskrivelse av risiko til personell, miljø, og verdier. ISO definisjonen er "systematisk bruk av informasjon til å identifisere kilder og tilegne risikoverdier". En risikoanalyse må derfor være fokusert på identifisering av risiko og beskrivelse av anvendelig risiko til personell, miljø, og verdier.

Det finnes mange forskjellige metoder for risikohåndtering som har blitt utviklet og tatt i bruk av oljebransjen. Generelt sett kan de klassifiseres ut i fra to faktorer:

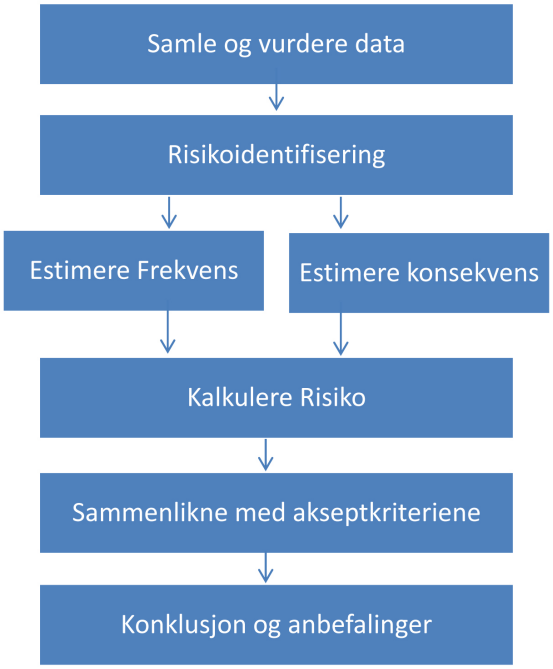
- Hvordan de beskriver den individuelle risikoen; kvalitativt eller kvantitativt.
- Prosessen for risikoidentifikasjon; scenariobasert mot systembasert.

Kvalitativt mot kvantitativt Kvalitativ risikohåndtering er avhengig av vurderingen til erfarne medarbeidere og eksperter for informasjon om sannsynlighet og konsekvensutredelser. Disse sannsynlighetene og konsekvensene blir klassifisert i forskjellige nivåer som høy, medium, og lav i stedet for spesifikke sannsynligheter eller økonomiske påvirkninger. Kvalitativ risikohåndtering foretrekkes når det er mangel på pålitelig informasjon i forbindelse med sannsynligheten til spesifikke trusler og tilhørende konsekvenser.

Kvantitativ risikohåndtering bygger på omfattende datasett som dokumenterer hyppigheten til ulykker basert på eksponering til trusler og sårbarhet. Hvis denne informasjonen er tilgjengelig kan den gi mer presise risikoestimater enn kvalitative risikohåndteringsmetoder. På grunn av at industrielle kontrollsystemer i økende grad blir eksponert mot IT-risiko, er den relative sjeldenheten til slike hendelser og den hurtige utviklingen av disse risikoene en direkte grunn til at det ikke finnes datasett som kan bistå i en slik risikohåndtering. På dette stadiet er kvalitativ risikohåndtering den foretrukne metoden for å evaluere IT-risiko på en offshoreinstallasjon.

Scenariobasert mot systembasert I gjennomføringen av risikohåndtering er det hjelpsomt å fokusere deltakernes tanker enten rundt scenariene der trusler utnytter seg av sårbarheter og påvirker systemene, eller systemene i seg selv. Den scenariobaserte tilnærmingen tenderer mot å ta i bruk erfaring med faktiske hendelser eller nesten-hendelser. Utfordringene med denne tilnærmingen er at den kanskje ikke identifiserer trusler eller sårbarheter som tidligere ikke har vært i søkelyset. Den systembaserte tilnærmingen tenderer mot å ta i bruk kunnskap om en organisasjons systemer, arbeidsmetoder og spesifikke eiendeler som utgjør stor risiko hvis det blir kompromittert. Imidlertid, kan denne tilnærmingen få problemer med å oppdage hvilke typer trusler og sårbarheter som setter disse verdiene i fare, eller scenarioer som involverer mer enn en verdi. I denne oppgaven brukes scenariobasert, men det beste er gjerne en kombinasjon av begge tilnærmingene for å få en mer gjennomgående risikohåndtering og oppdage nye trusler.

Figur 3.1 Viser hvordan en tradisjonell offshore risikoanalyse utføres, inspirert av en konfidensiell analyse utført for en operatør på Norsk sokkel. Denne fremgangsmåten har også mange likheter med den vi finner i NORSOK-Z013 [39]



Figur 3.1: Tradisjonell Risikoanalyse

Samle og vurdere data Samle all relevant data slik at analysen kan bygges på så nøyaktig informasjon som mulig. Relevant data kan være tegninger, dokumenter, rapporter. De samlede data er en viktig faktor for å gjøre seg kjent med plattformen. Det bør også gjennomføres et besøk til den aktuelle installasjonen for å samle informasjon om operasjonelle forhold, bemanningsforhold, hot work aktivitet, værforhold etc.

Risikoidentifisering En systematisk måte å identifisere ulykkeshendelser som kan lede til tap av liv, personskader, miljøskader og økonomisk tap.

Frekvens og Konsekvens Risiko er definert som en funksjon av frekvens og konsekvens. Frekvensen tilbyr informasjon om hvor ofte hendelsen kan forekomme, mens konsekvensene beskriver oppførselen til en initiell hendelse.

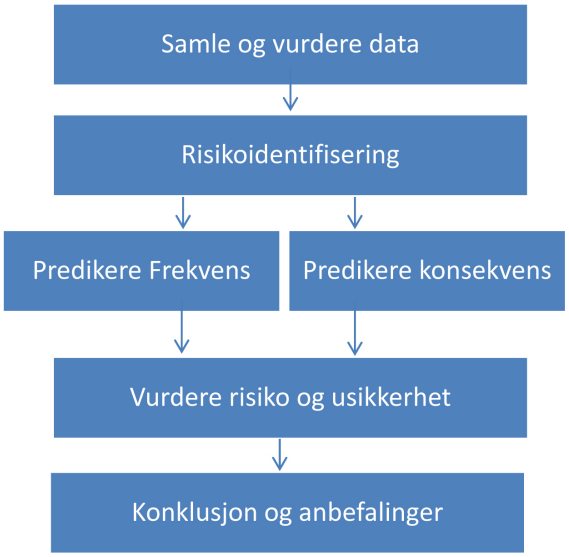
Kalkulere Risiko Basert på frekvens og konsekvens av flere ulykker som hydrokarbonlekkasjer, skipskollisjoner, fallende objekter etc. blir risiko til personell, sikkerhetsfunksjoner og miljø kalkulert for å vise den totale risikoen fra alle hendelsene.

Sammenlikne med akseptkriteriene Operatørene skal definere akseptkriterier for risiko i aktivitetene. Akseptkriteriene skal defineres før en risikoanalyse utføres og brukes som sammenlikningsgrunnlag for analysen.

Konklusjon og anbefalinger Risikoanalysen inkluderer en diskusjon av de kalkulerte resultatene med en ranking av de viktigste risiko-bidragsyterne. Relevante risikoreduserende tiltak blir identifisert. Basert på ALARP-prinsippet (As low as reasonably possible) bør en kostnadseffektivitetsanalyse utføres før en tar bestemmelser om implementering av noen av de foreslåtte tiltakene.

3.4 Forslag til analysemetode

Med utgangspunkt i den tradisjonelle risikoanalysen skal oppgaven presentere en modifisert modell som baserer seg på IT og det gjeldende risikoperspektivet. Figur 3.2 viser den foreslåtte modellen med påfølgende forklaringer og endringer:

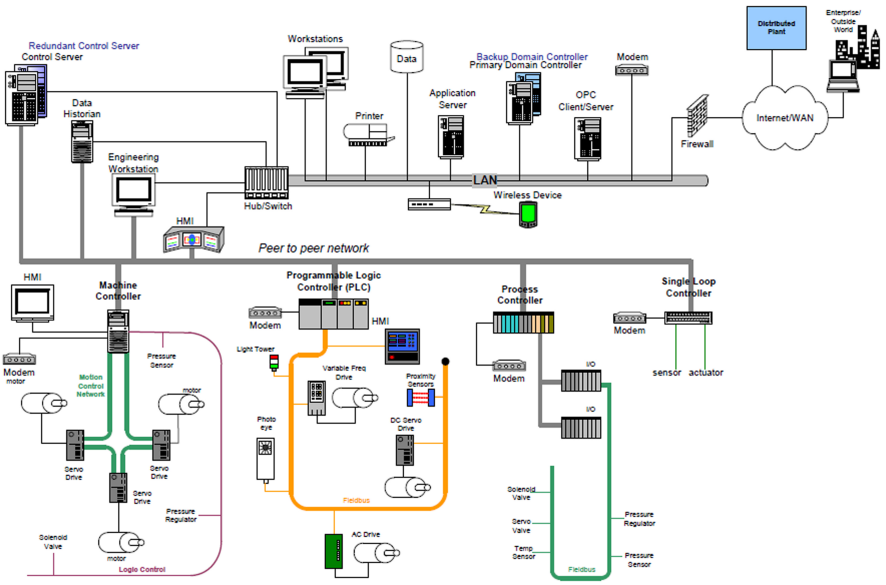


Figur 3.2: IT-Risikoanalyse

3.4.1 Samle og vurdere data

Samle all relevant data slik at analysen kan bygges på så nøyaktig informasjon som mulig. Relevant data kan være tegninger, dokumenter, rapporter, nettverkstopologier og systeminformasjon. De samlede data er en viktig faktor for å gjøre seg kjent med den aktuelle installasjonen, og danner grunnlag for resten av analysen. Det bør også foretas et besøk på den aktuelle installasjonen for å skaffe informasjon om operasjonelle forhold, samt kontrollere at tegninger og topologier stemmer overens med den virkelige verden.

Før en kan begynne å identifisere og prioritere systemene på en offshoreinstallasjon er det viktig at en har en klar forståelse for omfanget og helheten i dem. Et nettverksdiagram er et viktig verktøy for å visualisere nettverkene og svært nyttig for videre risikohåndtering. Det kan være et veldig enkelt blokkdiagram som viser enheter, systemer og grensesnittet, eller et mer detaljert et som vist i figur 3.3. Erfaring viser at sårbarhetsanalyser svært ofte oppdager tilkoblinger som ikke er identifisert i designprosessen, og disse diagrammene bør derfor ikke benyttes som eneste kilde til å vurdere sammenkobling foruten en mer detaljert fysisk validering. I følge ISA (Instrumentation, Systems and Automation Society) [28] er de nyttige for omfanget til risikoanalysen og for å definere soner og kabling.



Figur 3.3: Nettverkstopologi [28]

3.4.2 Risikoidentifisering

HAZOP (Hazard and operability studies) [38] eller CHAZOP (Computer HAZOP) [40] som er spesifikt rettet mot IT-risikoidentifisering er systematiske metoder for å identifisere ulykkeshendelser som kan lede til tap av liv, personskader, miljøskader og økonomisk tap. Et typisk kjennetegn på slike metoder er at de benytter en type strukturert idèmyldring hvor en bruker sjekklister og ledeord som er relatert til problemet som granskes. Risikoidentifiseringen bør være en kreativ prosess der en også prøver å identifisere uvanlige hendelser. En vanlig regel er at det tar 20% av tiden å identifisere 80% av truslene [38]. Dette er de vanligste og tidligere kjente truslene. Den resterende tiden brukes til å identifisere de uvanlige og uforutsette hendelsene. Det er ofte disse hendelsene som kan føre til ulykker med de største konsekvensene. Det du ikke har identifisert kan du heller ikke håndtere, men å innse at det uforutsette er svært relevant, og heller tilrettelegge for at slike uforutsette hendelser i større grad skjer under

kontrollerte omstendigheter kan være verdifullt.

I følge ISA [28] bør kjernen av personer i en slik prosess være sammensatt av tverrfaglig kompetanse som tilføyer kunnskap som en vanligvis ikke finner i en person. Gruppen bør bestå av folk med følgende roller:

- Personer som driver med implementering og support av de aktuelle industrielle kontrollsystemene.
- Operasjonspersoner som er ansvarlige i prosessene som styres av ICS.
- HMS-ansvarlige.
- IT-medarbeidere som kjenner til nettverksdesignet, drift, support og oppdateringsrutiner.
- Sikkerhetsansvarlige som har ansvar for både den fysiske og informasjonssikkerheten.
- Ytterligere ressurser kan være; eksterne konsulenter, juridiske personer, kundesupport og leverandører.

3.4.3 Predikere frekvens og konsekvens

Frekvensen tilbyr informasjon om hvor ofte hendelsen kan forekomme, mens konsekvensene beskriver oppførselen til en initiell hendelse. Disse verdiene kan i et kvantitativt perspektiv finnes ved hjelp av datasett og historiske hendelser. Med et kvalitativt IT-perspektiv må prediksjoner av frekvenser og konsekvenser gjøres av en ekspertgruppe. Disse vurderingene må ikke overdrives, men gjøres på et nøkternt grunnlag. Forskjellige risikostyringssystemer har blitt utviklet for å håndtere en stor variasjon av risiko, og det finnes mange forskjellige måter å skalere og gradere frekvens og konsekvens.

