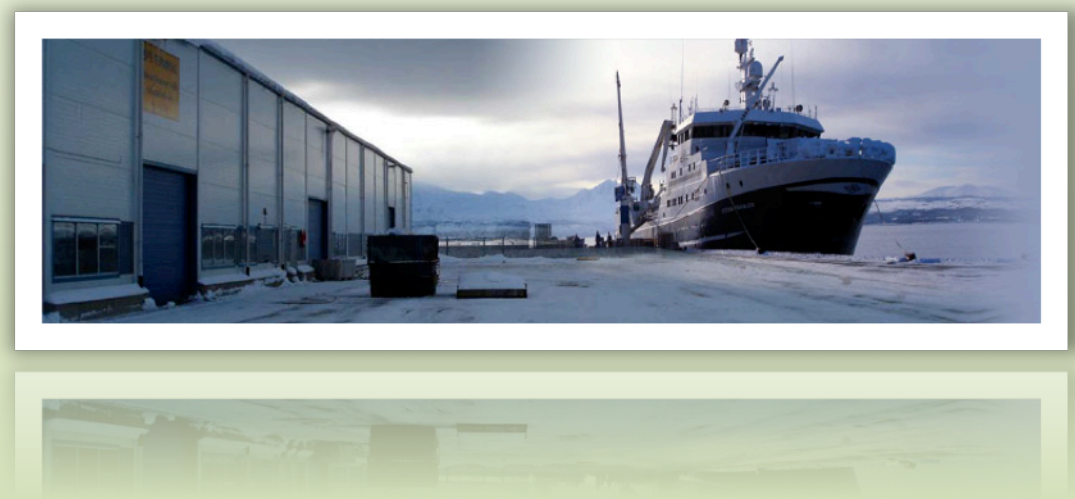
Hovedprosjekt ingeniørfag sikkerhet HMS

ISPS-områder, fokus på av-på havneterminaler



Figur 1: Troms fryseterminal.

Utarbeidet av:
Kandidatnr. 21 John Håkon Næss 129159
Kandidatnr. 43 Bertha Louise S. Myhre 127421
Kandidatnr. 59 Natasza Bjordal Grønfur 112023

HOVEDPROSJEKT

Studenten(e)s navn: Bertha Louise S. Myhre, Natasza Bjordal Grønfur, John Håkon Næss

Linje & studieretning: Sikkerhet, HMS

Oppgavens tittel: *ISPS-områder, fokus på av-på havneterminaler.*

Oppgavetekst:

1. Krav / retningslinjer til "av/på havneterminaler", utfordringer i forhold til regelverket.

   ISPS "av-på havneterminaler" er et spesielt fenomen og vi ønsker å se nærmere på denne formen for ISPS-havneterminaler, og kartlegge eventuelle utfordringer i forbindelse med denne løsningen.
   Som hjelpemiddel vil vi foreta en sikkerhetsvurdering i henhold til "Et verktøy for egenkontroll av Security ved en havneterminal" utgitt av Kystverket, samt gjennomføre risikoanalyser (grovanalyser) av de aktuelle ISPS-havneterminalene.

2. Opplæring og krav til personell som skal ha adgang til ISPS havneterminalen.

   Hvilke løsninger har bedriftene/havneterminalene brukt for opplæring av personell som har arbeidsoppgaver i ISPS "av-på havneterminaler".
   Spesielt problematikk knyttet til "ikke autorisert" personell i henhold til ISPS-koden, både internt og eksternt, som skal inn og gjøre en jobb av kort varighet.

Endelig oppgave gitt: *3. mars 2011*

Innleveringsfrist: Fredag 6.mai 2011 kl. 12.00

Intern veileder Morten Alsaker Lossius, seniorrådgiver i Sjøfartsdirektoratet

Ekstern veileder Hallgeir Tofte/Bente Larsen Selle, Aker Stord

Godkjent av studieansvarlig: Brit Fuller
Dato: 27. april 2011

HØGSKOLEN STORD/HAUGESUND

Høgskolen Stord/Haugesund
Studie for ingeniørfag
Bjørnsonsgt. 45
5528 HAUGESUND
Tlf. nr. 52 70 26 00
Faks nr. 52 70 26 01

Oppgavens tittel		Rapportnummer
ISPS-områder, fokus på av-på havneterminaler		
Utført av		
Bertha Louise Salvanes Myhre, Natasza Bjordal Grønfur, John Håkon Næss		
Linje		Studieretning
Sikkerhet, HMS		Ingeniørfag
Gradering	Innlevert dato	Veiledere
Åpen	6. mai 2011	Morten Alsaker Loussius Bente Larsen Selle/Hallgeir Tofte

Ekstrakt

Rapporten omhandler security med fokus på ISPS koden. Problemstilling har vært utfordringer i forhold til krav og regelverk for ”av-på” havneterminaler, samt hvilken opplæring personell som skal ha adgang til ISPS havneterminalen må inneha.
Oppgaven er utført ved 4 ulike havneterminaler i distriktet.

Det er brukt følgende metoder:
- Kartlegging med
  - Intervju av PFSO og havnepersonell
  - Grovanalyse
  - Kystverket sitt skjema: ” Et verktøy for egenkontroll av security ved en havneterminal”
  - SWOT analyse

Noen av utfordringene de ulike havneterminalene opplever går igjen, i tillegg er det funnet noen merknader og observasjoner ved havneterminalene.
ISPS er en liten del av den daglige driften, men regelverket er likt for faste ISPS havneterminaler og ”av-på” havneterminaler, og de må derfor forholde seg til det samme regelverket. Selv om ISPS har mindre fokus blir det gjennomført faste øvelser, samt øvelser i samarbeid med andre havneterminaler som kan føre til god erfaringsutveksling.

Forord

Denne rapporten er utarbeidet som et ledd i studiet bachelor i ingeniørfag, sikkerhet HMS, og er vårt hovedprosjekt. Hovedprosjekt skrives i 5 og 6 semester, og gir 15 studiepoeng, det er også et krav for å oppnå bachelorgrad i dette studiet. Formålet er at studentene skal bruke det de har lært til å samle inn nødvendig informasjon, sortere ut det mest essensielle stoffet og videre ta nødvendige avgjørelser som en må argumentere for og bevise i form av regelverk og referanser for å løse en konkret problemstilling. I tillegg skal oppgaven omhandle problemstillinger som har tilknytning til et eller flere av de underviste fagområdet.

Rapporten omhandler ISPS-havneterminaler, med fokus på "av-på" sertifisering. Hvilke krav/retningslinjer finnes, og hvilke utfordringer disse terminalene har i forhold til regelverket. Rapporten har også vektlagt opplæring og krav til personell som skal ha adgang til ISPS havneterminaler.

ISPS-koden står for "International Ship and Port Facility Security Code", og dette er et regulativ som ble innført gjennom "The Diplomatic Conference on Maritime Security" avholdt i London desember 2002. Samtidig ble det innført nye forskrifter I SOLAS for å forsterke maritim Security. I Norge ble det fra 1.juli 2004 innført krav til havneterminaler med internasjonal trafikk om at de skal følge ISPS koden.

Fire ulike havneterminaler er belyst med det mål å kartlegge de ulike utfordringene disse havnene kan komme borti, og forslag til løsning er beskrevet. Målsettingen har vært å rapportere disse utfordringene og løsningene med det formål å vekke interesse for samarbeid mellom flere havneterminaler og bruk av hverandres data for å optimalisere løsningen med av-på sertifisering.

Rapporten er utarbeidet av John Håkon Næss, Bertha Louise S. Myhre og Natasza Bjordal Grønfur. Vi ønsker å takke for all hjelp og bistand vi har fått fra alle involverte parter under skrivingen av denne rapporten.
Spesielt ønsker vi å takke vår veileder Morten Loussius hos Sjøfartsdirektoratet, som har bistått med det faglige innhold. Samt Sveinung Hustoft hos Kystverket og Bente Selle hos Aker Stord som har fulgt arbeidet og gitt innspill og kommentarer underveis.

Gruppens dynamikk og samarbeidsevner har fungert veldig bra. Vi har ulik bakgrunn og erfaring, noe som har ført til mange gode og ulike innspill, samt ulik innfallsvinkel. I et slikt prosjekt er tverrfaglig innsikt og innlevelse viktig, da det ikke alltid er slik at bare det ene er rett. Dette har vært et spennende og læringsrikt prosjekt som vi føler er relevant for vårt studie.

Innholdsfortegnelse

FORORD ..... **I**

INNHOLDSFORTEGNELSE ..... **III**

FIGURLISTE ..... **IV**

TABELLISTE ..... **IV**

SAMMENDRAG ..... **V**

ORDFORKLARINGER **1**

1. INNLEDNING **3**

1.1 BAKGRUNN 3

1.2 FORMÅL 5

1.3 HVA ER ISPS-KODEN? 5

1.4 HVORFOR ISPS? 9

1.5 PRAKSIS OG EFFEKTUERING 10

1.6 "AV-PÅ" ISPS-HAVNETERMINALER 12

1.7 OPPLÆRING 13

1.8 BESKRIVELSE AV ISPS HAVNETERMINALENE 15

2 METODE **21**

2.1 KARTLEGGING 21

2.1.1 Intervju *21*

2.1.2 Skjema for egenkontroll av security ved en havneterminal *22*

2.1.3 Grovanalyse *23*

2.1.4 SWOT-analyse *24*

3 RESULTAT **25**

3.1 INTERVJUER 25

3.2 SKJEMA FOR EGENKONTROLL AV SECURITY VED EN HAVNETERMINAL 31

3.3 GROVANALYSE 39

3.4 SWOT-ANALYSE 43

4 DISKUSJON **48**

4.1 INTERVJU OG "EGENKONTROLLSKJEMA" 48

4.2 GROVANALYSE 55

5 KONKLUSJON **58**

6 TILTAK **63**

REFERANSER ..... **I**

VEDLEGG ..... **II**

Figurliste

Figur 1: Troms fryseterminal. _____ *1*
*Figur 2: Risikotenking.*_____ *6*
*Figur 3: Objekter og infrastruktur som er viktige å beskytte i en havneterminal.*_____ *7*
Figur 4: Sikkerhetsnivåer i forhold til risiko og tiltak. _____ *7*
Figur 5: Myndighetshierarki i forhold til ISPS. _____ *10*
Figur 6: Oversiktsbilde havn 1. _____ *15*
Figur 7: Oversiktsbilde havn 2. _____ *16*
Figur 8: Oversiktsbilde havn 3. _____ *18*
Figur 9: Oversiktbilde havn 4. _____ *19*
Figur 10: Gangen i en risikoanalyse. _____ *23*
*Figur 11: Handlingsplan i forhold til ISPS. Plan for iverksetting av tiltak.*_____ *63*

Tabelliste

Tabell 1: Resultat av intervju PFSO havn 1 ..... *25*
Tabell 2: Resultat intervju havnearbeider 1 havn 1. ..... *26*
Tabell 3: Resultat intervju havnearbeider 2 havn 1. ..... *27*
Tabell 4: Resultat intervju leder havn 1. ..... *28*
Tabell 5: Resultat intervju PFSO havn 2. ..... *29*
Tabell 6: Resultat intervju havnearbeider havn 2. ..... *29*
Tabell 7: Resultat intervju PFSO havn 3. ..... *30*
Tabell 8: Resultat intervju PFSO havn 4. ..... *30*
Tabell 9: Grovanalyse Havn 1 ..... *39*
Tabell 10: Grovanalyse Havn 2 ..... *40*
Tabell 11: Grovanalyse Havn 3 ..... *41*
Tabell 12: Grovanalyse Havn 4 ..... *42*
Tabell 13: SWOT-analyse havn 1. ..... *43*
Tabell 14: SWOT-analyse havn 2. ..... *45*
Tabell 15: SWOT-analyse havn 3. ..... *46*
Tabell 16: SWOT-analyse havn 4. ..... *47*

Sammendrag

Denne rapporten tar for seg security, med ISPS som tema. Den er utarbeidet i samarbeid med fire ”av-på” havneterminaler.

Fokus har vært å se på krav og retningslinjer til “av-på” havneterminaler, og hvilke utfordringer de kan møte på i forhold til regelverket. I tillegg er det sett på hvilken opplæring og krav som er gjeldende for personell som skal ha adgang til ISPS havneterminalen.

For å løse de ulike problemstillingene er det gjennomført en kartlegging av havneterminalene ved hjelp av grovanalyse, og intervju av PFSO samt noen havnearbeidere. Videre er Kystverket sitt skjema ”Et verktøy for egenkontroll av security ved en havneterminal” (egenkontrollskjema) brukt. Dette er gjort for å få et bilde av havneterminalene, samt kartlegge hvilken opplæring ulik type personell har gjennomført/skal gjennomføre. For å se hvilke styrker, svakheter, trusler og muligheter de ulike havneterminalene har, er det i tillegg utført en SWOT analyse.

Resultatene viser at enkelte utfordringer går igjen, da spesielt med hensyn på informasjon og opplæring av havnepersonell, både med og uten security-ansvar. Det er også oppdaget noen merknader og observasjoner i forbindelse med ”egenkontrollskjemaet”. Dette går primært ut på å kontrollere om løsninger i forhold til bestemmelsene i ISPS koden er á jour. Utfordringer i forhold til ISPS koden med tilhørende løsninger er vurdert, men resultatene er ikke sammenlignet med security-planen og sårbarhetsanalysen, da dette er graderte dokument. Alle havneterminalene er godkjent av Kystverket, og det er derfor tatt utgangspunkt i dette.
Felles for alle havneterminalene er at ISPS er en liten del av den daglige driften, og blir av den grunn mindre prioritert. Likevel er de fleste havneterminalene er flinke til å utføre felles øvelser og driller, noe som fører til faglig oppdatering, kompetanseoverføring og god erfaringsutveksling.

ISPS koden har ikke egne regler for praktisering av ”av-på” havneterminaler, da dette er en tolkning av regelverket. Det vil si at når havneterminalen er på-sertifisert, gjelder samme krav og regler som ved en fast ISPS havneterminal.

Ordforklaringer

International Ship and Port Facility Security (ISPS)

Designated authority (DA):
Organisasjonen eller administrasjonen innenfor ”the Contracting Government” som er ansvarlig for å sikre gjennomføringen i kapittelet som omhandler havneanlegg. I Norge er dette Kystverket.

Contracting government (CG):
Overordnet forvaltningsmyndighet for havnepolitikken. I Norge er dette Fiskeri- og Kystdepartementet.

Recognised Security Organization (RSO):
En organisasjon med ekspertise innen sikkerhetsspørsmål og med nødvendig kunnskap om skip og havneoperasjoner autorisert til å foreta en vurdering, eller en bekreftelse, eller en godkjenning eller en sertifiseringsaktivitet.

Sikkerhet-safety/security:
I det norske språk finnes det ingen god oversettelse av ordet security. Noen ganger blir ”sikring” brukt, men dette er ikke dekkende . I denne oppgaven brukes det engelske ordet **security** for å beskrive/forklare ”trusler fra utsiden”. På norsk brukes ordet ”sikkerhet” som fellesbetegnelse/oversettelse for ”safety/security”.

Havneterminal:
En del av et havneanlegg. Et havneanlegg (havn) kan bestå av flere havneterminaler

PFSO:
Port Facility Security Officer (havnens sikkerhetsoffiser)

SSO
Ship Security Officer (Skipets sikkerhetsoffiser)

PFSP:
Port Facility Security Plan (havnens sikkerhetsplan)

PFSA:

Port Facility Security Assessment (havnens sårbarhetsvurdering)

Sikringspersonell:

Personer som har arbeidsoppgaver knyttet til ISPS-havneterminalen.

DoS:

Et avtaledokument mellom skip og havn som spesifiserer hvem som skal iverksette og gjennomføre hvilke security-tiltak før og under anløpet.

SOLAS:

Safety of Life at Sea, 1974

Security nivå 1:

Det nivået hvor et minimum av relevante security-tiltak skal opprettholdes til enhver tid.

Security nivå 2:

Det nivået hvor relevante security-tiltak skal opprettholdes for en viss tidsperiode som et resultat av øket risiko for en security-hendelse.

Security nivå 3:

Det nivået hvor relevante security-tiltak skal opprettholdes for en begrenset tidsperiode når hendelse er umiddelbar forestående eller sannsynlig.

1. Innledning

1.1 Bakgrunn

I løpet av HMS & K studiet har det vært mye fokus på helse, miljø og kvalitet. På bakgrunn av dette ble fokuset i denne hovedoppgaven sikkerhet (security).
Norge som stor sjøfartsnasjon har opp gjennom tidene hatt mye fokus på sikkerhet langs kystlinjen og til sjøs. Med tanke på landets betydelige kystlinje (ca. 22.000 km), og de mange private og offentlige havneanleggene, er det interessant å se på hvordan ulike aktører løser utfordringer knyttet til internasjonale lover, forskrifter og regler. I den forbindelse er ISPS koden et relevant regelverk, hvor det vil være spennende å se på hvordan ulike havneterminaler i Norge håndterer denne koden.

I første omgang var det meningen å skrive hovedoppgaven ved en spesifikk ISPS havneterminal som løser regelverket ved "av-på"[1] sertifisering. Det skulle fokuseres på hvordan denne havnen løser utfordringene vedrørende denne type sertifisering.
Innsyn i security-planen og sårbarhetsanalysen kunne i denne sammenheng bidratt til å gi et helhetlig bilde av havneterminalen.

ISPS koden sier (A/16.3.11, A/16.7, A/16.8 & B/16.8.6):
"Planen skal beskyttes mot uautorisert adgang eller innsyn, og tiltak for å beskytte security-relatert informasjon bør etableres… ".
På grunn av regelverket kunne ikke oppgaven løses som først planlagt, men hovedoppgavens tema skulle fremdeles være ISPS "av-på" sertifisering. Utfordringen ble da å utforme en ny oppgavetekst som vil ha en nytteverdi for flere havneterminaler som forholder seg til denne tolkningen av koden.

Det tidligere ønsket om å gå dypt ned i problematikken rundt ISPS ved en spesifikk havneterminal ble ikke mulig, fokuset ble i stedet rettet mot mer generelle problemstillinger.
I samarbeid med intern veileder ble oppgaven utvidet til å omhandle fire ulike havneterminaler i distriktet, der ønsket blant annet var å se om noen utfordringer går igjen.

[1] En ISPS-havneterminal som blir "stengt" og sikkerhetsklarert ved hvert anløp av skip som omfattes av ISPS-koden. Se punkt 1.6

Alle terminalene er såkalte ”av-på” ISPS-havneterminaler, og med tanke på utvelgelsen av disse var tjenestemenn ved Kystverket til god hjelp.