Frekvens De fleste organisasjoner synes det er vanskelig å sette frekvens på hendelser, og det er lite informasjon og tall tilgjengelig for å understøtte slike avgjørelser. Forskjellige meninger om verdiene kan radikalt forandre resultatet av en analyse. Frekvensen kan adresseres med følgende metoder:

- Bruke en verdi på 1 for sannsynlighet og dermed bare fokusere på konsekvenser.
- Bli enige om en rangering av sannsynligheter etter grupperte kategorier
- Forsøke å oppnå mer presisjon ved å se på data fra industrien om angrep og hendelser på IT-systemer.
- Skille sannsynligheten for en hendelse i to faktorer; sannsynligheten for et angrep og sannsynligheten for at det lykkes. Ved å dele opp i disse faktorene er det lettere å se den reelle kilden til trusselen. Ved å bruke denne metoden kan en ta i bruk følgende risikoligning der P er lik sannsynlighet:

$$P_{trussel\_realisert} \times P_{sårbarhet\_utnyttet} = P_{hendelse\_forekommer}$$

$$Risiko = P_{hendelse\_forekommer} \times Konsekvens$$

> Hvis det kommer klart frem at et virus lett kan kompromittere et system og argumentet for at det ikke utgjør noen trussel avhenger av at de håper det ikke skjer, kan benyttelsen av dette skape et nytt bilde av situasjonen

Den tidligere begrunnelsen for valg av kvalitativ metode taler for bruk av en gruppering av frekvensene. En typisk frekvensskala er vist i tabell 3.1. Dette er bare et eksempel, organisasjonen må selv gjøre en vurdering på de faktiske verdiene.

Kategori	Frekvens
3 Høy	En trussel/sårbarhet som trolig forekommer innen 1 år
2 Medium	En trussel /sårbarhet som trolig forekommer innen 10 år
1 Lav	En trussel / sårbarhet som det ikke finnes historisk data på og av den grunn regnes som usansynlig

Tabell 3.1: Eksempel på en frekvensskala

Konsekvens Det er viktig å følge en høy grad av intellektuell ærlighet når en håndterer konsekvensene. I konsekvensutredningen må en identifisere antakelser som kan påvirke risikonivået. Konsekvensvurderingen må nødvendigvis utføres med tanke på organisasjonens interesser og prinsipper. Risikoen assosiert med prosessene om bord en offshoreinstallasjon kan lett knyttes opp mot de industrielle kontrollsystemene som styrer dem, men det er viktig å skille mellom risiko som samfunnet anser som kritisk og det som bedriften anser som kritisk. En sikkerhetsfeil med kontrollsystemene som resulterer i flere dager med nedsatt produksjon, kan ha stor finansiell innvirkning for selskapet. For dette selskapet har dette kontrollsystemet en høy risikoprioritering selv om samfunnet anser dette som lav-risiko fordi det ikke har helse-, sikkerhets- eller miljømessige konsekvenser for allmennheten. Likeledes kan den samme organisjasjonen (på grunn av interne bestemmelser eller eksterne sikkerhetsreguleringer) vurdere en industriell prosess som håndterer farlige materialer som høy-risiko, selv om den ikke påvirker produksjonen.

Konsekvens blir målt i forskjellige vilkår for forskjellige typer risiko. En typisk konsekvensskala er vist i tabell 3.2 Dette illustrerer hvordan IT-risikoanalyse også kan vurderes mot prosessikkerhet og andre deler av organisasjonen [28].

Konsekvens							
	Informasjonssikkerhet			Operasjonell sikkerhet		Virksomhets-risiko	Miljø-sikkerhet
Kategori	Kostnad (millioner NOK)	Juridisk	Omdømme	Personer on-site	Personer off-site	Produksjons-stans	Miljø
3 Høy	> 100	Grov forbrytelse	Tap av omdømme	Dødsfall	Dødsfall eller store samfunns-messige skader	> 7 dager	Langvarig signifikant skade over store områder
2 Medium	> 1	forseelse, mindre alvorlig forbrytelse	Tap av kundetillit	Skader og fravær	Klager eller samfunns-messig innvirkning	> 2 dager	Lokalt utslipp eller skade
1 Lav	< 1	ingen	ingen	Førstehjelp eller mindre skader	ingen klager	< 1 dag	Lite, håndterbart utslipp

Tabell 3.2: Eksempel på konsekvensskala

3.4.4 Vurdere risiko og usikkerhet

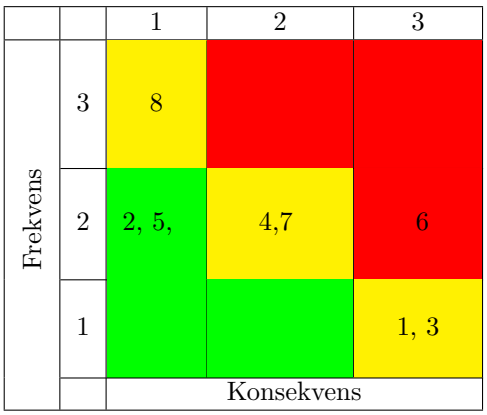
Basert på frekvens, konsekvens og ekspertvurderinger av flere scenarioer som virusinfisering, hardware-feil, software-feil, inntrengning etc. blir risiko til personell, sikkerhetsfunksjoner, miljø og verdier kalkulert for å vise den totale risikoen fra alle hendelsene. Utviklingen til mange hendelser er avhengige av mange faktorer, menneskelig reaksjon, hardware- og softwareversjoner, komponentlevetid og sikkerhetsbarrierer som er vanskelige å modellere skikkelig for alle mulige hendelser. I tabell 3.3 setter vi opp eksempler på hendelser som skal vurderes. Dette er et eksempel på hvordan en slik vurdering kan gjennomføres, og både hendelser og årsaker er forslag som er inspirert av de indentifiserte trusslene i foregående kapitler.

Tabell 3.1 og. 3.2 beskriver klassifiseringen av de ulike hendelsene i henholdsvis frekvens og konsekvens, og er et mål på kritikaliteten til tallene som settes inn i tabell 3.3. Skjæringspunktet til konsekvensene og sannsynlighetsnivåene angir risikonivået. Dette tallet gir en god oversikt for prioriteringen til hver enkelt sårbarhet, men sier lite om usikkerheten knyttet til dem, samt hvorvidt det er en hendelse med høy frekvens og lav konsekvens, eller omvendt.

I denne tabellen knyttes sannsynlighet (P) og konsekvens (C) til hver kritisk hendelse (A) for å gjøre en kvalitativ vurdering

Risiko Nr	Hendelse	Årsak	P	C	Risikonivå
1	Usikker fjerntilgang til systemer på prosessnettverket	Funksjoner som gir ingeniører og leverandører fjerntilgang til systemer har ikke gode nok sikkerhetsbarrierer for å hindre uautoriserte individer fra å få tilgang til prosessnettverket	1	3	3
2	Sensitiv informasjon om IT-systemene på avveie	Tapping av sensitiv data i løpet av forskjellige faser fra engineering, konfigurering, bygging, installering og drift.	2	1	2
3	Uautorisert overstyring av kritisk system	Ondsinnet programvare som kommer inn i prosessnettverket	1	3	3
4	Programvarefeil	Feilspesifisering eller feil i kildekoden til styringsprogrammene i prosesskontrollsystemene	2	2	2
5	Hardwarefeil	Sviktende komponenter i kritiske systemer	2	1	2
6	Datavirus i prosessnettverket	USB minnepinne, laptop fra leverandør, sammenkobling med kontornettverk	2	3	6
7	Tjenestenektsangrep (DDoS)	SCADA -og andre prosessystemer er sårbare mot DoS-angrep, og kan resultere i hindret tilgang til systemene eller forsinke operasjoner og funksjoner	2	2	4
8	Unøyaktig representasjon av utstyr og tilkoblinger	For å sørge for sikkerheten til et prosessnettverk, må dokumentasjonen av utstyr og tilkoblinger være nøyaktig. En unøyaktig representasjon av kontrollsystem og komponenter kan bane vei for uautoriserte tilgangspunkt eller bakdører til prosessnettverket	3	1	3
9					

Tabell 3.3: Risikoevaluering



Figur 3.4: Risikomatrise uten hensyn til usikkerhet

Vi ender da opp med en risikomatrise som i figur 3.4.

Det fremkommer av risikomatrisen i tabell 3.4 at hendelse 6 er den eneste som ender opp i feltet merket med rødt som impliserer at dette er den eneste kritiske risikofaktoren av eksemplene. Dette kan, i og for seg, være en riktig vurdering i forhold til de kjente faktorene og forutsetningene, men hvordan kan vi oppnå et bedre beslutningsgrunnlag der vi også tar hensyn usikkerheten knyttet til både frekvensene og konsekvensene?

Usikkerhetsfaktorer For å vurdere usikkerheten til en hendelse må en se hvilken kunnskap og viten som ikke er tilstede. Usikkerhet som skyldes mangel på nødvendig kunnskap kan reduseres ved å 1) skaffe mer viten i form av nærmere undersøkelser, 2) få frem sentrale avgjørelser eller 3) dele problemet opp i mer håndterbare størrelser [41]. At verden er i forandring knyttes også opp mot noe usikkert. Begrepet betyr i så måte at man ikke har oversikt over et fremtidig hendelsesforløp og eventuelle konsekvenser av dette forløpet.

For å vurdere usikkerhet knyttet til frekvens og konsekvens må det i dette tilfellet utføres en kvalitativ vurdering av faktorene som bidrar til økt usikkerhet. Formålet er å belyse hvilke hendelser og systemer det kan forventes et stort avvik fra de prediksjonene som fremkommer av analysen. Denne vurderingen skal bidra til å plassere hver hendelse i ulike grupperinger. Tabell 3.5 er inspirert av usikkerhetskriterier fra artikkelen; Integrated framework for safety management and uncertainty management [42].

Kategori	Usikkerhet
3 Høy	a) Antakelsene som er gjort for å beskrive (P) og (C) representerer store forenklinger. b) Data er ikke tilgjengelig eller tilstrekkelig. c) Det er ikke enighet blant eksperter.
2 Medium	a) Antakelsene som er gjort for å beskrive (P) og (C) er noe forenklet. b) Noe tilgjengelig data c) Delvis enighet blant eksperter.
1 Lav	a) Antakelsene som er gjort for å beskrive (P) og (C) vurderes som akseptable. b) Mye pålitelig data er tilgjengelig. c) Det er en bred enighet blant eksperter.

Tabell 3.4: Eksempel på usikkerhetsskala

For å kartlegge usikkerhetsfaktorene må både den tilgjengelige og utilgjengelige informasjonen struktureres og beskrives. I tabell 3.6 gjøres en kvalitativ vurdering av grunnlaget for gradering av frekvens og konsekvens. Ut i fra den informasjonen som danner grunnlaget for klassifiseringen kan en knytte en usikkerhetsvurdering fra tabell 3.4 til hver hendelse, som for enkelthets skyld vurderer usikkerhet knyttet til frekvens og konsekvens sett under ett.

- Kolonnen (A) angir fremtidig hendelse og mulig årsak.
- Kolonnen P(A | K) er forventet sannsynlighet for en hendelse A, gitt bakgrunnskunnskap K
- Kolonnen E(C | K) er forventet konsekvens C, gitt bakgrunnskunnskap K
- Kolonnen U er graden av usikkerhet som tildeles denne hendelsen i henhold til tabell 3.5 med bakgrunn i informasjonen som finnes i P(A | K) og E(C | K).