Denne omstillingsprosessen ble tidkrevende og skapte en del usikkerhet med tanke på oppgavens gyldighet. Noen positive resultater vil nok uansett komme frem av denne ”snuoperasjonen”. Resultatet av den opprinnelige oppgaven ville sannsynligvis blitt en gradert rapport pga. sensitiv informasjon om havneterminalen. Ved å gå bort ifra å arbeide med sikkerhetsplaner og sikkerhetsvurderinger, og i stedet anonymisere havneterminalene, kan rapporten forhåpentligvis brukes i et større omfang både av private og offentlige institusjoner. Utfordringer som disse fire ”av-på” ISPS havneterminalene opplever er sannsynligvis også gjenkjennelige ved andre havneterminaler i Norge. Eventuelle tiltak som blir foreslått kan forhåpentligvis myndighetene bruke i sitt videre arbeid med å øke sikkerheten og forståelsen for ISPS-koden.

Oppgavetekst

Problemstilling ble som følger:

1. Krav / retningslinjer til "av/på” havneterminaler, utfordringer i forhold til regelverket.
   Da såkalte ”av-på” havneterminaler er et spesielt fenomen ønsker vi å se nærmere på denne formen for ISPS-havneterminaler, og kartlegge eventuelle utfordringer i forbindelse med løsningen.
   Som hjelpemiddel vil vi foreta en sikkerhetsvurdering i henhold til “Et verktøy for egenkontroll av security ved en havneterminal” utgitt av Kystverket.
   Samt gjennomføre risikoanalyser (grovanalyser) av de aktuelle ISPS-havneterminalene.

2. Opplæring og krav til personell som skal ha adgang til ISPS havneterminalen.
   Hvilke løsninger har bedriftene/havneterminalene brukt for opplæring av personell som har arbeidsoppgaver i ISPS-havneterminaler.
   Spesielt problematikk knyttet til ”ikke autorisert” personell i henhold til ISPS-koden, som skal inn å gjøre en jobb av kort varighet.

1.2 Formål

På bakgrunn av grovanalyse, SWOT analyse (S=Strengths, W=Weaknesses, O=Opportunities, T=Threats) og ”Et verktøy for egenkontroll av security ved en havneterminal” er målsettingen å kartlegge utfordringer i forbindelse med ISPS ”av-på” sertifiserte havneterminaler. Verktøyene er tatt i bruk ved 4 havneterminaler, og på denne måten vil det komme frem om noen av utfordringene går igjen. Ønsket er at denne informasjonen kan komme til nytte hos andre havneterminaler som benytter seg av ”av-på” løsningen.

Gjennom kartlegging av havneterminalene har opplæring, driller og øvelser blitt vurdert. Formålet er å få en oversikt over hvordan de ulike havneterminalene har tolket og iverksatt ISPS-kodens krav. Opplæring av ”ikke autorisert” personell, dvs. personell uten sikkerhetsansvar, er en kjent utfordring. Av den grunn er ønsket å ta en gjennomgang av kravene i ISPS-koden og tolke hva koden sier om opplæring.

1.3 Hva er ISPS-koden?

ISPS-koden står for ”International Ship and Port Facility Security Code”. Koden har som hovedmål, gjennom både proaktive og operative sikringstiltak, å forhindre at skip i internasjonal fart benyttes til terrorhandlinger. Videre å begrense direkte trusler rettet mot skip og havneterminaler.
Skip som omfattes av koden er passasjerskip, lasteskip over 500 brutto registreringstonn (BRT) og mobile offshore borerigger som opererer i internasjonal fart samt havneterminaler som betjener disse, (Det Norske Veritas, 2004)

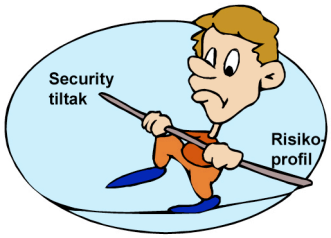
Denne oppgaven tar for seg ISPS-havneterminaler, og det vil derfor skrives om og tas hensyn til regelverk og formål med nettopp disse. I den sammenheng fokuseres det på løsningen ved ”av-på” sertifisering og hvilke utfordringer en slik løsning kan medføre.

ISPS-koden setter minimumskrav til blant annet:

- Sårbarhetsvurdering (Port Facility Security Assessment, PFSA)
- Security plan (Port Facility Security Plan, PFSP)
- Dokumentasjon (logg, vedlikehold av tekniske innretninger, tegninger og evt. kart)
- Sikkerhetsoffiser for havneterminal (Port Facility Security Officer, PFSO)
- Trening, drill og kompetansekrav

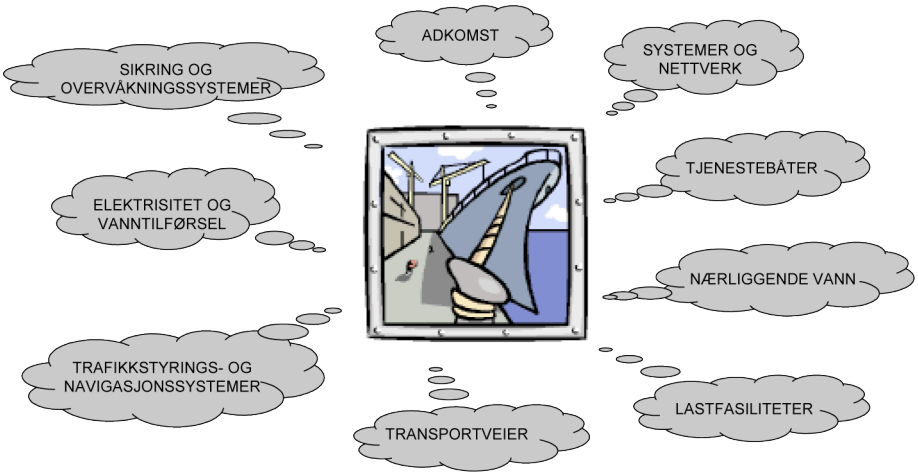
Norge har gjennom Kystverket satt noen egne minimumskrav, blant annet til adgangskontroll. I denne forbindelse har Norge sett behovet for å benytte gjerder til å avgrense de definerte ISPS-områdene, hvor koden krever at det gjennomføres adgangskontroll. Her er det verdt å nevne at ikke alle land som berøres av regelverket har definerte egne minimumskrav.

ISPS-koden er basert på moderne risikotenking og innebærer en systematisk evaluerings- og beslutningsmåte. I forbindelse med koden er security og risikoprofil sentrale elementer som må balanseres. Med dette menes blant annet at havneterminaler med lav risikoprofil, ikke nødvendigvis trenger å opprettholde de samme security-tiltakene som mer sårbare eller utsatte havneterminaler. Denne balansen skal synliggjøres gjennom havneterminalens sårbarhetsvurdering.



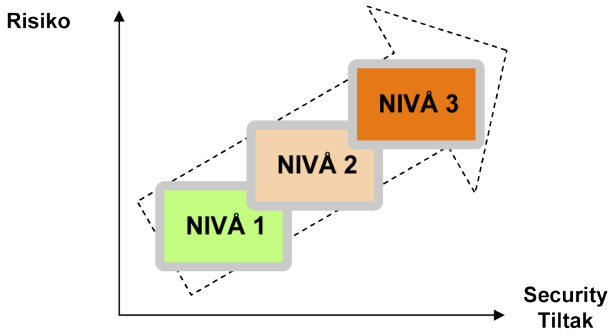
Figur 2: Risikotenking.
(Det Norske Veritas, 2004)

Samtlige havner som omfattes av ISPS-koden skal gjennomføre en sårbarhetsvurdering, bedre kjent som risikoanalyse (Det Norske Veritas, 2004). Denne vurderingen skal innbefatte havnens infrastruktur og operasjoner for å vurdere hvilke deler som er mer utsatt eller mottakelig for å bli rammet av en security-trussel. PFSA utarbeides gjennom et samarbeid mellom eksterne eksperter og internt personell. På den måten vil havneterminalen bli kartlagt på best mulig måte. Sårbarhetsvurderingen er utarbeidet med basis i den daglige drift, "business as usual", uten forhøyet trusselbilde, altså security-nivå 1. Denne vurderingen gir et grunnlag for hvilke tiltak og prosedyrer som skal gjennomføres og opprettholdes ved normal drift.



Figur 3: Objekter og infrastruktur som er viktige å beskytte i en havneterminal.
(Det Norske Veritas, 2004)

En godkjent sårbarhetsvurdering er utgangspunktet for utformingen og vedlikeholdet av security-planen, som i tillegg skal beskrive supplerende tiltak og prosedyrer som iverksettes ved Security nivå 2 og 3 (Det Norske Veritas, 2004). Både sårbarhetsvurderingen og sikkerhetsplanen er graderte dokumenter som kun autorisert personell skal ha tilgang til. Nøyaktig hvem som har tilgang til dokumentene skal angis i security-planen.



Figur 4: Sikkerhetsnivåer i forhold til risiko og tiltak.
(Det Norske Veritas, 2004)

Security-planen skal også inneholde prosedyrer for interaksjon mellom skip og havn vedrørende security. I enkelte tilfeller beskriver regelverket bruk av DoS i denne forbindelsen. DoS er et dokument som i utgangspunktet kun er relevant for skipet.

Vedrørende dokumentasjon setter koden krav til havneterminalene med tanke på loggføring, journalføring, tegninger og kart. I forbindelse med tekniske innretninger som benyttes, setter koden krav til beskrivelser og vedlikehold av disse.

Samtlige ISPS godkjente havneterminaler er pålagt å ha en sikkerhetsoffiser (PFSO), (Det Norske Veritas, 2004). PFSO er ansvarlig for utvikling, implementering, revisjon og vedlikehold av security-planen (PFSP).
I forbindelse med sikkerhetsoffiseren setter ISPS koden spesifikke ansvarsområder samt krav til opplæring av disse, (International Maritime Organization, 2003).
Koden setter også krav til opplæring og informasjon til havnepersonell og annet personell som skal utføre oppdrag ved havneterminalen.