Tabell 3.5: Usikkerhetsevaluering

Nr	(A)	P (A | K)	E(C | K)	(U)
1	*Usikker fjerntilgang til systemer på prosessnettverket* Funksjoner som gir ingeniører og leverandører fjerntilgang til systemer har ikke gode nok sikkerhetsbarrierer for å hindre uautoriserte individer fra å få tilgang til prosessnettverket	Vi vet at lignende episoder har skjedd tidligere (kapittel 2.2.4), dog ikke offentlig tilgjengelige rapporter fra offshorenæringen. Kapittel 2.2.5 impliserer at sikkerhetsbarrierene ikke er godt nok dokumenterte for å hindre slik tilgang. 2.2) Rapport fra Scansafe [43] indikerer at petroleumsnæringen er et populært mål for angrep, men det er ikke historisk datagrunnlag for å hevde at dette er en trussel som forekommer innen 10 år. P = 1	Konsekvensene av en slik handling inneholder store usikkerhet og er avhengig av formål og sikkerhetsbarrierer. Det antas at et vellykket forsøk vil være målrettet og med formål om å sabotere eller forpurre en eller flere prosesser. Imidlertid, kan en anta at sikring av fjerntilgang har høy prioritering i organisasjonen, og ikke undervurderes. Usikkerhet eksisterer rundt; adgangskontroll, begrensning på hvilke kommandoer som kan gjøres via fjerntilgang, deteksjon og den operasjonelle tilstanden til offshoreinstallasjonen. C = 3	3

Nr	(A)	P (A | K)	E(C | K)	(U)
2	*Sensitiv informasjon om IT-systemene på avveie* Tapping av sensitiv data i løpet av forskjellige faser fra engineering, konfigurering, bygging, installering og drift.	Ettersom McAfee rapporten fra 2011 [12] og Scansafe rapporten fra 2009 [43]slår fast at flere oljeselskaper har blitt kompromittert og tappet for sensitiv informasjon de siste årene kan vi predikere en middels frekvens av denne hendelsen. P = 2	Usikkerhet er knyttet til hvilken grad av kritikalitet den tappede informasjonen består av, og til hvilke hensikter den kan brukes til. Konfidensialiteten til dataene kan variere fra personopplysninger til bankinformasjon, informasjon om prosesstyringssystemer og bedriftshemmeligheter. Større usikkerhet knyttet til konsekvensene fører til en større spredning i risikobildet, men i mangel av historiske hendelser settes en lav konsekvens. C = 1	2

Nr	(A)	P (A | K)	E(C | K)	(U)
3	*Uautorisert overstyring av kritisk system* Ondsinnet programvare som kommer inn i prosessnettverket	Det er stor usikkerhet knyttet til fremtidige hendelser, det finnes få dokumenterte eksempler på denne typen trussel utenom Stuxnet (kap 2.2.2) En rapport fra McAfee [9] vitner om opprustning av digital infrastruktur i form av internettvåpen og sikkerhetstiltak i land rundt om i verden. Tilstandsrapporten fra norsk sokkel i kapittel 2.2.5 viser at det mangler dokumentasjon på uavhengighet mellom nettverkene, noe som kan gjøre det lettere for en angriper. Ett dokumentert tilfelle og store utgifter forbundet med utvikling og infisering av en slik programvare taler imidlertid for en lav predikasjon av slike tilfeller. P = 1	Konsekvensene til en slik målrettet orm kan være fatale og forårsake store økonomiske og miljømessige skader. Usikkerhet er knyttet til responstid og hvilke prosessystemer som blir rammet, men Stuxnet er et bevis på at ondsinnet programvare kan forårsake stor ustabilitet og potensielle katastrofer. C = 3	2

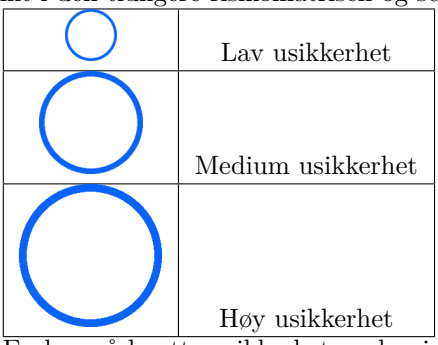
Nr	(A)	P (A | K)	E(C | K)	(U)
4	*Programvarefeil* Feilspesifisering eller feil i kildekoden til styringsprogrammene i prosessystemene	Feilspesifisering regnes som hovedårsaken til denne typen feil, men også uforutsette tilstander kan trigge en feil i styringsprogrammene (kap 2.1.4). Ettersom det er sikkerkritiske funksjoner det er snakk om, bør ikke frekvensen av slike feil oppstå ofte. Deepwater Horizon hadde flere systemfeil i viktige operasjoner, og selv om det ikke kan knyttes mot SCADA eller kontrollsystemene kan en ikke utelate at dette er noe som kan fremkomme hyppigere enn en gang innen 10 år. P = 2	Historisk sett har programvarefeil forårsaket store konsekvenser i mange forskjellige industrier. Et whitepaper fra Deepwater Horizon Study group [23] avslører at datafeil er den største bidragsyteren til ulykker knyttet til DP. En av ulykkene var knyttet til DP på et servicefartøy der en programvarefeil gjorde at båten drev ut av posisjon. Det antas at konsekvensene til feil i kildekode kan skape uheldige situasjoner på en offshore installasjon men ikke nok til å plassere det i den høyeste konsekvensgruppen. C = 2	3

Nr	(A)	P (A | K)	E(C | K)	(U)
5	*Hardwarefeil* Sviktende komponenter i kritiske systemer	Forventet levetid til hardware kan estimeres og utskifting av hardware er en integrert del av vedlikeholdsarbeidet ombord på en plattform. Komponenter og systemer har estimerte verdier som MTTF (mean time to failure) som sier noe om levetiden. Imidlertid er det usikkerhet knyttet til disse tallene fordi utregningen av slike estimater må gjøres ved å ta i bruk et stort antall komponenter og teste de over en periode. Påliteligheten vil alltid avvike noe fra virkeligheten. P = 2	Alt eller deler av et prosesskontrollsystem kan bli satt ut av drift ved en feil, avhengig av feilens natur. Dette kan føre til delvis eller fullstendig tap av kontroll og data. Imidlertid skal sikkerhetskritiske prosesser på en offshoreinstallasjon være redundante og del av et vedlikeholdsprogram, så en hardwarefeil vil sannsynligvis ikke falle inn under de mest kritiske konsekvensene C = 1	1

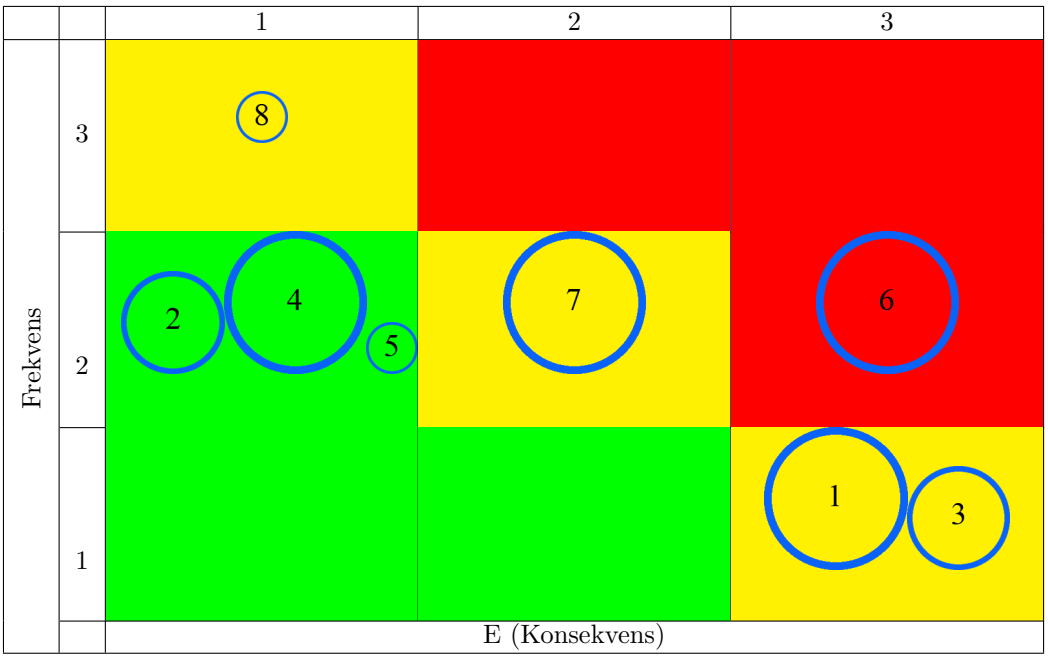
Nr	(A)	P (A | K)	E(C | K)	(U)
6	*Datavirus i prosessnettverket* USB minnepinne, laptop fra leverandør, sammenkobling med kontornettverk	Kommentarer fra fagfolk tyder på at dette er et økende problem også i oljebransjen. Imidlertid blir ikke disse hendelsene offentliggjort og publisert, noe som gjør det svært vanskelig å predikere frekvensen av denne typen hendelse. Stuxnet og den manglende testingen av uavhengighet i prosessnettverk [36], samt tall fra Scansafe [29] som taler for at petroleumsindustrien er et attraktivt mål for datavirus gjør at en hendelse kan sies å være sannsynlig innen 10 år. P = 2	Konsekvensene kan variere fra nedetid og utgifter i forbindelse med å fjerne viruset, til produksjonsstans og tap av sensitive data. Usikkerhet rundt hvilken hensikt viruset har og grad av spredning i nettverket før det blir oppdaget gjør at en må vurdere et bredt konsekvensbilde. Tidligere hendelser i kapittel 2.2 og tilstedeværelsen av prosesskontrollsystemer i mange sikkerhetskritiske operasjoner, samt dårlig dokumentasjon av konsekvensene gjør at konsekvensen settes høyt. C = 3	3

Nr	(A)	P (A | K)	E(C | K)	(U)
7	*Tjenestenektsangrep (DDoS)* SCADA -og andre prosessystemer er sårbare mot DoS-angrep, og kan resultere i hindret tilgang til systemene eller forsinke operasjoner og funksjoner	På tross av at vi har sett en stor økning i tjenestenektsangrep mot organisasjoner [16] og dokumentert dets effekt på prosesstyringssystemer (kap 2.2.1), finnes det få eksempler på slike hendelser i oljebransjen. Imidlertid kan ikke tjenestenektsangrep fraskrives som en risiko. Prosesskontrollsystemene blir i økende grad koblet mot Internett, og dermed øker faren for at vi kan oppleve slike hendelser i nærmeste fremtid. P = 2	Et DDoS angrep kan i noen tilfeller ta ned et SCADA-system (kap 2.2.1) men mest sannsynlig vil det føre til en nedgradering i systemets evne til å utføre prosessene det skal. Selv med bruk av VPN (virtual private nettwork) til å beskytte kommunikasjonen, vil et stort DDoS-angrep spise opp prosesseringskraft og båndbredde som det trenger. C = 2	3
8	*Unøyaktig representasjon av utstyr og tilkoblinger* For å sørge for sikkerheten til et prosessnettverk, må dokumentasjonen av utstyr og tilkoblinger være nøyaktig. En unøyaktig representasjon av kontrollsystem og komponenter kan bane vei for uautoriserte tilgangspunkt eller bakdører til prosessnettverket	Erfaring viser at hver detaljerte sårbarhetsanalyse av offshoreinstallasjoner oppdager koblinger som ikke er identifisert i planleggingsfasen [28]. P = 3	Unøyaktig representasjon kan i verste fall føre til at deler av et nettverk er eksponert og sårbart for uvedkommende. Det er også en viktig informasjonskilde for resten av IT-analysen så store avvik her kan redusere analysens virkningsgrad. Det er imidlertid få dokumenterte hendelser og mye usikkerhet rundt utfallet, som taler for et konservativt syn på konsekvensene C = 1	1

For å illustrere forholdet mellom risikonivå og usikkerhet, tas det utgangspunkt i den tidligere risikomatrisen og supplerer med mål for usikkerhet:



En kan så knytte usikkerhetsevalueringen til risikomatrisen



Figur 3.5: Risikomatrise med tilhørende usikkerhetsklassifisering

I figur 3.5 fremkommer det at risiko nummer 1, 7 og 3 som ligger på det gule feltet inneholder mye usikkerhet, og bør utredes grundigere for risikoen det utgjør på en offshoreinstallasjon. Stor usikkerhet tilsier at en har for lite informasjon til å fastslå risikonivået til trusselen. Risikoanalytikere skiller mellom aleatorisk og epistemisk usikkerhet: epistemisk usikkerhet kan reduseres med videre vitenskapelig forskning, mens aleatorisk usikkerhet vil forbli uklar likegyldig til hvor mye forskning som investeres i emnet [44]. Det bør jobbes med å minske epistemisk usikkerhet relativt til de hendelsene med liten usikkerhet. Der dette ikke er mulig (aleatorisk) må trusselen behandles i henhold til det faktum at risikonivået kan ha større spredning. De faktiske verdiene og prediksjonene i hendelse 7 vil variere, og uforutsette hendelser kan forekomme i større grad enn i for eksempel risiko nummer 8 som til sammenlikning inneholder lite

usikkerhet.

Det finnes flere verktøy for å modellere epistemisk usikkerhet. Det nederlandske veiledningsdokumentet på usikkerhetshåndtering og kommunikasjon [45] nevner følgende: sensitivitetsanalyse, feilpropageringsmetode, Monte Carlo analyse, scenarioanalyse, ekspertvurderinger og PRIMA (pluralistic framework of integrated uncertainty management and risk analysis).

I denne fiktive analysen er det gjort et forsøk på å belyse usikkerhet ved hjelp av bakgrunnskunnskap og ekspertvurderinger. Et problem med å forsøke å prioritere disse risikoene, er kompleksiteten rundt eskalerende hendelser som kan lede til ulykker. Et enkelt system kan tilsynelatende ha tilfredsstillende sikkerhet og redundans, mens det i realiteten kan oppstå svært kritiske situasjoner dersom en eller flere slike hendelser tiltrer på et uheldig tidspunkt. Når usikkerhetene i konsekvensmetodikken kombineres med tilhørende data og antagelser, er det viktig å være klar over at predikert risikonivå kan ha en så vid utstrekning at det er vanskelig eller til og med umulig å oppnå overbevisende konklusjoner om risiko [41]. Dette viser at det er svært vanskelig å utføre en slik vurdering med presisjon. Hvis antallet estimerte hendelser er høyt og kjeden til eskalerende hendelser er tydelig (som med for eksempel bilulykker), er validering relativt enkelt og redelig. Hvis imidlertid håndteringen fokuserer på risiko der årsak-effekt er vanskelig å sjelne, blir det vankeligere å validere resultatene [46]. Imidlertid vil en risikoanalyse med tilstrekkelig fokus på evaluering av usikkerhet være nyttig med tanke på beslutningsgrunnlag og videre støtte til sikkerhetstiltak.

3.4.5 Konklusjon og anbefalinger

Risikoanalysen inkluderer en diskusjon av de kalkulerte resultatene med en rangering av de viktigste risiko-bidragsyterne. Relevante risikoreduserende tiltak blir identifisert, og resultatene kan være til hjelp for å velge mellom alternative løsninger og designprinsipper. Videre undersøkes det hva som kan implementeres for å gjøre et system mindre sårbart og motstandsdyktig. Basert på ALARP-prinsippet bør en kostnadseffektivitetsanalyse utføres før en tar bestemmelser om implementasjon av noen av de foreslåtte tiltakene. Risikohåndtering er ikke en enkeltstående aktivitet, men en kontinuerlig prosess. Dette betyr at risikobildet må overvåkes og vurderes kontinuerlig. Dette tjener som et grunnlag for å vurdere om nye analyser må gjennomføres. I tillegg skal virksomheten løpende kontrollere at sikringstiltakene som er pålagt eller etablert faktisk er iverksatt og fungerer etter sin hensikt. Samtidig bør en overordnet analyse av virksomheten gjennomføres med faste intervaller, for eksempel årlig eller hvert andre år, avhengig av virksomhetens objekter/informasjon og trusselbilde.

3.5 Andre verktøy

I denne seksjonen beskrives to andre verktøy som kan være nyttige i en IT-risikoanalyse.

3.5.1 FMEA

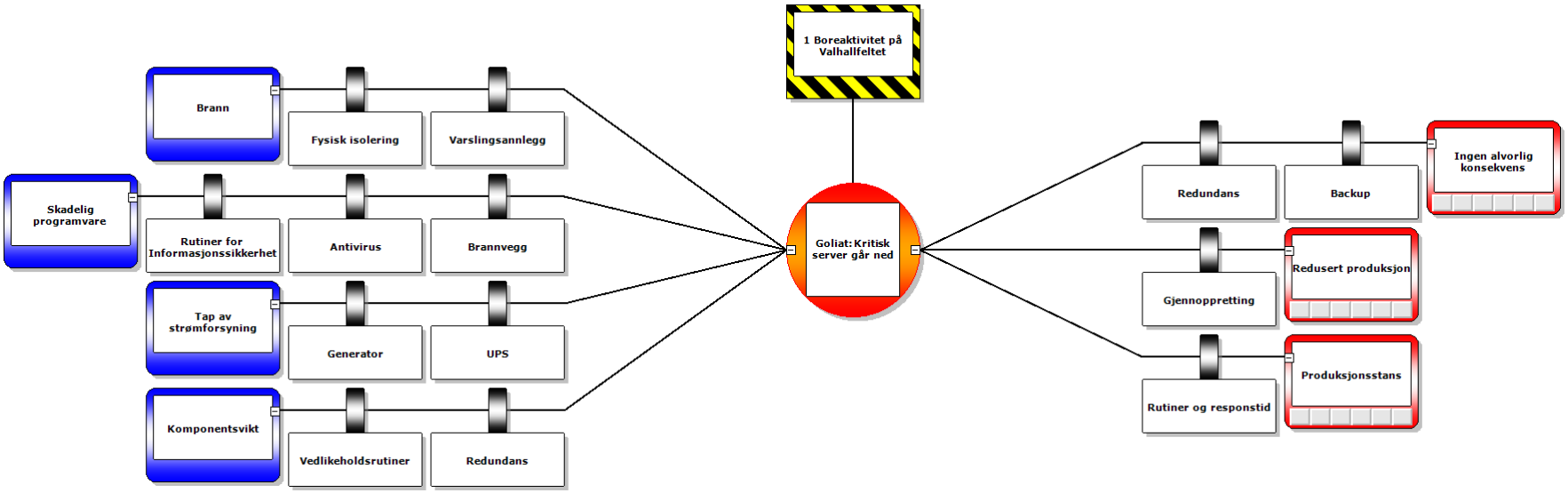
Failure Mode and Effect Analysis (FMEA) er en viktig og veletablert metode for risikoanalyse av sikkerhetskritiske systemer som inkluderer både hardware og software [23]. FMEA er en enkel analyse som avslører mulige feil og forutser effekten det har på hele systemet. Metoden er induktiv, den ser på hver komponent i systemet og undersøker hva som skjer hvis denne komponenten feiler. FMEA representerer en systematisk analyse av komponentene til systemet og identifiserer de viktigste feilmodusene og vurderer hvor viktige de er for ytelsen til systemet. Bare en komponent blir vurdert om gangen og alle andre komponenter blir da regnet som å fungere perfekt. FMEA er derfor ikke egnet til å avsløre kritiske kombinasjoner av feil. FMEA analyser av software-komponenter blir vanligvis utført av leverandørene selv uten en tredjeparts testing og verifisering. Under havpøver for nybygg ligger fokuset på testing av hardware-komponentene og til dels I/O laget til datasystemene. Programvarens funksjonalitet blir bare overfladisk testet på grunn av mangel på tilstrekkelige testverktøy.

3.5.2 Bowtie

Bowtie-diagram er et strukturert og svært utbredt verktøy for risikoanalyser i alle typer industri og selskaper. Det er vanlig å bruke i scenarioer der kvantifisering ikke er mulig eller ønskelig. Bowtie-diagrammet er en grafisk representasjon av risikohåndteringsprosessen som lett kan forstås av utenforstående individer. Diagrammet består av et feiltre på venstre siden (årsak) og et hendelsestre på den andre siden (konsekvens), med en risiko i midten som binder dem sammen slik at det minner om en sløyfe (bowtie). Et bowtie diagram kan konstrueres ved å definere:

- Hendelsen som skal forhindres.
- Trusler som kan forårsake hendelsen.
- Konsekvensene som hendelsen medfører.
- Barrierer som forhindrer hendelsen.
- Barrierer som minimerer konsekvensene.

Bowtie-diagram fungerer utmerket til å representere IT-hendelser. Dette er vist i eksempelet figur 3.6 hvor vi fokuserer på hendelsen; “kritisk server går ned”.



Figur 3.6: Bowtie - Kritisk server går ned

Bruksområder

Identifisere risiko Bowtie diagram er effektive til å systematisk identifisere farer, håndtere kontroll og fremme diskusjon. Det demonstrerer hvilke kontrollere som er på plass for å redusere risiko til ALARP og dokumenterer HAZOP eller CHAZOP resultatene.

Opprettholde oversikt av risikofaktorer Bowtie diagram tilbyr en enkel, lettfattelig og oppdaterbar representasjon av farene involvert i en organisasjons aktiviteter og tiltakene som er igangsatt for å kontrollere risiko.

Organisatoriske forbedringer Det er mulig å bruke bowtie-diagrammer i samsvar med andre teknikker for å identifisere svake ledd. Det sørger for ansvarsfordeling og eierskap til kritiske barrierer og passer på at de ikke overses.

Kapittel 4

Investering i informasjonssikkerhet

Gjennomførelsen av en IT-risikoanalyse vil bestå av å vurdere hvilke systemer og trusler som er mest kritiske å håndtere, og herav danne et beslutningsgrunnlag for operatører og leverandører vedrørende investering i sikkerhetstiltak. I dette kapitelet drøftes det hvorvidt en kan måle nytten av informasjonssikkerhetstiltak i kroner og ører, og om det lar seg forsvare å bruke store summer på analyser og tiltak for å hindre en nedprioritert men komplisert og voksende trussel.

Informasjonssikkerhet har lenge blitt betraktet som en ren utgift. Det lager hindringer og det skaper friksjon ved å komplisere kommunikasjonen mellom to parter, transaksjoner eller oppgaver. De beste informasjonssikkerhetssystemer streber etter å oppfylle 2 krav : uunngåelig og ulastelig. Med uunngåelig menes det faktum at et sikkerhetssystem som en kan omgå ikke er et særlig bra sikkerhetssystem. Med ulastelig menes minimering av de operasjonelle byrdene som sikkerhet kan påtvinge. Hvis du trenger mange forskjellige ID-kort, passord og USB-nøkler som må skiftes ofte for å få gjort jobben din, så kan sikkerhet være en byrde. Ute på plattformene må mekanikere enkelte ganger huske syvåtte passord [47]. Disse passordene skal sikre IT-systemene, men mekanikerne skjønner ikke hvorfor. De føler at alle passordene stjeler tid og hindrer dem i å gjøre jobben sin. Manglende informasjon og kulturforskjeller fører til gnisninger. I digital sikkerhet og i et samfunn generelt, er det fordelaktig å unngå nye byrder.

Hvis vi først skal se på datasikkerhet som en byrde med et økonomisk perspektiv, så må målet være å balansere kostnadene. I dette tilfellet må en gjøre aveiing mellom kostnaden til sikkerhet, som er byrden en må ta i fraværet av en uønsket hendelse, og kostnaden ved å rydde opp i feilene som skjer hvis en ikke velger å bære byrden.

Når det diskuteres hvor mye en ønsker å bruke på informasjonssikkerhet, vil en del av diskusjonen være "Hvor mye bruker alle andre?" Det spørsmålet tar lite tekniske hensyn, men hvis en ligger i feil ende av den fordelingen kan det stilles spørsmål til hvorfor. Hvis det brukes mye mindre penger, så kan en uønsket hendelse ende opp med å blottlegge det faktum at du ligger langt under kostnadene som de andre firmaene betaler. Har du brukt X-antall millioner på informasjonssikkerhet på ett år, og kan slå i bordet med at du ikke har

hatt en eneste hendelse, vil ledelsen trolig si at de har brukt for mye penger. Dette er ikke en feil tankegang. En nulltoleranse for feil og sårbarheter vil trolig føre til en overinvestering i sikkerhetstiltak. Derfor er det ofte bedre å se på datasikkerhet som en investering enn en byrde. Ingen ser på en investering og forventer perfeksjon. De håper at utleggene vil betale seg.

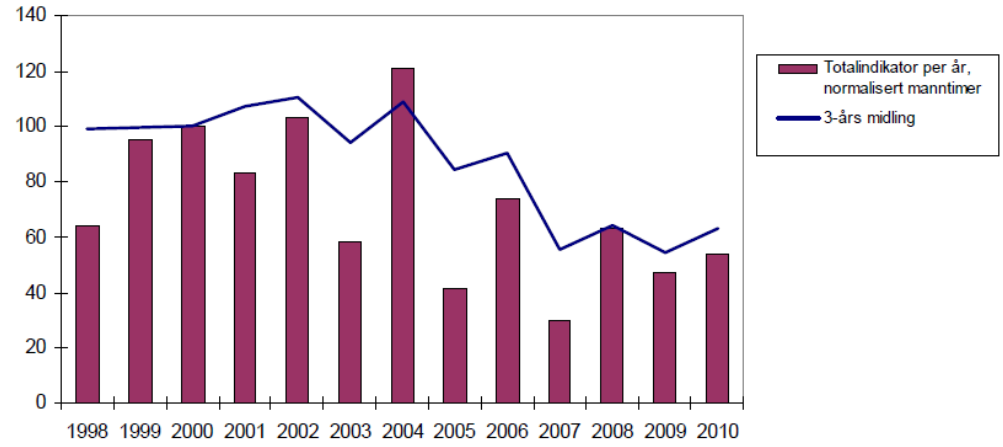
Investeringskostnadene for sikringstiltak må veies mot det potensielle tapet som et sikkerhetsbrudd kan forårsake. Samtidig må en slik tilnærming brukes med fornuft. I visse tilfeller kan det være vanskelig å kvantifisere kostnadene ved et sikkerhetsbrudd, og for objekter som er av høy betydning bør man ofte investere mer for sikkerheten. I mange tilfeller vil det også være vanskeligere å fastsette nytte i kroner og øre ved de tiltak man ønsker å implementere. En slik vurdering vil likevel ofte være etterspurt i forbindelse med å forsvare de aktuelle investeringsutgiftene. En må være klar over at de færreste investeringer i forebyggende sikkerhet genererer nytte i form av inntekter.

4.1 Alternativkostnad

Alternativkostnad betegner som oftest kostnaden som kommer om man lar være å gjøre en investering. Skal man bygge en bro, kan alternativkostnaden være hva det koster å drive fergen videre. Om vi ikke kjøper ny bil, er alternativkostnaden hva den gamle vil koste oss i tiden frem til neste gang vi vurderer spørsmålet. Den egentlige kostnaden ved en investering er kostnadsøkningen i forhold til alternativkostnaden.