1.4 Hvorfor ISPS?

Etter terrorangrepet mot USA 11. September 2001 satte ”International Maritime Organiszation” (IMO) i gang flere tiltak for å øke security for skip og havner. I november 2001 ble medlemslandene enstemmig enige om å utvikle nye tiltak relatert dette. Tiltakene skulle presenteres for ”Conference of Contracting Government for the Safety of Life at Sea, 1974” (SOLAS), kjent som ”Diplomatic Conference on Maritime Security” i desember 2002. Forberedelsene til konferansen ble betrodd til organisasjonens ”Maritime Safety Committee” (MSC) på basis av henstillinger gitt fra medlemslandene, offentlige (statlige) og private organisasjoner i konsultativ status med Organisasjonen.

I MSC sin første ekstraordinære samling, som også ble avholdt i november 2001 for å akselerere utviklingen og godkjenningen av de formålstjenlige security-tiltakene, ble det etablert en ”MSC Intersessional Working Group on Maritime Security”. Deres første møte ble holdt i februar 2002, og resultatene fra diskusjonene ble rapportert til, og vurdert av, den 75. sesjon av MSC i mai 2002. Der ble en ad hoc arbeidsgruppe etablert for å videreutvikle forslagene som ble lagt fram. Den 75. sesjon av MSC behandlet rapporten fra arbeidsgruppen og anbefalte at arbeidet skulle videreføres via en ytterligere ”MSC Intersessional Working Group”, denne ble avholdt i september 2002.

Den 76. sesjon av MSC behandlet resultatet fra september, og det videre arbeidet ble foretatt av ”MSC Working Group” i samsvar med ”the Commitee´s” 76. sesjon i desember 2002 umiddelbart før ”the Diplomatic Conference”. Her ble de enige om det endelige forslaget som skulle vurderes av ”the Diplomatic Conference”.

”The Diplomatic Conference on Maritime Security” som ble avholdt i London i desember 2002 innførte nye forskrifter i SOLAS og ISPS-koden[2] for å forsterke maritim security. De nye bestemmelsene setter internasjonal basis for hvordan skip og havneanlegg kan samarbeide for å identifisere og hindre security-trusler innen den maritime transportsektor.

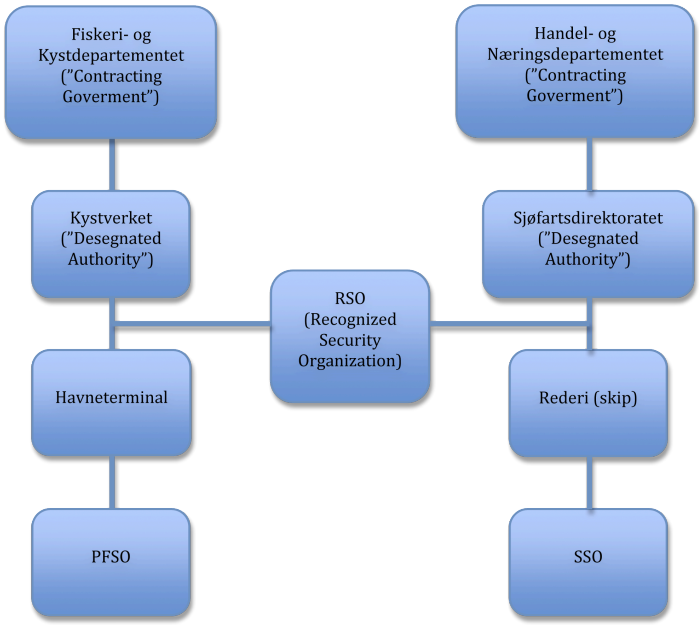
[2] Det fulle navnet til ISPS-koden er ”the International Code for the Security of Ships and of Port Facilities. I dagligtale brukes International Ship and Port Facility Security koden, som den blir omtalt i forskrift XI-2/1 i SOLAS 74, eller forkortet til ISPS-koden

1.5 Praksis og effektuering

En stor del av regelverket innenfor skipsfart utformes på den internasjonale arena. Norske myndigheter, havnemyndigheter og skipsfartsnæringen deltar i det arbeidet som gjøres internasjonalt for å styrke sikkerheten og terrorberedskapen i havner og på skip.
EU har i etterkant av arbeidet i IMO vedtatt en ny forordning, 725/2004 om tiltak for økt terrorberedskap på skip og i havneterminaler i EU-området. Denne forordningen inkluderer IMO-regelverket innenfor maritim security og er en EU tilpasning av ISPS koden. Samtidig utvider den virkeområdet og skjerper kravene til skip og havner. I Norge blir ikke innenriksfarten omfattet av regelverket etter denne forordningen, men i kraft av at regelverket er blitt utvidet vil mange av kravene bli lagt til grunn for skip og havneterminalet her til lands, (Fiskeri- og Kystdepartementet, 2005).

EU-kommisjonen la også frem et nytt havnesikkerhetsdirektiv (EU-direktiv 65/2005) som tar sikte på å utvide virkeområdet for regelverket om sikkerhet og terrorberedskap til havnene i EU-området. Dette gjelder de havner som ikke er omfattet av IMO-regelverket og forordningen (725/2004). Dette direktivet ble gjort gjeldende i 2006.

I Norge er det Fiskeri og kystdepartementet som er den overordnede forvaltningsmyndighet for havnepolitikken, det vil si ”Contracting Government” slik det er spesifisert i ISPS koden. Nærings- og Handelsdepartementet er overordnet forvaltningsmyndighet for skipsfart. Sjøfartsdirektoratet følger opp den delen av regelverket som retter seg mot skip (”Designated authority”), og Kystverket følger opp bestemmelsene vedrørende havner (”Designated authority”). Kystverket har godkjent et utvalg konsulentselskap for å gjennomføre sikkerhetsvurderinger og utarbeide sikkerhetsplaner for den enkelte havn eller havneterminal, såkalte RSO (Recognized Security Organization).



Figur 5: Myndighetshierarki i forhold til ISPS.

Anslagsvis 1000 norske skip og ca. 600 havner og havneterminaler omfattes av IMO-regelverket.

I henhold til EØS-avtalen er Norge pålagt å innføre EU-direktiv 65/2005 om bedre havnesikring og EU-forordning 324/2008 om inspeksjoner innen maritim security og terrorberedskap. Formålet med direktivet er å bidra til økt sikkerhet og terrorberedskap i de delene av havnen som ikke omfattes av ISPS-koden eller forordning 725/2004.

Havneterminaler som omfattes av "Forskrift om sikring av havner og havneterminaler mot terrorhandlinger m.v.", skal følge de relevante kravene i SOLAS kap. XI-2 og ISPS-koden del A. ISPS-koden del B er veiledende retningslinjer, dersom annet ikke er bestemt i del A.

Havner og rederier skal selv utarbeide planer i henhold til ISPS-koden.
I Norge har Kystverket ansvaret for å godkjenne havners sikkerhetsplaner, mens skipets planer godkjennes av skipets klasseselskap som har fått dette delegert fra Sjøfartsdirektoratet.

Ettersom havnene er i kommunal eller privat eie, påløper det ikke direkte investeringskostnader i forbindelse med innføringen av ISPS regelverket for Staten. Selv om havnene er i kommunalt eller privat eie fører likevel Kystverkets ansvar og oppgaver til administrative og økonomiske kostnader. Dette er i første rekke knyttet til godkjenning av havnenes sårbarhetsanalyser og sikkerhetsplaner. Utgifter knyttet til sikkerhetstiltakene i havnene dekkes inn av dem som bruker infrastrukturen.

Kostnadene ved å gjennomføre sikkerhets- og terrorberedskapstiltak ved havner og skip er anslått til å ligge rundt kr. 100.000 pr. skip, og mellom kr. 3 og 10 mill. for de største havnene. Kostnadene for de mindre havnene er anslått til å variere fra kr. 200.000 til 1 mill. Innføring av havnesikkerhetsdirektivet kan forventes å påføre havnene tilsvarende kostnader.

Det finnes ca. 600 ISPS havneterminaler i Norge. Siden det finnes mange private kaier langs kystlinjen, ble ordningen med "av-på" sertifisering en praktisk tilnærming. Det vi si at havneterminalen er lukket, klargjort og godkjent etter regelverket ved anløp av ISPS godkjent skip. Etter anløpet åpnes havneterminalen, og blir dermed klassifisert som ikke sertifisert, og kan ta imot anløp av ikke sertifiserte skip.

Før havnene kan starte arbeidet med fysiske sikkerhetstiltak må godkjenning av sårbarhetsvurdering og sikkerhetsplan foreligge. Det skal etableres sjekklister knyttet til de elementene som må godkjennes, og det skal fastsettes akseptkriterier. Akseptkriteriene skal inneholde likeverdige sikkerhetstiltak i forhold til det som er beskrevet i ISPS-koden.

Det skal verifiseres om sikkerhetstiltakene er gjennomført i havnene. Dette blir utført av Kystverket gjennom revisjoner. Godkjent havneterminal gir grunnlag for utstedelse av dokumentet "Statement of Compliance". Dette dokumentet er gyldig i 5 år fra utstedt dato.

1.6 "Av-på" ISPS-havneterminaler

"Av-på" ISPS-havneterminaler er et spesielt fenomen som ikke direkte blir omtalt i ISPS-koden. Kort fortalt går dette ut på at til daglig er havneterminalen åpen for allmenn ferdsel, så sant den ikke ligger inne på et allerede avgrenset bedriftsområde. Når det er meldt om ankomst av ISPS-skip blir havneterminalen stengt ned og kontrollert av godkjent ISPS-personell. Dette vil si at "business as usual" er security nivå 0. I ISPS-koden er security nivå 1 det laveste nivå. Løsningen blir praktisert i flere land og er internasjonalt akseptert.