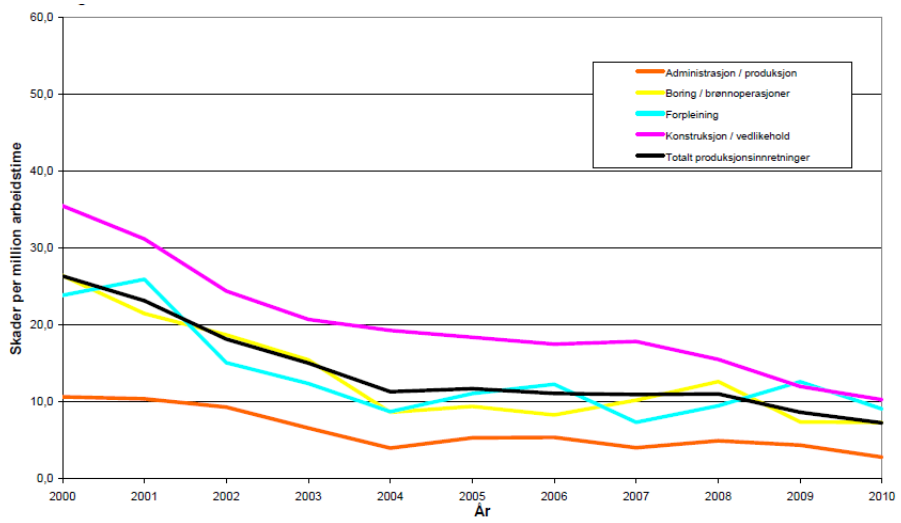
Før man innfører nye analyser og sikkerhetstiltak ønsker man å undersøke hvilken verdi en slik investering kan tilføye. Vil det gi bedre alternativkostnad å investere i andre sikkerhetstiltak som historisk og statistisk sett er mer målbare? Ta for eksempel prosesslekkasje og skipskollisjon som er antatt å være en av de mest kritiske hendelsene for en offshoreinstallasjon, og er av de større bidragsyterne til storulykker. Vil det være mer hensiktsmessig å investere midlene i tradisjonelle risikoreduserende tiltak her enn for IT-relatert risiko? Navigering, dynamisk posisjonering og informasjon om værforhold er dataassisterte prosesser som bør vurderes som en risiko og årsak til skipskollisjon. Petroleumsindustrien er fortsatt den energisektor med høyest antall ulykker og storulykker på verdensplan, og nettopp derfor kan det være vanskelig å rettferdiggjøre frigjøring av mer midler til å håndtere IT-risiko. Imidlertid ser vi en klar nedgang i antall storulykker på norsk sokkel i følge en rapport fra Ptil [48], noe som illustreres i figur 4.1.

Den samme rapporten stadfester også at personskadefrekvensen per million arbeidstimer de siste 11 årene har gått ned. Figur 4.2 viser at Fra 2000 til 2004 har det vært en klar og jevnt nedgang fra 26,4 til 11,3 per million arbeidstimer i 2004. Fra 2004 til 2008 har den samlede skadefrekvensen stort sett vært uforandret rundt 11 skader per million arbeidstimer. I 2009 fikk vi en nedgang fra 11 til 8,6 skader per million arbeidstimer. Fallet i antall personskader har flatet ut de siste årene. Har vi nådd et punkt der vi har lite forbedringspotensiale i tradisjonell risiko samtidig som antallet IT-hendelser øker? Statistikken underbygger at det finnes en grense for effektiviteten av tradisjonelle sikkerhetstiltak. I tillegg er tendensen at stadig flere jobber blir flyttet til land fordi mange av instrumentene som tidligere ble operert manuelt styres nå av prosesskontrollsystemer og stadig flere av de kritiske arbeidsoppgavene blir digitalisert. Dette



Figur 4.1: Totalindikator for storulykker per år, normalisert mot arbeidstimer [48]

vil sansynligvis føre til at personskadefrekvensen synker ytterligere. Hvis man velger å bruke 100 millioner på nye sikkerhetstiltak for å minske konsekvensene ved fremtidige kollisjoner, vil trolig deler av de pengene være fornuftige å bruke på å forbedre sikkerheten til IT-systemet som posisjonerer riggen.



Figur 4.2: Personskader per million arbeidstimer, produksjonsinnretninger [48]

4.2 Mangler petroleumsbransjen incentiv til å utvikle analyser og sikkerhetstiltak?

På tross av oppgavens fokus på de mangelfulle IT-rutinene i oljeindustrien, er det ikke slik at informasjonssikkerhet er et ukjent begrep i bransjen. Tabell 4.1 og 4.2 viser eksempler på retningslinjer og beste praksis samlinger som blir fulgt av operatører gjennom inkludering i styrende dokumenter.

Referanse	Tittel
IEC 17799	Information Technology- Security techniques - Code of practice for information security management
IEC 62443	Security for industrial process measurement and control - Network and system security
RFC 1918	Address Allocation for Private Internets
RFC 2246	Transport Layer Security
ANSI / ISA 99[28]	Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program

Tabell 4.1: Standarder

Referanse	Tittel
OLF 104 [2]	OLF Retningslinje Nr. 104 - Krav til informasjonssikkerhetsnivå i IKT-baserte prosesskontroll-, sikkerhets- og støttesystemer
API & NPRA	Security Vulnerability Assesment Methodology for the Petroleum and Petrochemical Industries
API 1164	Pipeline SCADA security
AGA 12	Cryptographic Protection of SCADA communication

Tabell 4.2: Anbefalte retningslinjer

Operatørene på norsk sokkel har stor grad av frihet til å velge hvordan de vil vurdere informasjonssikkerheten og tilfredstille kravene gitt av Petroleumstilsynet (Ptil). Hvis det imidlertid viser seg at informasjonssikkerheten ikke var blitt ivaretatt på en tilfredsstillende måte i etterkant av en alvorlig hendelse på norsk sokkel, kan det føre til sanksjoner fra Ptil og i ytterste konsekvens, tap av konsesjoner. Noe av grunnen til inkonsekvensen i forhold til krav og håndtering av risiko som eksisterer i dag kan være knyttet til uoverensstemmelser for hvilken anvendbarhet og verdi de har for bransjen.

Det finnes mange eksempler på storulykker i andre industrier som er forårsaket av datafeil, se kapittel 2.2. Vi har enda tilgode å dokumentere storulykker i petroleumsindustrien som resolutt skyldes en feil i IT-systemer eller brudd på informasjonssikkerhet. Imidlertid, kan avsløringene rundt Deepwater Horizon-ulykken i kapittel 2.2.1 peke på en innvirkning i forkant av ulykken. Trolig er

det også mange hendelser som holdes hemmelig. Problemet med hendelser på offshoreinstallasjoner er at de sjelden skyldes en feil alene, det er gjerne en kombinasjon av uforutsette hendelser. Dette er en av utfordringene med å lage IT - risikoanalyser på en offshoreinstallasjon, først og fremst siden all IT inngår i et eller annet system der det er vanskelig å isolere ut det risikobidrag som kan knyttes mot IT fra det risikobidrag som utgjøres av alle andre elementer i systemet - og ikke minst den menneskelige innvirkning. Det finnes databaser som også dekker IT-relaterte hendelser, men det er mer innen spesielle industrier eller organisasjoner at dette logges konsistent. Imidlertid, viser hendelsestatistikk fra International Marine Contractors Association (IMCA) at datafeil ble rapportert som den største hovedårsaken til ulykker forbundet med Dynamic Positioning på offshorefartøy, se tabell 4.3. Selv om det kan forventes at de rapporterte tilfellene bare representerer et fragment av det totale antall offshoreulykker hvert år, viser statistikken at datafeil kan forårsake hendelser og at de i dette tilfellet skjer med en høyere frekvens sammenliknet med andre årsaker. Statistikken er hentet fra et whitepaper i Deepwater Horizon Study group [23].

Cause of incident	Main cause	Secondary cause
Computer	15	4
Electrical	2	3
Environment	3	1
Human error	7	6
Power generation	10	4
Reference	10	0
Thruster	5	0
Procedures	0	7
Other	1	3
TOTAL	53	27

Tabell 4.3: Årsaker til hendelser vedrørende DP, rapportert til IMCA i 2007 [23]

OLF har utført en analyse av verdien til videre innføring av IO på Norsk sokkel [49]. Konklusjonen er at verdien fra IO representerer et potensial på 250 mrd NOK netto nåverdi (NPV - se kapittel 4.3 for definisjon) . Kostnadene for å realisere denne verdien er 25 mrd NOK (NPV) over de neste 15 årene. De største bidragsyterne til gevinstpotensialet er reserveøkning og akselerert produksjon som følge av produksjonsoptimalisering. Det virker logisk å eskalere investeringer i risikoreduserende tiltak for IT-risiko i takt med den videre satsingen på IO. I det minste kan det være et godt intensiv for å rettferdiggjøre investeringene. IT bør ikke behandles ulikt andre fagfelt og flere av antakelsene i standard risikohåndtering baserer seg på illusjonen om at IT-systemene er isolerte, lokale bokser som gjør jobben sin perfekt.

Manglende vilje og incentiv for å bedre informsjonssikkerheten kan forbedres ved å få på plass gode rutiner for rapportering og oppfølging av uønskede hendelser. En bør også følge opp alvorlighetsgraden av uønskede hendelser, slik at man får på plass risikoforståelsen av hendelsen. Erfaring viser at oppmerksomheten rundt uønskede IT hendelser innen olje og gass er lav, og en mangler gode eksempler for å skape forståelse av hva som kan gå galt. HMS og IT må også ses på i en sammenheng, da en IT-hendelse kan få HMS-konsekvenser.

4.3 Verdien av informasjonssikkerhetstiltak

Prinsipielt er det tre alternative måter å behandle risiko i prosjekter som berører sikkerhet. En kan (1) ta alle konsekvensene av en ulykke selv, (2) redusere sannsynligheten og / eller konsekvensene for en ulykke ved sikkerhetstiltak eller (3) overføre konsekvensene for en hendelse til en part som kan håndtere dem bedre, for eksempel ved å kjøpe forsikring [50].

En måte å vurdere slike avgjørelser er ved å ta i bruk tradisjonell lønnsomhetsanalyse. Dette er en metode for å tallfeste de risikoreduserende tiltakene i kroner og ører. I prosjekter over lengre tid er det sjeldent at kostnadselementene og nytteelementene oppstår samtidig. For å få en oversikt over nytteeffekter og kostnader i løpet av en periode, brukes netto nåverdi. Denne verdien finner man ved å beregne følgende formel.

$$NPV \sum_{i=0}^{n} \frac{U_t}{(1+k)^i}$$

Der U_t er kontantstrømmen over en tidsperiode t, k er diskonteringsrenten og n er antall år. Diskonteringsrenten i en slik analyse forutsettes å være konstant, men det vil ligge en del usikkerhet knyttet til tallet. Med diskonteringsrenten kan en finne ut hva kostnadene er ved å binde kapital i et prosjekt. Dersom man investerer 10 millioner kroner i et sikkerhetstiltak og forventer en besparelse på 5 millioner hvert år i fem år, og setter diskonteringsrenten til 5% vil man få en forventet gevinst på:

$$E[NPV] = -10 + \frac{5}{(1+R)} + \frac{5}{(1+R)^2} + \frac{5}{(1+R)^3} + \frac{5}{(1+R)^4} + \frac{5}{(1+R)^5} \approx 11,6$$

Det vil si at man verdsetter en krone i dag, mer enn en krone til neste år. Når en planlegger et investeringsprosjekt, så er den "ekte" netto nåverdi (NPV) ukjent. Det er med andre ord vanskelig å si hvor store kostnadene vil bli. I slike tilfeller benytter man derfor forventet netto nåverdi E[NPV], og lar diskonteringsrenten variere i takt med bankrenten. En operatør kan da velge det alternativet med høyest forventet netto-nåverdi.

Tradisjonell lønnsomhetsanalyse forutsetter at alle ikke-økonomiske dimensjoner må gjøres om til sammenlignbare enheter, for eksempel ved verdisetting av menneskeliv. Health and Safety Executive (HSE) anbefaler for eksempel en verdi på £ 1 000 000 [51]. Slike omregninger blir kritisert i boken; "Dangerous Work and the Value of Human Life" [52]. Det kan likeledes være problematisk å knytte en kostnad til konsekvensen av en hendelse relatert til informasjonssikkerhet. Dette på grunn av mangel på relevante historiske hendelser og kompleksiteten knyttet til utfallet av sikkerhetsbrudd. Det å sette en kostnad på konsekvensene av et datavirus i prosessystemene eller programvarefeil kan være vanskelig og lite hensiktsmessig. Det er ikke ønskelig å benytte slike forutsetninger som basis i oppgavens økonomiske modell. Den videre analysen benytter den forventede nytteteorien for å vurdere de forskjellige alternativene. Forventet nytteteori er et av de mest sentrale begrepene i økonomisk tenking. I forventet nytteteori antas det at en operatør velger det alternativet som tilbyr høyest mulig forventet nytteverdi.

Det vil være av interesse for oppgaven å tydeliggjøre hva som skjer hvis en operatør ønsker å investere i et bestemt sikkerhetstiltak uten å ta hensyn til mulige IT-tiltak.

For å vise at en overser en viktig del av risikohåndteringen hvis IT ikke betraktes som en del av risikobildet, er det ønskelig å sette opp en økonomisk modell som søker å nyttemaksimere håndteringen av risiko i to forskjellige scenarioer:

1. I det første velger vi å se vekk ifra investeringer i informasjonssikkerhet når vi vurderer et sikkerhetstiltak

2. I det andre velger vi å vurdere et sikkerhetstiltak med hensyn til at det finnes alternative investeringer i sikkerhetstiltak for IT

4.3.1 Investerer ikke i informasjonssikkerhetstiltak

Denne modellen er basert på artikkelen "On how access to an insurance market affects investments in safety measures, based on the expected utility theory" av Eirik Bjorheim Abrahamsen og Frank Asche [50]

I dette tilfellet skal vi vurdere hvordan en maksimerer forventet nytteverdi når en investerer i et sikkerhetstiltak uten å vurdere alternative tiltak for informasjonssikkerhet.

Betrakt et firma som har preferanser relatert til formue y og en ikke-økonomisk variabel h. I følgende eksempel er h referert til datatap, men kan i prinsippet være alle slags typer ikke-økonomiske verdier som dødsfall, skader osv. Preferansene er representert av nyttefunksjonen

$$U(y, h) \tag{4.1}$$

Nyttefunksjonen er økende og konkav i y, noe som impliserer at firmaets marginale nytteverdi ($\partial U/\partial y$) synker ettersom formuen øker. Det antas også at nyttefunksjonen er synkende og konveks i h, noe som impliserer at ulempen med påfølgende datatap synker. Det første datatapet forårsaker altså mer ulempe enn å gå fra 100 til 101. For å forenkle modellen antar vi at det finnes kun 2 tilstander i verden. I den ene skjer det en uønsket hendelse som går på bekostning av informasjonssikkerhet, la oss kalle det en IT-hendelse. I den andre skjer det en hendelse som ikke involverer informasjonssikkerhet, la oss kalle det en vanlig hendelse.

Hvis en IT-hendelse forekommer er firmaets formue og antall systemfeil henholdsvis y_1 og $h_1(h_1 > 0)$. Hvis en vanlig hendelse forekommer er firmaets formue og antall datatap henholdsvis $y_2(y_2 > y_1)$ og $h_1(h_1 = 0)$. Den initielle verdien for datatap og størrelse på formue er h_0 og y_0. Sannsynligheten for en IT-hendelse (h er i tilstand 1) er angitt som p.

Anta at firmaet kan investere (r) i sikkerhetstiltak som påvirker konsekvensene i tilfelle det skjer en vanlig hendelse. Vi antar at kostnaden til sikkerhetstiltaket c,$c(r)$ er en voksende og konveks funksjon; $\partial c/\partial r > 0$ og $\partial^2 c/\partial r^2 > 0$. Dette betyr at kostnaden øker som følger av økt implementering av sikkerhetstiltak, men gradvis bidrar den økte implementeringen til økt kostnad for firmaet.

Størrelsesordenen til reduseringen i tap av formue (l) og reduseringen av omfanget til hendelsen (v) er avhengige av investeringene i r. Som en forenklet antakelse kan vi si at reduksjonen i tap av formue og reduksjonen i omfanget

til hendelsen, gitt investering i sikkerhetstiltak er deterministisk. Vi antar at reduksjonen i tap av formue når en hendelse inntreffer på grunnlag av investering i r,$l(r)$, er økende og konveks; $\partial l/\partial r > 0$ og $\partial^2 l/\partial r^2 > 0$. De samme antakelsene gjelder for $v(r)$, noe som betyr at $\partial v/\partial r > 0$ og $\partial^2 v/\partial r^2 > 0$, Fra disse antakelsene kan en se at firmaets marginale nytteverdi fra sikkerhetstiltak blir mindre ettersom investeringene i sikkerhetstiltak øker.

Under disse antakelsene må firmaet velge r for å maksimere

$$EU = (1-p)U(y_1, h_1) + pU(y_2, h_2) \tag{4.2}$$

der

$$y_{1\,formuen\,hvis\,det\,skjer\,en\,IT-hendelse} = y_{0\,den\,initielle\,formuen} - c(r)_{kostnad\,for\,sikkerhetstiltaket}$$

$$y_{2\,formuen\,hvis\,det\,skjer\,en\,vanlig\,hendelse} = y_{0\,den\,initielle\,formuen} - c(r)_{kostnad\,for\,sikkerhetstiltaket} - l(r)_{det\,reduserte\,tapet}$$

$$h_{1\,antall\,systemfeil\,hvis\,det\,skjer\,en\,IT-hendelse} = h_{0\,antall\,datatap}$$

$$h_{2\,antall\,systemfeil\,hvis\,det\,skjer\,en\,vanlig\,hendelse} = 0$$

Den deriverte av forventet nytteverdi, gitt r er

$$\partial EU/\partial r = pU_{1y}(-c_r) + pU_{1h} + (1-p)U_{2y}(-c_r - l_r)$$

$$= -(1-p)U_{2y}l_r - pU_{1h} - [pU_{1y} + (1-p)U_{2y}]c_r = 0 \tag{4.3}$$

Dette betyr at det optimale nivået av sikkerhetstiltak er på det punktet der den marginale nyttekostnaden av nedgang i firmaets formue på grunn av kostnadene til tiltakene $[pU_{1y} + (1-p)U_{2y}]c_r$ er lik den marginale nytteverdien til sikkerhetstiltakene $(1-p)U_{2y}l_r - pU_{1h}$. Firmaets optimale investering i sikkerhetstiltak (r) når vi ikke vurderer IT-tiltak, er på det punktet der nytteverdien til den siste kronen brukt på sikkerhetstiltak (r) er lik nytteverdien til det reduserte tapet som er forårsaket av den siste kronen brukt på sikkerhetstiltak (r).

Den marginale nytteverdien består av to deler:

1. Den marginale nytteverdien fra en økning i firmaets formue gjennom redusert tap i formue hvis det skjer en vanlig hendelse: $(1-p)U_{2y}l_r$.

2. Den marginale nyttekostnaden fra økt datatap hvis det skjer en IT-hendelse: pU_{1h}

Ingen investering i IT-tiltak betyr at det ikke blir noen redusering i datatap eller redusert tap i formue hvis vi får en IT-hendelse. h er en funksjon for preferanser i forhold til datatap, og vanlige sikkerhetstiltak kan derfor ikke påvirke h i denne modellen. I den grad firmaet ønsker å unngå slike hendelse, vil det påvirke firmaets avgjørelser. Hvis firmaet ikke har interesse av å unngå datatap eller redusere kostnadene ved en IT-hendelse vil det overinvestere i vanlige sikkerhetstiltak avhengig av den egentlige sannsynligheten til P (IT-hendelse).

4.3.2 Tar hensyn til alternativ investering i informasjonssikkerhetstiltak

I dette tilfellet kan firmaet velge å investere r i sikkerhetstiltak for vanlige hendelser og s i sikkerhetstiltak for IT-hendelser. Vi bruker de samme betingelsene fra forrige modell.

Under disse antakelsene må firmaet velge r og s for å maksimere

$$EU = (1-p)U(y_1, h_1) + pU(y_2, h_2)$$

der

$$y_{1\,formuen\,hvis\,det\,skjer\,en\,IT-hendelse} = y_{0den\,initielle\,formuen} - c(r)_{kostnad\,for\,vanlig\,sikkerhetstiltak} - c(s)_{kostnad\,for\,IT-tiltak} - l(s)_{redusert\,tap}$$

$$y_{2\,formuen\,hvis\,det\,skjer\,en\,vanlig\,hendelse} = y_{0den\,initielle\,formuen} - c(r)_{kostnad\,for\,vanlig\,sikkerhetstiltak} - c(s)_{kostnad\,for\,IT-tiltak} - l(r)_{redusert\,tap}$$

$$h_{1antall\,systemfeil\,hvis\,det\,skjer\,en\,IT-hendelse} = h_{0antall\,datatap} - v(s)_{det\,reduserte\,antal\,datatap}$$

$$h_{2antall\,systemfeil\,hvis\,det\,skjer\,en\,vanlig\,hendelse} = 0$$

Den deriverte av forventet nytteverdi, gitt r er:

$$\partial EU/\partial r = pU_{1y}(-c_r) + pU_{1h} + (1-p)U_{2y}(-cr - lr)$$

$$= -(1-p)U_{2y}l_r - pU_{1h} + [pU_{1y} + (1-p)U_{2y}]c_r = 0 \qquad (4.4)$$

$\partial EU/\partial r$ er lik i begge scenarioene

Den deriverte av forventet nytteverdi, gitt s er:

$$\partial EU/\partial s = pU_{1y}(-c_s - l_s) + pU_{1h}(-v_s) + (1-p)U_{2y}(-c_s)$$

$$= -pU_{1y}l_s - pU_{1h}v_s - [pU_{1y} + (1-p)U_{2y}]c_s = 0 \tag{4.5}$$

Dette betyr at det optimale nivået av sikkerhetstiltak for IT er på det punktet der den marginale nyttekostnaden av nedgang i firmaets formue på grunn av kostnadene til tiltakene $[pU_{1y} + (1-p)U_{2y}]c_s$ er lik den marginale nytteverdien til sikkerhetstiltakene $pU_{1y}l_s - pU_{1h}v_s$. Firmaets optimale investering i sikkerhetstiltak (s), er på det punktet der nytteverdien til den siste kronen brukt på sikkerhetstiltak (s) er lik nytteverdien til det reduserte tapet som er forårsaket av den siste kronen brukt på sikkerhetstiltak (s).

Den marginale nytteverdien består igjen av to deler:

1. Den marginale nytteverdien fra en økning i firmaets formue gjennom redusert tap i formue hvis det skjer en IT-hendelse: $pU_{1y}l_s$.

2. Den marginale nytteverdien fra redusert datatap hvis det skjer en IT-hendelse:$pU_{1h}v_s$

Tolkning av resultatene Fra ligningene 3 og 4 ser vi at en rasjonell operatør, som aksepterer risikoen for IT-hendelser, vil håndtere den ved å kombinere investeringer i vanlige sikkerhetstiltak, IT-sikkerhetstiltak og å selv ta kostnadene med en ulykke hvis det skjer en hendelse, slik at den marginale nytteverdien til de forskjellige handlingene er den samme.

I økonomiske modeller for investering i sikkerhetstiltak, eksisterer det en aveiing mellom kostnaden til sikkerhetstiltak når en uønsket hendelse ikke skjer, og fordelen med lavere sansynlighet og konsekvens forbundet med hendelsen [50]. Dette blir forenklet ved å representere konsekvensene med en samlet enhet; penger. Analyser som hovedsaklig er fokusert på økonomiske faktorer og ikke de ikke-økonomiske faktorene, vil føre til en underinvestering i sikkerhetstiltak. Vanligvis blir disse variablene transformert til kroner og øre. I slike tilfeller blir forkjellen i investeringene avgjort av hvordan variablene blir vektlagt for å fastslå nivået av sikkerhetsinvesteringene.

I modellen har forbrukeren (operatøren) ubegrenset med resurser til rådighet og da er det ikke nødvendig å økonomisere med ressursene. Den rasjonelle forbruker vil i et slikt tilfelle tilpasse seg på det nivået der hans behovstilfredsstillelse blir størst, altså der marginal nytteverdi blir størst. Virkeligheten er imidlertid slik at de aller fleste i vårt samfunn er nødt til å tilpasse seg innenfor rammen av begrensede økonomiske ressurser. Ved å introdusere en budsjettbetingelse kan en lettere svare på hvordan en operatør skal fordele de begrensede ressursene på forskjellige sikkerhetstiltak. Det vil være interessant å få fram hva en tilleggsbevilgning i et spesifikt tiltak vil medføre. Det kan jo for eksempel hende at et selskap ikke ønsker at en fremtidig investering i sikkerhetstiltak for IT skal gå på bekostning av investeringen i andre typer tiltak. Men vil da en slik tilleggsbevilgning, som utelukkende blir forbeholdt sikkerhetstiltak for IT, være hensiktsmessig? En potensiell fremgangsmåte for å behandle dette temaet

er presentert i Appendix A, men modellen blir presentert som et utgangspunkt for videre arbeid og er ikke en ferdig modell.

Kapittel 5

Drøfting

5.1 Behov for risikoanalyser

Risikoanalyser tar tradisjonelt sett utgangspunkt i å minimere ulykker forbundet med tap av liv (storulykker), og IT er historisk sett ikke en annerkjent årsak til storulykker på offshoreinstallasjoner. Imidlertid kan vi knytte IT-problemer opp mot en av mange initierende årsaker til Deepwater Horizon ulykken. Ser vi vekk fra petroleumsindustrien finner vi flere eksempler på liv som har gått tapt på grunn av virus og svikt i IT-systemer. Som et eksempel finnes det sterke indikatorer på at en trojaner om bord Flight 5022 forårsaket krasjet på Madrid-Barajas flyplass i 2008 som resulterte i 154 dødsfall. Det er i følge kilden [53] enda ikke utgitt en havarirapport som kan konkludere med denne årsaken. Sett i lys av Stuxnet kan en ikke se bort i fra at vi i fremtiden kan oppleve ulykker på offshoreinstallasjoner som skyldes dårlig informasjonssikkerhet.