Norge har ca. 600 ISPS-havneterminaler og ca. 5 millioner innbyggere. Aktiviteten på hver ISPS-havneterminal blir av den grunn liten. Geografien i Norge, sammen med få anløp, kan gjøre faste ISPS-havneterminaler lite hensiktsmessig og kan ha økonomiske konsekvenser for bedrifter.

Overvåkningsorganet ESA (EFTAs Surveillance Authority) kjenner til praksisen, men har ikke reagert på den. Løsningen med "av-på" ISPS-havneterminaler kan relateres til der koden omtaler "restricted areas, part B, 16.21" (International Maritime Organization, 2003), og videre i "Forskrift om sikring av havner og havneterminaler mot terrorhandlinger mv. 2007/825" vedlegg 5 "Gjerdestandarder" som omhandler flyttbare gjerder, (Kystverket, 2005).

1.7 Opplæring

Kodens del A punkt 18 setter krav til opplæring, driller og øvelser i havnesikkerhet. PFSO og egnet sikringspersonell skal ha kjennskap til, samt ha opplæring i henhold til retningslinjene i del B. Videre skal havnepersonell som har spesifikke security-oppgaver forstå sine oppgaver og sitt ansvar for havnesikkerheten slik den blir beskrevet i PFSP, og inneha tilstrekkelig kunnskap og ferdighet til å utføre de gitte oppgavene i henhold til retningslinjene i del B av koden.

For å sikre en effektiv implementering av PFSP skal det gjennomføres driller og øvelser med passende intervall. Dette med hensyn på type oppdrag, utskifting av security-personell, type skip terminalen interagerer med, og andre relevante forhold i henhold til retningslinjene i del B av koden.
PFSO skal sikre effektiv koordinering og implementering av PFSP ved å delta på øvelser, ref. del B av koden.

I henhold til koden Del B 18.2 bør også havnepersonell (som har spesifikke oppgaver på terminalen, sikringspersonell) ved ISPS havneterminaler ha kunnskap om og bli trent i noen eller alle av de følgende punktene:

- Kjennskap til gjeldene security-trusler
- Gjenkjenne og detektere våpen, våpendeler, farlige substanser og innretninger.
- Gjenkjenne karakteristiske tegn og atferdsmønstre til personer som kan være en trussel mot sikkerheten
- Teknikker brukt til å omgå sikkerhetstiltak
- Mengdestyring og kontrollteknikker
- Security-relatert kommunikasjon
- Bruk av security-utstyr og security-systemer
- Testing, kalibrering og vedlikehold av security-utstyr og security-systemer
- Inspeksjons, kontroll og overvåkingsteknikker
- Metoder for søk på personer, personlige effekter, bagasje, gods og skipsproviant

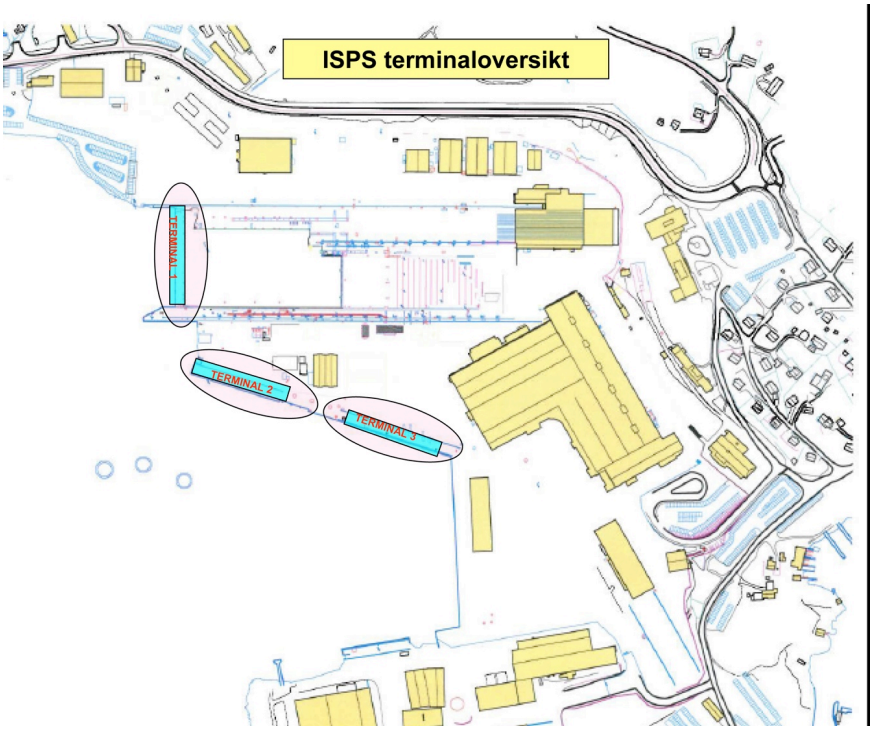
Alle (Del B, pkt 18.3) andre som er innom og gjør oppdrag på terminalen bør ha kunnskap om, og være kjent med, bestemmelser i PFSP i noen eller alle av de følgende punkter.

- Meningen og derav følgende krav i de forskjellige security-nivåene
- Gjenkjenne og detektere våpen, våpendeler, farlige substanser og innretninger
- Gjenkjenne karakteristiske tegn og atferdsmønstre til personer som kan være en trussel mot sikkerheten
- Teknikker brukt til å omgå sikkerhetstiltak

Koden sier ikke noe spesifikt om oppfølging og oppdatering av kunnskaper personell har fått via opplæring, men det bør være underforstått at all kunnskap må oppdateres og vedlikeholdes.

1.8 Beskrivelse av ISPS havneterminalene

Havn 1.



Figur 6: Oversiktsbilde havn 1

Havneterminalen (terminal 1, figur 1) har beliggenhet på dokkporten inne på et privat bedriftsområde. Det er adgangskontroll til selve bedriftsområdet med rundell og Securitasvakt, og alle ansatte har personlige id-kort. Bedriften har mange tilsette som benytter seg av dokkporten i forbindelse med gjennomferdsel når havneterminalen er av-sertifisert. Det ISPS-sertifiserte området er lite og oversiktlig med 24 timers overvåking fra Securitas vakter.

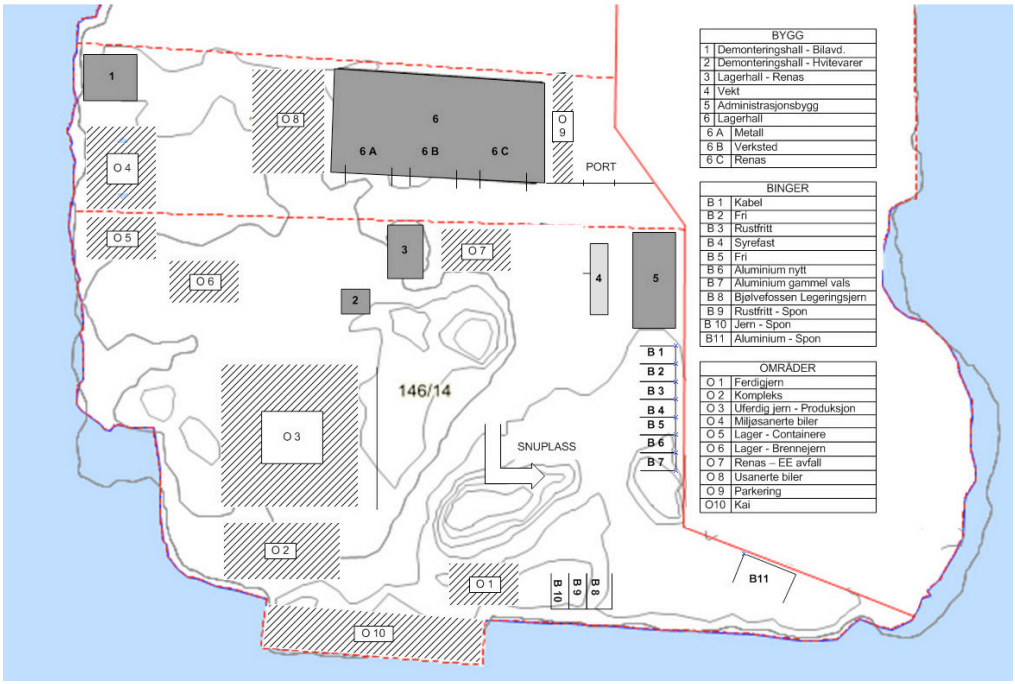
Ved på-sertifisering av området settes det opp gjerder på hver side av dokkporten. Et annet tiltak for adgangskontroll er en rondell. Pr. dags har alle ansatte tilgang til ISPS-havneterminalen med sitt eksisterende adgangskort. Ved kortvarige oppdrag inne på området blir det utlevert besøkskort. Kommunikasjonsmiddel ved anløp er mobiltelefon og maritim VHF. Maritim VHF er et internasjonalt system for kortdistanseradioforbindelse for skipsfarten på VHF båndet.

Havneterminalen har 12-18 anløp i året av skip som i hovedsak frakter stålplater og annet utstyr til arbeidet som pågår på bedriften. Terminalen tar ikke i mot forsyninger eller gods,

men dersom dette skulle være aktuelt har bedriften avtale med en annen havneterminal i nærheten.