Alt tyder på at utviklingen i petroleumsindustrien skjer i takt med videre integrering av informasjonsteknologi. Norge ønsker å fortsette å være ledende innen IO, noe som kan forårsake at vi kan være de første til å oppleve konsekvensene av en alvorlig hendelse. Dette innebærer et visst ansvar for å også være først ute med de rette metodene for å minimere risikoen.

Fra et annet perspektiv kan IO også benyttes til HMS-formål ved raskere deteksjon av faresituasjoner og avvik av betydning for personell, miljø, utstyr og produksjon. Risikoeksponeringen offshore vil også reduseres fordi det blir mindre helikoptertransport når ansatte kan utføre flere arbeidsoppgaver fra land. IO gir dessuten også mulighet for å utnytte kompetansen til personell som av ulike helsemessige årsaker ikke lenger kan arbeide offshore.

Det har vært skrevet mye om "cyber terrorister" i mediene de siste årene, men trolig er mange av disse historiene overdrevet. Ja, Al Qaeda hadde mye informasjon om SCADA-systemer [54], men ingenting indikerte at de faktisk hadde en plan. En av de som mener en potensiell trussel fra "cyber terrorister" er sterkt overdrevet er Bruce Schneier, en kryptografiekspert og grunnleggeren av Counterpane Internet Security i USA. Han sier at de store "cyber-terroristangrepene" som alle har forventet seg, ikke har hendt fordi de er mye vanskeligere å utføre enn de fleste tror. Han argumenterer med at sedvanlig terrorisme, som å kjøre en lastebil full av eksplosiver inn i et atomkraftverk, er lettere og mye mer effektivt. La oss se på dette fra et annet perspektiv. Kevin Driscoll, en forsker fra

Honeywell Technology Center uttalte følgende:

> "I am both a controls engineer and former commercial pilot, and let me tell you, learning to program a PLC is a hell of a lot easier than learning to fly a 747."
>
> Kevin Driscoll [54]

Det må settes spørsmålstegn med hvilke eventuelle motiv en gruppe skulle hatt for å planlegge og gjennomføre et slikt angrep. Det virker mer innlysende at militære organer er i stand til nettopp dette. De har både motiv og resursene til å utvikle og bruke Internettvåpen rettet mot offshoreinstallasjoner, ettersom det kan forårsake store økonomiske lammelser i et land som for eksempel Norge og samtidig holdes anonymt. Som nevnt i kapittel 2.1 driver flere land i verden å ruster opp til Internettkrigføring, og senest i slutten av mars i år, dagen etter at Forsvaret startet bombeaksjonene i Libya ble Forsvaret utsatt for et massivt, målrettet dataangrep [55]. I følge Forsvaret responderte de raskt på trusselen og angriperen lyktes kun å hente ut ugradert informasjon fra en av PCene, og skriver samtidig at systemene daglig blir utsatt for forsøk på infiltrasjon. Det er svært vanskelig å finne kilden til slike angrep og angriperen forblir trolig anonym, noe som er ønskelig for militære operasjoner og ikke nødvendigvis for terrorhandlinger.

Den fremvoksende industrien for skadelig programvare har gjort det enkelt å tilegne seg virus og trojanere mot betaling. Skadelig programvare bestilles av organisasjoner og enkeltpersoner. En cyber-kriminell fra Kina bekrefter at han også får oppdrag fra myndigheter og militære organer [43]. Programvaren skreddersys av cyber-kriminelle til formål som; industriell spionasje, sabotasje, svindel, informasjon om produktstrategier og patentutvikling.

Det ligger i luften at myndighetene kommer til å innføre strengere krav til industrien. Informasjonssikkerhet er i dag veldig lite regulert og det opp til hver enkelt leverandør eller eventuelt reder/eier/operatør hva slags policy de har for software security. Reglene åpner for fjernstyrt support av sanntidssystemer over Internett, men det finnes ikke generelle krav eller standarder som påtvinges slike systemer. Det økende trusselnivået og antall hendelser taler for at vi i nær fremtid får klarere regler for hvordan systemene skal sikres. Dagens risiko- og sårbarhetsanalyser mangler oversikt og har ofte mer fokus på å holde produksjonen i gang enn på mannskapets sikkerhet

5.2 Metode

Det finnes ikke en foretrukket metode for IT-risikoanalyse, de fleste operatører bruker standardanalyser og mangler et behov for å videreutvikle den så lenge det tilfredstiller OLF's krav.

IT-hendelser er vanskelige å kvantifisere, og mye av grunnen til dette er mangelen på hendelsesrapportering vedrørerende IT. Det finnes mange forskjellige databaser som håndterer tradisjonelle ulykker og vedlikeholdskomponenter, men svært få inneholder noen form for informasjon om IT-systemer. Økt rapportering og fokus på slike hendelser kan bidra til mer kunnskap som kan redusere usikkerheten forbundet med IT. Sintef har utarbeidet en systematisk måte for hendelsesrapportering på norsk sokkel som kalles Incident Response Management (IRMA) [13]. Etter samtaler med Sintef virker det som om denne

metoden ikke fikk det gjennomslaget som de hadde håpet på. Fremstøt på et oppfølgerprosjekt som skulle måle effekten av dette ble nedprioritert under fusjonen mellom Statoil og Hydro. Imidlertid kan Sintef melde at de nå har fått et oppfølgerprosjekt som heter IMMER som skal starte opp over sommeren 2011, og skal blant annet se på effekten av sikkerhetstiltak.

En annen årsak til problemene med risikohåndteringen er at det er to forskjellige verdener skal integreres. På den ene siden har vi kulturen som jobber med kontrollsystemene som prioriterer pålitelighet og tilgjengelighet, ikke sikkerhet. Så lenge systemene fungerer er det ikke ønskelig med oppdateringer og patcher som muligens kan forårsake ustabilitet. Tradisjonelt sett har disse stolt på at obskuritet og isolering av systemene er sikkerhet i seg selv, og mange prosesskontrollsystemer opereres med standard brukernavn passord for enkel tilgang.

På den andre siden har vi IT-kulturen som vet at de tradisjonelle sikkerhetsverktøyene ikke er tilstrekkelig for kontrollsystemene ettersom bedriftsnettverkene blir tilkoblet. De har ikke ansvar for eller tilstrekkelig kunnskap om kontrollsystemene og har derfor lett for å overse viktige aspekter med prosessene. Det er trolig et tverrfaglig samarbeid som er nøkkelen til suksess. Tettere samarbeid mellom leverandører, operatører, verft og de ulike disiplinene, samt en økt forståelse for det nye risikobildet vil bidra til en sikrere hverdag.

Valget av en ren kvalitativ metode i oppgaven kan så klart diskuteres. Der man har mulighet for å oppdrive kvantitative beregninger og tall som viser seg nyttige, bør dette tas hensyn til. Dette kan gjelde interne oversikter over antall angrep, statistikk for hardwarefeil og databaser over registrerte hendelser. Siden denne oppgaven ble laget uten tilgang på slik informasjon, falt valget på kvalitative vurderinger naturlig. Ofte kan slike kvalitative vurderinger komme med mer verdifull informasjon enn prediksjoner basert på frekvensen av tidligere hendelser.

Det kan diskuteres om ikke det er nødvendig å vurdere usikkerhet i frekvens og konsekvens hver for seg, og ikke slå dem sammen som gjort i denne oppgaven. Det vil føre til en mer nøyaktig representasjon. Det kan for eksempel øke beslutningsgrunnlaget hvis det viser seg at det finnes stor usikkerhet i konsekvensen av en hendelse men frekvensen er lav og inneholder lite usikkerhet. IT medfører en annen type trussel enn det vi tidligere er vant med på offshoreinstallasjoner. Beste praksis for IT-risikoanalyse offshore vil etterhvert modnes og aksepteres.

5.3 Økonomisk modell

Integrerte operasjoner handler om å redusere kostnader og effektivisere produksjonen på norsk sokkel, så hvis man stiller for store sikkerhetskrav slik at tiltakene totalt sett blir for dyre, er man dømt til å mislykkes. På den annen side representerer IO et gevinstpotensiale på mange milliarder norske kroner og dermed burde man kunne bake inn kostnader til informasjonssikkerhet i begrepet ”the cost of doing business”. Det er i dag ingen krav til informasjonssikkerhet på samme måte som det er krav til HMS.

En stans i produksjonen kan fort koste flere millioner i timen. Det burde derfor være god økonomi i å innføre tiltak mot informasjonssikkerhetstrusler som kan medføre stopp, men da må en ha metoder for å identifisere disse, noe som IT-risikoanalyser vil kunne bistå med.

Hva slags argumentasjon, dokumentasjon eller beviser trenger en operatør for å bruke millioner på informasjonssikkerhet? Hvis ikke operatører og leverandører investerer mer i å dokumentere risikoen som IT utgjør, tyder mye på at forskrifter eller pålegg er nødvendig

Den økonomiske modellen som oppgaven presenterer for å vurdere investeringer i IT-sikkerhet, viser at hvis en ikke tar hensyn til investeringer i IT-sikkerhetstiltak, vil en trolig overinvestere i vanlige sikkerhetstiltak. En må altså investere i vanlige sikkerhetstiltak opp til det punktet der den marginale nytteverdien til sikkerhetsinvesteringene er lik den marginale nytteverdien av å ta alle konsekvensene hvis/når en ulykke skjer.

Kapittel 6

Konklusjon

Datasystemer er åpenbart delaktige i hendelser som kan skade individer, organisasjoner og dens verdier. Potensiell skade kan komme i form av ødeleggelse eller tap av liv, tap av omdømme, tapt inntekt eller nedsatt produksjon. Digitale systemer har startet en diskre revolusjon i måten petroleumsbransjen opererer på, men risikostyringen har ikke holdt følge. Digitale systemer introduserer nye feilmoduser som forandrer årsaken og hendelsesforløpet til uønskede hendelser.

Risikoanalyser for IT er allerede i bruk hos flere operatører. Det eksisterer imidlertid ikke noen konsensus i bransjen på hvordan disse skal gjennomføres og de er i liten grad fokuserte på sikkerhet, men på å opprettholde produksjonen. En lurer seg selv hvis en tror at de attraktive fordelene med en digital livsstil, om det er for personer eller selskaper, ikke kommer med en pris i form av datakontroll og sikkerhet.

For å utvikle bedre IT-risikoanalyser må en få på plass gode rutiner for rapportering og oppfølging av uønskede hendelser. Oppmerksomheten rundt uønskede IT hendelser innen olje og gass er lav. De som opererer systemene må ha kompetanse til å følge opp alvorlighetsgraden av uønskede hendelser, slik at man får på plass risikoforståelsen. HMS og IT må ses på i en sammenheng, da en IT-hendelse kan få HMS-konsekvenser.

Det er mye usikkerhet rundt frekvensen og konsekvensen av IT-hendelser, og det er en begrensning på hvor mye informasjon vi kan få fra hendelsesrapportering alene. Å forutsi risiko betyr å forutsi hva som kan skje, hva som kan gå galt, hvordan systemet er forberedt, og hvordan det takler uforutsette variasjoner og hendelser. IT-risikoanalyser bør derfor ha et økt fokus på å beskrive usikkerheten best mulig, samt redusere usikkerhet der det er mulig.

På det engelske språket skilles det mellom security og safety, der security omhandler sikring av eiendeleler og informasjon, mens safety er mer HMS-relater. På norsk dekkes begge disse begrepene av ordet *sikkerhet*. Etterhvert som systemer blir mer integrerte, vil trolig ordet sikkerhet bli stående mens forskjellen mellom “security” og “safety” viskes ut.

Bibliografi

[1] OLF. HMS og integrerte operasjoner: Forbedringsmuligheter og nødvendige tiltak. Technical report, OLF, 2007.

[2] OLF retningslinje nr.104 - krav til informasjonssikkerhetsnivå i ikt-baserte prosesskontroll-, sikkerhets- og støttesystemer, 2007.

[3] Rosing-prisen, 2008. URL `http://www.dataforeningen.no/it-sikkerhetsprisen.4796706-160557.html`.

[4] Per Oscarson. *Informationssäkerhet i verksamheter- begrepp och modeller som stöd för förståelse av informationssäkerhet och dess hantering i verksamheter*. Linköpings universitet, 2001.

[5] Joel Carter Eric Byres, John Karsch. Good practice guide on firewall deployment for SCADA and process control networks. *National Infrastructure Security Co-ordination Centre (NISCC)*, 1.4:42, 2005.

[6] Petter Wedum Håvard Husevåg Garnes. Innbruddstesting på prosesskontrollsystemer på oljeplattform. Master's thesis, NTNU, 2007.

[7] OLF. OLF-rapport om IO og HMS. *OLF*, 1:46, 2007.

[8] R. Rosness E. Bjerkebaek T. O. Grötan, E. Albrechtsen. The influence on organizational accident risk by integrated operations in the petroleum industry. *Safety Science Monitor*, 14:11, 2010.

[9] George Ivanov Stewart Baker, Shaun Waterman. In the crossfire - critical infrastructure in the age of cyber war. Technical report, MCAfee, 2009. URL `http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf`.

[10] Forsvarets informasjonsinfrastruktur. URL `http://forsvaret.no/`.