Ved anløp er det havnearbeiderne som tar i mot skipene, men i noen tilfeller er det også annet personell inne på området som skal gjøre en jobb av kort varighet.
Når det gjelder opplæring har flertallet av havnepersonellet gjennomført kurs innenfor ISPS. Annet personell som utfører sporadisk arbeid på havneterminalen når den er på sertifisert har ikke noen form opplæring i forbindelse med koden.
Havneterminalen gjennomfører driller internt. Her deltar blant annet havnepersonell og PFSO. En gang i året deltar de også på storøvelser i samarbeid med to andre havneterminaler i nærområdet.

Havn 2



Figur 7: Oversiktsbilde havn 2.

Havneterminal nr. 2 er et privat område (figur 2). Den ligger på et industriområde med andre private bedrifter. Eneste trafikk på industriområdet er av arbeidere og besøkende til de ulike bedriftene. Hele havneterminalens område benyttes til lagring av. Det er egne gangstier frem til kaien.

Hele industriområdet er inngjerdet med bare en inngang. Inngangspartiet består av en stor port. Ved på-sertifisering av havneterminalen stenges porten, og besøkende må registreres ved adgangspunktet. Alle skip som benytter seg av havneterminalen er der i forbindelse

med levering/henting av varer fra bedriften. Det forekommer ikke andre anløp enn det som er av relevans for bedriften. Totalt er det ca. 24 skipsanløp pr. år.

Havneterminalen kan ta imot gods og proviant og det foreligger rutiner for mannskapsbytte. PFSP beskriver tiltak som gjennomføres ved slike mottak.

Alle ansatte har gjennomgått sikkerhetsopplæring slik at det aldri forekommer personell uten godkjent opplæring inne på området. I tillegg har de egne id-kort. Besøkende eller annet personell som er blitt registret ved adgangspunktet er alltid fulgt av godkjent personell fra bedriften.

I tillegg til inngjerdet og merket område, har bedriften automatiske varslingsanlegg og videoovervåkningsutstyr. Ved anløp av ISPS skip blir DoS utarbeidet og signert av representanter for havn og skip. Kommunikasjonsmiddel ved anløp er telefon og maritim VHF.
Det er PFSO som er ansvarlig for ISPS anløp, men det er alltid ekstra personell til stede etter behov.

Havn 3

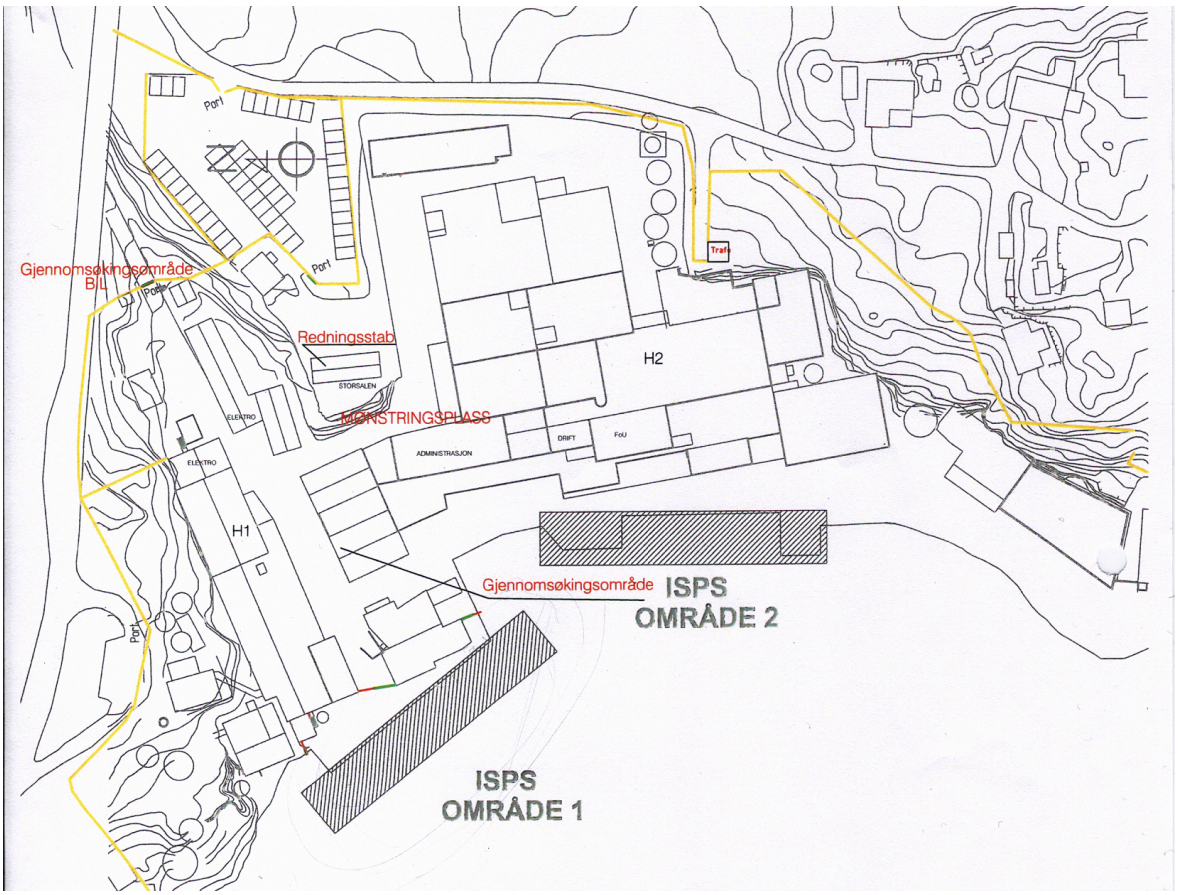
Figur 8: Oversiktsbilde havn 3.

Den tredje havneterminalen er i motsetning til de andre en kommunal havn. Beliggenheten er i et område trafikkert av fotgjengere og biler. Det ISPS sertifiserte området ved havneterminalen er oversiktlig og relativt lite, men med mulighet for at større båter kan legge til kai. ISPS-området er markert med rødt felt på figur 8.

Ved på-sertifisering av havneterminalen settes det opp områdesikring i form av gjerder. Dette plasseres et bestemt antall meter inn mot kaiområdet, og ved hver ende går gjerdet et lite stykke ut mot sjøsiden. Sistnevnte for å hindre at uautorisert personell skal kunne komme seg inn på det sertifiserte området via sjøen. Et annet tiltak er adgangspunktet som ved på sertifisering er bemannet av Securitasvakter 24 timer i døgnet. Når området er lukket er dette havneterminalens eneste adgangspunkt. For å komme gjennom denne adgangskontrollen må personellet ha et godkjent id kort. Slike kort blir også levert ut ved kortere oppdrag. Kommunikasjonsmiddel ved anløp er telefon og maritim VHF.

Havneterminalen har omtrent 20 anløp i året, og er kun trafikkert av passasjerskip og militære fartøy. I hovedsak tar ikke havneterminalen imot gods, men dersom det skulle være nødvendig blir dette håndtert manuelt.
Ved anløp er PFSO i stor grad alene om å ta imot disse, men ved behov finnes andre ressurser tilgjengelig.

Havn 4



Figur 9: Oversiktbilde havn 4

Fjerde havneterminal er en privat terminal (ISPS-område1) relatert til en fabrikk som driver med produksjon for annen industri. Denne ligger i nærheten av bebodd område. Hele industriområdet er inngjerdet, og det er elektronisk adgangskontroll med rundell. Industriområdet har i tillegg til gjerder naturlige hindringer som klipper og generelt kupert terreng.

På området er det to ISPS-havneterminaler, men bare den ene er i jevnlig bruk. Den andre er ”backup” i tilfeller der den primære terminalen er opptatt eller ikke kan benyttes. Terminal 1 er på egen kai og det er flere bygninger som virker som naturlig hinder mellom terminalen og resten av industriområdet. Ved på-sertifisering av ISPS-havneterminal blir det montert gjerder og lukking av porter mellom bygninger og sjø. Dette isolerer havneterminalen fra resten av industrianlegget. Dører fra bygningene som går ut til ISPS-havneterminalen blir også avstengt, men vinduer har ikke noen spesiell form for avlåsing.

Det er anløp av ca. 20 skip i året, +/- 5, og disse leverer kun kjemikalier/syrer til bruk i produksjonen. Hovedtyngden av anløpene skjer på kveld og natt. Operatørene har en

vaktordning der de har ansvar for ISPS-havneterminalen en uke hver. Ved anløp blir operatør på vakt varslet en time i forkant. Denne har da ansvar for å stenge av og sikkerhetsklarere terminalen.

Alle ansatte som involvert i ISPS-havneterminalen har opplæring, og resten av de ansatte får informasjon som er nødvendig (need to know) i forhold til deres virke på bedriften. Det er ingen spesielle adgangskort for de som har tilgang til ISPS-havneterminalen.

Det er ikke noen form for kommunikasjonssystemer som VHF, og det er heller ingen nødstrømanlegg for overvåkingssystemene.

Selve havneterminalen er naturlig utfor ”allfarvei” på bedriften, så en på-sertifisering vil ikke han noen form for negativ innvirkning på produksjon eller den daglige drift.

2 Metode

2.1 Kartlegging

Kartlegging er systematisk innsamling av data til analysering. Tilstanden til det aktuelle objektet blir vurdert, og det dannes deretter grunnlag for en eventuell prioritert handlingsplan til forbedringer.

Kartlegging av ISPS havneterminaler er en måte å verifisere om bedriftens effektuering samsvarer med kravene i ISPS-koden. Dette er en kvalitetskontroll av havneterminalens evne til å opprettholde de security-nivåene som koden krever. Kartleggingsrutiner er nødvendig for å systematisk følge opp og dokumentere endringer som gjennomføres ved havneterminalen. Hverdagen endrer seg og uforutsette hendelser kan oppstå. Ved systematisk gjennomgang/kartlegging av havneterminalens prosedyrer og rutiner i forhold til ISPS koden, vil havneterminalen være forberedt på utfordringer knyttet til dette.

Kartlegging er gjennomført ved alle ISPS-havneterminaler. Formålet har vært å få en generell forståelse for hvordan de ulike havneterminalene fungerer i praksis, og om dette er i samsvar med ISPS-koden. Fokuset har vært generelt på opplæring, øvelser og adgangskontroll. Spesielt på ”ikke autorisert” personell i henhold til ISPS-koden som skal inn og gjøre en jobb av kort varighet.

2.1.1 Intervju

Et intervju er en samtale mellom to personer, intervjuer og intervjuobjekt, der intervjueren spør en person om en sak for å få personens mening og synspunkter vedrørende denne saken.

Tema i intervjuene var intervjuobjektets erfaringer og opplevelse i forhold til ISPS-koden og hvordan denne koden fungerer i praksis ved de aktuelle havneterminalene. PFSO har vært intervjuobjekt ved samtlige havneterminaler og ved enkelte har også havnepersonell blitt intervjuet. Dette er personer som har spesifikke arbeidsoppgaver inne på havneterminalene når den er på-sertifisert. Ved å intervjue personell med ulike oppgaver i forbindelse med ISPS-havneterminalen, kan flere utfordringer knyttet til den praktiske gjennomføringen bli avdekket.

Brukernes subjektive tilbakemeldinger skal, sammen med bestemmelsene i ISPS-koden, danne et grunnlag for å fange opp og vurdere ulike sider ved den praktiske gjennomføringen ved de ulike havneterminalene.

Antall intervjuobjekter er forskjellig for de respektive havnene, dette på grunnlag av bedriftens størrelse.
Ved havn 1 ble tre havnearbeidere intervjuet i tillegg til PFSO.
Ved havn 2 ble en havnearbeider intervjuet i tillegg til PFSO.
Ved havn 3 og 4 ble kun PFSO intervjuet.

2.1.2 Skjema for egenkontroll av security ved en havneterminal

Kystverket har utarbeidet et skjema kalt ”Et verktøy for egenkontroll av security ved en havneterminal”, omtales videre som ”egenkontrollskjema”. Dette er ment som et hjelpemiddel for havneterminalene for å kontrollere om deres løsninger i forhold til bestemmelsene i ISPS-koden er à jour.

Skjema er fylt ut og gjennomgått i samarbeid med PFSO ved de respektive havneterminalene. Dette for å avdekke eventuelle avvik, merknader og/eller utfordringer i forhold til kravene i koden. De fire utfylte skjemaene vil settes opp mot hverandre for å se om noen av avvikene/utfordringene går igjen hos de aktuelle havneterminalene. Resultatene etter gjennomgått skjema har ikke blitt satt opp mot havneterminalens sikkerhetsplaner og sårbarhetsvurdering da regelverket setter begrensinger til innsyn.

2.1.3 Grovanalyse

Risikoanalyse er sentrale verktøy for å oppnå høy sikkerhet i tilknytning til ISPS ved havneanlegg. Analysen går ut på å identifisere hendelser som kan forekomme, sannsynligheten for hendelsene, mulige konsekvenser og hvordan hendelsene kan forebygges. Grovanalyse er en enkel og mindre kompleks risikoanalyse for å finne elementer som spesielt utpeker seg.

Figur 10: Gangen i en risikoanalyse.

Analysene gjennomføres etter nærmere bestemte prosedyrer. Resultatene av analysene sees i forhold til gitte akseptkriterier, og danner grunnlag for eventuelle tiltak (Gassnormen, 2005). Alle tiltak som reduserer sannsynligheten for eller konsekvensen av hendelsen blir dokumentert.

Ved gjennomgang av ISPS havneterminalene er det utført en grovanalyse med fokus på adgangskontroll, sikringsbarrierer, overvåkningsutstyr og automatiske varslingsanlegg. Formålet med grovanalysen har vært å gjennomgå de ulike punktene for å se på:

- Hvilke faremomenter som eksisterer
- Hva årsaken til faremomentene kan være
- Hvilke hovedeffekter faremomentene kan gi
- Hvilke konsekvenser faremomentene kan føre til
- Hvilke mulige tiltak som kan redusere faremomentene

Resultatene fra de fire havneterminalen blir gjennomgått, og risikoreduserende tiltak anbefalt.

2.1.4 SWOT-analyse

En SWOT analyse er en strategisk planleggingsmetode og hjelpemiddel brukt for å evaluere et område/tiltak sine styrker og svakheter, muligheter og hindringer. Formålet med området/tiltaket spesifiseres og interne og eksterne nøkkelfaktorer identifiseres. Fokus holdes på et tema eller område, og gunstige samt ugunstige faktorer beskrives. Analysen gir et øyeblikksbilde som kan hjelpe i begrunnelse for tiltak og prioritering (HSH Lederhuset, 2009)

- S = Strengths
  Nåværende styrker, egenskaper til objektet/område/tiltaket som gir en fordel i forhold til andre
- W = Weaknesses
  Nåværende svakheter, egenskaper til objektet/området/tiltaket som gir en ulempe i forhold til andre
- O = Opportunities
  Eksterne og interne muligheter som bør ivaretas i fremtiden
- T = Threats
  Fremtidige hindringer som det kan støtes på ved realisasjon av foreliggende muligheter, både internt og eksternt

Eksterne faktorer beskriver påvirkningen fra miljøet på organisasjonen sine muligheter og trusler fra miljøet. Eksempel på eksterne faktorer er makroøkonomiske[3] forhold, teknologiske forandringer, markedsforhold samt lovendringer nasjonalt og internasjonalt.

Interne faktorer beskriver styrkene og svakhetene internt i organisasjonen. Faktorer innad i systemet kan være personell, finans, innkjøp, produksjon osv. Det som representerer svakhet for et punkt, kan være styrke i et annet punkt.

SWOT analysene har gitt en oversikt over styrkene og svakhetene ved de ulike havneterminalene. Denne analysen er blitt utarbeidet ved hjelp av resultatene fra egenkontrollskjema, intervju og grovanalyse. De ulike utfordringene havneterminalene står ovenfor, likheter og forskjeller mellom dem, kan gi en oversikt over hvilke utfordringer som kan oppstå ved andre havneterminaler.

3 Makroøkonomi omhandler internasjonale og nasjonale økonomiske sammenhenger. I samfunnsøkonomi sees det på makroøkonomiske modeller og hvordan disse påvirker hverandre.

3 Resultat

3.1 Intervjuer

Det er fokusert på intervjuobjektets positive erfaringer ved havneterminalen, samt hvilke utfordringer og forbedringspotensialer den enkelte ser.

Havn 1:

PFSO

Tabell 1: Resultat av intervju PFSO havn 1

Positivt	Utfordringer

• Har kurs og repetisjon
• Holder seg faglig oppdatert på eget initiativ
• Årlige fellesøvelser
• Kompetente i forhold til regelverket
• Ingen økonomiske begrensninger i forhold til opplæring
• Mulighet for intern opplæring
• Samarbeid med andre ISPS-havneterminaler
	• Opplæring, trening, øvelser og kurs
	  ○ Trene mannskap som har sporadiske oppdrag innenfor terminalen
	• Få fast gruppe som drifter havneterminalen
	  ○ Stor utskifting av personell
	• Manglende ressurser
	• Størrelsen
	• Informasjonsflyt
	• Personlig oppfølging av ISPS-personell

Havnearbeider 1

Tabell 2: Resultat intervju havnearbeider 1 havn 1.

Positivt	Utfordringer
• Kursing og opplæring	• Prosedyrer og rutiner i forhold til oppgaver som skal utføres • Adgangskontroll/rondell • Portløsning • Personlig oppfølging av opplæring • Stor utskifting av personell • Ikke kurset personell som utfører oppgaver på havneterminalen • Kommunikasjon • For lite kvalifisert personell • Informasjonsflyt • Manglende deltagelse på øvelser og driller • Forståelse for kodens intensjon

Havnearbeider 2

Tabell 3: Resultat intervju havnearbeider 2 havn 1.

Positivt	Utfordringer
• Mobilitet • Tilgang til kran ved tunge løft	• Portløsning • Adgangskontroll/rondell • Informasjonsflyt • Prosedyrer og rutiner i forhold til oppgaver som skal utføres • Ferdselsvei ved av-sertifisert terminal o Manglende informasjon til personell som ikke har oppgaver i forhold til ISPS • Opplæring • Øvelser og driller

Leder

Tabell 4: Resultat intervju leder havn 1.

Positivt	Utfordringer
• Av-på løsningen i forhold til havneterminalen • Bruke andre områder • Lite og oversiktlig område • Differensierte id-kort skal innføres	• Prosedyrer og rutiner i forhold til oppgaver som skal utføres • Opplæring • Informasjonsflyt • Personlig oppfølging av opplæring • Øvelser og driller • Portløsning • Praktiske løsninger

Havn 2

PFSO

Tabell 5: Resultat intervju PFSO havn 2.

Positivt	Utfordringer
• Kurs og repetisjon • Informasjonsflyt • Differensiert kursing/opplæring • Øvelser og driller • God kontroll og lite svinn • Personell • Samarbeid med andre ISPS-havneterminaler • Personlig oppfølging av opplæring • Tilgangskontroll dagtid	• Informasjon til eksterne aktører • Belysning • Vedlikehold av systemene • Kursing og intern informasjon

Havnearbeider

Tabell 6: Resultat intervju havnearbeider havn 2.