[11] Nasjonal sikkerhetsmyndighet. Sikkerhetsvarsel fra NSM - informasjon om skadevaren stuxnet. Technical report, NSM, 2010.

[12] McAfee. Global energy cyberattacks: night dragon". Technical report, McAfee Foundstone Professional Services and McAfee Labs, 2011. URL `http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf`.

[13] Maria B. Line Odd Helge Longva Inger Anne Tøndel Eirik Albrechtsen Irene Wærø Martin Gilje Jaatun, Stig Ole Johnsen. Incident response management in the oil and gas industry. Technical report, Sintef, 2007.

[14] Symantec. Symantec report on attack kits and malicious websites. Technical report, Symantec, 2011. URL `http://www.symantec.com/content/en/us/enterprise/other_resources/b-symantec_report_on_attack_kits_and_malicious_websites_21169171_WP.en-us.pdf`.

[15] François Paget. Cybercrime and hacktivism. Technical report, McAfee Labs, 2010. URL `http://www.mcafee.com/us/resources/white-papers/wp-cybercrime-hactivism.pdf`.

[16] McAfee Labs. Mcafee threats report: Fourth quarter 2010. Technical report, MCAfee, 2010. URL `http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2010.pdf`.

[17] Maria Kjærland. *Cyber Incident Risk Profiling - Applying Systematic Profiling for Assessing Information Systems Security Risks*. PhD thesis, Universitetet i Stavanger, 2007.

[18] S. Lüders. CERN tests reveal security flaws with industrial networked devices. Technical report, CERN, 2006. URL `http://cdsweb.cern.ch/record/1000756/files/open-2006-074.pdf?version=1`.

[19] Christina Walrond David Albright, Paul Brannan. Stuxnet malware and natanz:. Technical report, Institute for Science and International Security, 2011. URL `http://www.isisnuclearіran.org/assets/pdf/stuxnet_update_15Feb2011.pdf`.

[20] Randi Roisli Stig Johnsen, Rune Ask. Reducing risk in oil and gas production operations. *Critical Infrastructure Protection*, 1:83–95, 2008.

[21] Karen Scarfone Keith Stouffer, Joe Falco. Guide to industrial control systems ICS security. Technical report, National Institute of Standards and Technology, 2008. URL `http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf`.

[22] Jerome Radcliffe. SCADA systems - a computer security nightmare? *IBM X-Force Threat Insight Quarterly*, 1:3–6, 2010.

[23] Øyvind Smogeli Jon Espen Skogdalen. Looking forward - reliability of safety critical control systems on offshore drilling vessels. *DHSG*, Working Paper:17, 2011.

[24] CA technologies. The avoidable cost of downtime - the impact of it downtime on employee productivity. Technical report, CA technologies, 2011. URL `http://www.arcserve.com/~/media/Files/SupportingPieces/acd_report_110110.ashx`.

[25] Nancy G. Leveson. *Engineering a Safer World - Systems Thinking Applied to Safety*, volume Draft. Unpublished, 2010.

[26] Trevor Kletz. *What went wrong? - Case Histories of Process Plant Disasters*, volume 4. Gulf Professional Publishing, 1999.

[27] Joe Weiss Marshall Abrams. Malicious control system cyber security attack case study - maroochy water services, australia. *NIST*, 1:16, 2008.

[28] Security for industrial automation and control systems: Establishing an industrial automation and control systems security program.

[29] Scansafe. The vertical risk - web-delivered malware impact by industry. Technical report, Scansafe, 2008.

[30] Jan Erik Vinnem Jon Espen Skogdalen, Ingrid B. Utne. Looking back and forward: Could safety indicators have given early warnings about the deepwater horizon accident? *DHSG*, Working Paper:26, 2011.

[31] Vitneutsagn fra Michael Williams; transocean chief electronics technician. URL `http://www.c-spanvideo.org/program/294728-1`.

[32] Henrik Arnestad Salthe. Oilinfo, dataorm truer norsk sokkel, 12 2010. URL `http://www.oilinfo.no/index.cfm?event=doLink&famId=143617`.

[33] Eric Chien Nicolas Falliere, Liam O Murchu. W32.stuxnet dossier. Technical report, Symantec, 2011. URL `http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf`.

[34] Hacker to go public with siemens SCADA control flaws, . URL `http://news.techworld.com/security/3284398/hacker-to-go-public-with-siemens-scada-control-flaws/`.

[35] SCADA vulnerabilities in industrial control systems, . URL `http://www.nsslabs.com/company/news/press-releases/scada-vulnerabilities-in-industrial-control-systems.html`.

[36] Tor Onshus Stein Hauge, Stig Ole Johnsen. Uavhengighet av sikkerhetssystemer. Technical report, SINTEF, 2009.

[37] Knut Øien Tor Olav Grøtan Sture Holmstrøm Mary Ann Lundteigen Stein Hauge, Tor Onshus. Uavhengighet av sikkerhetssystemer offshore - status og utfordringer. Technical report, SINTEF, 2006.

[38] Terje Aven. *Risk Analysis - Assessing Uncertainties Beyond Expected Values and Probabilities*. Wiley, 2008.

[39] *NORSOK Z-013 Risk and emergency preparedness analysis, Edition 3, October 2010*. Norsk Standard. URL `http://www.standard.no`.

[40] Peter Andow B Tech. M Che. PhD. C Eng. MI Chem E. MBCS. Guidance on HAZOP procedures for computer-controlled plants. Technical report, Health and Safety Excecutive, 1991.

[41] Jordanger I Magnussen O. M Torp O Austeng K, Midtbø J T. Usikkerhetsanalyse - kontekst og grunnlag. Technical report, NTNU, 2005.

[42] R S Iversen E B Abrahamsen, T Aven. Integrated framework for safety management and uncertainty management. *Proc. IMechE*, 224:97–103, 2009.

[43] ScanSafe. Annual global threat report 2009. Technical report, ScanSafe, 2009.

[44] Bazzurro P Carballo JE Shome N, Cornell CA. Earthquakes, records and nonlinear responses. *Earthquake Spectra*, 14:469–500, 1998.

[45] Petersen A Kloprogge P Risbey J Tuinstra W Ravetz J van der Sluijs J, Janssen P. Rivm/mnp guidance for uncertainty assessment and communication: Tool catalogue for uncertainty assessment. Technical report, Utrecht University, 2004.

[46] Renn O Klinke A. A new approach to risk evaluation and management: Risk-based, precaution- based and discourse-based management. *Risk Analysis 22*, 6:1071–1094, 2002.

[47] PTIL. Referat fra arbeidsseminar om ikt-sikkerhet og integrerte operasjoner. Technical report, Petroleumstilsynet, 2006. URL `http://sintef.org/uploadpages/10977/sluttrapport.pdf`.

[48] Petroleumstilsynet. Risikonivå i petroleumsvirksomheten norsk sokkel. Technical report, Ptil, 2010.

[49] OLF. Verdipotensialet for integrerte operasjoner på norsk sokkel. Technical report, OLF, 2006.

[50] Frank Asche Eirik Bjorheim Abrahamsen. On how access to an insurance market affects investments in safety measures, based on the expected utility theory. *Reliability Engineering and System Safety*, 96:361–364, 2010.

[51] UK HSE. Offshore information sheet no. 2/2006. Technical report, Health and Safety Excutive - Offshore, 2006. URL `http://www.hse.gov.uk/offshore/is2-2006.pdf`.

[52] P Dorman. *Markets and Mortality: Economics. Dangerous Work and the Value of Human Life.* Cambridge, 1996.

[53] Malware implicated in fatal spanair plane crash. URL `http://www.msnbc.msn.com/id/38790670/ns/technology_and_science-security/?gt1=43001`.

[54] Steven S. Smith. The scada security challenge: The race is on. *NA*, na: na, 2006. URL `http://www.infosecwriters.com/text_resources/pdf/SSmith_SCADA.pdf`.

[55] Målrettet angrep på forsvaret. URL `http://forsvaret.no/aktuelt/publisert/pressemeldinger/Sider/Malrettet-dataangrep-pa-Forsvaret.aspx`.

[56] Nasjonal sikkerhetsmyndighet. Årsmelding. Technical report, NSM, 2010.

[57] Eirik Albrechtsen. Risikovurderinger i informasjonssikkerhet - utlosende faktor og oppfølging. Master's thesis, NTNU, 2002.

[58] Dorothy E. Denning. Activism, hacktivism, and cyberterrorism. *Networks and Netwars*, 1:239–288, 2001.

[59] Trevor Kletz. *What went wrong? - Case Histories of Process Plant Disasters.* Gulf Professional Publishing, 2009.

[60] McAfee Labs. Mcafee threats report: Third quarter 2010. Technical report, McAfee, 2010. URL `McAfeeThreatsReport:ThirdQuarter2010`.

[61] Arun Raghu Nick Ellsmore. Cyber terrorism - are we there yet? *Stratsec*, 1:13, 2010.

[62] Petroleumstilsynet / Oljedirektoratet. Arbeidsseminar om ikt-sikkerhet og integrerte operasjoner. Technical report, Sintef, 2006.

[63] Pandalabs. Annual report 2010. Technical report, Pandalabs, 2010. URL `http://press.pandasecurity.com/wp-content/uploads/2010/05/PandaLabs-Annual-Report-2010.pdf`.

[64] Arild Sæther. *Mikroøkonomi*. Gyldendal akademisk, 2002.

[65] Roar Gulbrandsen m.f Torgeir Daler. *Håndbok I datasikkerhet*. Tapir akademiske forlag, 2002.

[66] Jan Erik Vinnem. *Offshore Risk Assessment*. Springer, 2007.

[67] Methusela Cebrian Ferrer Zarestel Ferrer. In-depth analysis of hydraq - the face of cyberwar enemies unfolds. Technical report, CA Technology, 2010.

[68] Forsvaret angrepet etter libya-beslutning. URL `http://www.vg.no/nyheter/utenriks/libya/artikkel.php?artid=10086018`.

Figurer

2.1 Rapporterte angrep på datasystemer frem til 2004 [28] 15
2.2 Prosentvis varians av skadevare fordelt på industrisektor og ondsinnet programvare [29] 16

3.1 Tradisjonell Risikoanalyse 24
3.2 IT-Risikoanalyse 25
3.3 Nettverkstopologi [28] 26
3.4 Risikomatrise uten hensyn til usikkerhet 32
3.5 Risikomatrise med tilhørende usikkerhetsklassifisering 41
3.6 Bowtie - Kritisk server går ned 44

4.1 Totalindikator for storulykker per år, normalisert mot arbeidstimer [48] 48
4.2 Personskader per million arbeidstimer, produksjonsinnretninger [48] 48

Tabeller

3.1 Eksempel på en frekvensskala 28
3.2 Eksempel på konsekvensskala 29
3.3 Risikoevaluering 31
3.4 Eksempel på usikkerhetsskala 33
3.5 Usikkerhetsevaluering 34

4.1 Standarder 49
4.2 Anbefalte retningslinjer 49
4.3 Årsaker til hendelser vedrørende DP, rapportert til IMCA i 2007 [23] 50

Appendiks A

Dette kapittelet er kun ment som et forslag til videre arbeid:

Ved å introdusere en budsjettbetingelse kan en lettere svare på hvordan en operatør skal fordele de begrensede ressursene på forskjellige sikkerhetstiltak.

Hvordan skal operatørene investere i vanlige sikkerhetstiltak (R), og sikkerhetstiltak for IT (S) for å oppnå størst mulig nytteverdi? Nytten skal gjøres størst mulig, det vil si maksimeres, gitt den summen som kan nyttes til sikkerhetstiltak. Gitt en budsjettsbetingelse $B = S + R$

der S er kostnaden og antallet sikkerhetstiltak for IT= $(p_1 X)$,

og R er kostnaden og antallet vanlige sikkerhetstiltak= $(p_2 Y)$.

Løser vi $B = (p_1 X) + (p_2 Y)$ med hensyn på X, får vi

$$X = -\frac{p_2}{p_1} Y + \frac{B}{p_1}$$

Utrykket for X setter vi inn i nyttefunksjonen$U = (X, Y)$, som dermed blir en funksjon i en variabel Y:

$$U = U\left[\left(-\frac{p_2}{p_1} Y + \frac{B}{p_1}\right), Y\right] = U(Y)$$

Førsteordensbetingelsen for maksimum av denne funksjonen er at den deriverte av U mhp Y er lik 0. Ved å bruke kjerneregelen for funksjoner av flere variabler får vi:

$$\frac{dU}{dY} = \frac{\partial U}{\partial Y} + \frac{\partial U}{\partial X} \frac{d\left(-\frac{p_2}{p_1} Y + \frac{B}{p_1}\right)}{dY} = U_{y+} U_x \left(-\frac{p_2}{p1}\right)$$

$$U_y = -U_x \left(-\frac{p_2}{p1}\right)$$

Betingelsen for optimalt valg av godekombinasjon ved et gitt budsjett kan da skrives:

$$\frac{U_x}{p_1} = \frac{U_y}{p_2}$$

Forholdet mellom de to sikkerhetstiltakenes grensenytter ved denne godekombinasjonen skal altså være lik forholdet mellom prisene på disse. Denne betingelsen kalles Gossens andre lov eller Gossen-betingelsen [64].