Positivt	Utfordringer
• Øvelser og driller • Informasjonsflyt • God plass, oversiktlig	• Informasjon i forhold til kodens formål • Differensiert opplæring • Tilgangskontroll natt (reguleres i DoS)

Havn 3

PFSO

Tabell 7: Resultat intervju PFSO havn 3.

Positivt	Utfordringer
• Opplæring, øvelser og driller ○ Personlig oppfølging • Kan tilkalle ekstramannskaper • Samhandling med lignende terminaler • Informasjonsflyt • Ingen økonomiske begrensninger i forhold til opplæring og kursing	• Det er tungvint å opprette ”av-på” • Samhandling mellom båt og havn • Terminalens beliggenhet. • Stort ansvarsområde og til tider lite personell • Manglende øvelser i forbindelse med passasjertrafikk

Havn 4

PFSO

Tabell 8: Resultat intervju PFSO havn 4.

Positivt	Utfordringer
• Opplæring, øvelser og driller • God bemanning • Ingen økonomiske begrensninger i forhold til opplæring og kursing	• Følge øvelsesplan • Tilkomst til havneterminalen • Informasjonsflyt • Ingen samhandling med andre havneterminaler

3.2 Skjema for egenkontroll av security ved en havneterminal

Ut fra egenkontrollskjemaet er det fokusert på merknader (som kan utvikle seg til avvik) og sikkerhetsløsninger havneterminalen har innført.
Merknader er i henhold til skjema og ikke nødvendigvis i forhold til bestemmelsene i koden. Det er PSFO ved den respektive havneterminalen som selv har definert eventuelle merknader. Resultatene er ikke kontrollert opp mot de respektive sikkerhetsplaner, da regelverket setter begrensninger for innsyn. Av den grunn kan det ikke konkluderes om merknadene er avvik i henhold til koden.

Havn 1 (Vedlegg 11)

Terminalens security-regime:
Punkt7: Udefinert opplæring på personell som skal inn og gjøre jobb av kort varighet. Uvisst om hvordan koden skal tolkes i forhold til dette.

Adgangskontroll:
punkt 14: Kan komme i kontakt med ikke klarert personell på vei ut fra ISPS-området.
Overvåking av terminalen etc:
Punkt 3: Følgende tiltak benyttes for å overvåke terminalen og adgangen til denne; vaktpatruljer og overvåkingsutstyr
Punkt 6: Tiltak for å øke security-tiltakene ved nivå 1 og 2etc; øke intensiteten ved patruljering og tilkalle ekstrapersonell.

Kontroll av avgrensede områder:
Punkt 3: Følgende elementer er beskrevet i PFSP vedrørende avgrensede områder;

- adgangskontroll for området
- kontroll av aktivitet på området
- tiltak for å forsikre at avgrensede områder gjennomsøkes forut for og etter etablering.

Punkt 11: Følgende security-tiltak benyttes for å kontrollere adgang til avgrensede områder;

- permanente eller midlertidige barrierer rundt det avgrensede området
- adgangspunkter ikke i bruk kan avlåses
- bruk av adgangskort

- bruk av automatiske overvåkningssystemer

Punkt 12: Etablerte tiltak for å øke security i avgrensede områder i security nivå 2;

- Redusere antall adgangspunkter
- Styrke kontroll i adgangspunktet
- Begrense parkering
- Kontroll av aktivitet inne på området
- Kontinuerlig overvåking
- Begrense adgang til område nært skip

Kontroll av kommunikasjonsutstyr

Punkt 1: Er terminalens kommunikasjonsutstyr og prosedyrer for bruk av dette i samsvar med de krav som framkommer av PFSP ved security nivå 1 og 2?

Ikke etablert spesielle tiltak for kommunikasjon, bruker mobiltelefon.

Punkt 7: Forefinnes prosedyrer for å beskytte radio- og telekommunikasjons utstyr, infrastruktur og datanettverk?

- Forefinnes ikke prosedyrer for dette.

Opplæring, drill og øvelser

Punkt 3: Er PFSO, annet security personell og øvrig personell ved terminalen kjent med de oppgaver som er tillagt dem gjennom PFSP og har de mottatt tilstrekkelig opplæring i disse?

- Security personell – security-ansvarlig for opplæring
- Minstekrav – intern opplæring i bedriften
-

Diverse

Punkt 2: Terminalen har etablert prosedyrer og gjennomført tiltak som kan benyttes dersom:

- det samhandler med et skip som kommer fra en stat som ikke har innført ISPS-koden (ikke CG)
- det samhandler med et skip som ikke er omfattet av ISPS-koden
- servicefartøyer som omfattes av PFSP samhandler med stasjonære eller flyttbare plattformer eller borerigger

Havn 2 (Vedlegg 12)

Terminalens security-regime

Punkt 4: Har terminalen etablert prosedyrer i tilfelle skipets alarmsystem skulle bli aktivert?

- Ved lydalarm på båten – prosedyrer fra skipets side
  Dette har ikke vært en aktuell problemstilling

Punkt 11: Terminalen har ikke prosedyrer for fortløpende måling og revidering av effektiviteten vedrørende security-tiltakene.

Overvåkning av terminalen etc.

Punkt 3: Følgende tiltak benyttes for å overvåke terminalen og adgangen til denne
Automatiske varslingsanlegg
Overvåkningsutstyr (kamera etc.)

Punkt 6: Følgende tiltak er etablert for å øke security-tiltakene ved security-nivå 1 og 2:

- Øke intensitet ved patruljering
- Tilkalle ekstra personell
- Overvåkning

Kontroll av avgrensede områder

Punkt 2: Det er ikke identifisert avgrensede områder innenfor terminalen.

Punkt 11: Følgende security-tiltak benyttes for å kontrollere adgang til avgrensede områder:

- Permanente eller midlertidige barrierer rundt det avgrensede område
- Adgangspunkter ikke i bruk kan avlåses
- Bruk av adgangskort
- Merking av kjøretøy
- Bruk av automatiske overvåkningssystemer
- Særskilt kontroll med kjøretøy som befinner seg i nærheten av skip

Punkt 12:

Følgende tiltak er etablert for å øke security i avgrensede områder ved security-nivå 2:

- Styrke barrierer
- Styrke kontroll i adgangspunkter
- Begrense parkering

- Kontroll av aktivitet inne på området
- Kontinuerlig overvåkning
- Øke hyppighet av patruljering
- Begrense adgang til områder nært skip

Kontroll av godshåndtering

Punkt 4: Følgende tiltak benyttes for å sjekke gods:

- Visuell kontroll
- Fysisk kontroll

Kontroll av forsyninger til skipet

Punkt 4 :Følgende tiltak benyttes for å kontrollere forsyninger til skip

- Visuell kontroll
- Fysisk kontroll

Punkt 7: Dersom ikke forsyninger er forhåndsanmeldt blir varene kontrollert og agent kontaktet for verifisering.

Punkt 11: Terminalen bruker ikke skanning/annet utstyr eller hunder ved security-nivå 2.

Diverse

Punkt 2: Terminalen har etablert prosedyrer og gjennomført tiltak som kan benyttes dersom:

- det samhandler med et skip som kommer fra en stat som ikke har implementert ISPS-koden (ikke CG)
- det samhandler med et skip som ikke er omfattet av ISPS-koden
- servicefartøyer som omfattes av PFSP samhandler med stasjonære eller flyttbare plattformer eller borerigger

Havn 3 (Vedlegg 13)

Overvåking av terminalen

Punkt 3: Følgende tiltak benyttes for å overvåke terminalen og adgangen til denne:

- Vaktpatruljer
- Overvåkingsutstyr

Punkt 6: Terminalen har etablert følgende tiltak for å øke security-tiltakene ved security-nivå 1 og 2

- Øke intensitet og dekning av belysning og overvåkningsutstyr
- Øke patruljering
- Tilkalle ekstra personell
- Overvåkning
-

Kontroll av avgrensede områder

Punkt 3: Følgende elementer er beskrevet i PFSP vedrørende avgrensede områder;

- Adgangskontroll for området
- Kontroll av aktivitet på området
- Tiltak for å forsikre at avgrensede områder gjennomsøkes forut for og etter etablering.

Punkt 11: Følgende security-tiltak benyttes for å kontrollere adgang til avgrensede områder;

- Permanente eller midlertidige barrierer rundt det avgrensede område
- Vakthold ved adgangspunkter som er i bruk
- Bruk av adgangskort
- Merking av kjøretøy
- Særskilt kontroll med kjøretøy som befinner seg i nærheten av skip

Punkt 12: Terminalen har etablert følgende tiltak for å øke security i avgrensede områder ved security-nivå 2;

- Styrke barrierer
- Redusere antall adgangspunkter
- Styrke kontroll i adgangspunkter
- Kontroll av aktivitet inne på området
- Kontinuerlig overvåkning

- Øke hyppighet av patruljering
- Begrense adgang til områder nært skip

Kontroll av godshåndtering

Punkt 4: Følgende tiltak benyttes for å kontrollere gods;

- visuell kontroll
- fysisk kontroll

Kontroll av forsyninger til skipet

Punkt 4: Følgende tiltak benyttes for å kontrollere forsyninger til skipet;

- Visuell kontroll
- Fysisk kontroll

Diverse

Punkt 2: Terminalen har etablert følgende prosedyrer og gjennomført tiltak som kan benyttes dersom

- det samhandler med et skip som kommer fra en stat som ikke har implementert ISPS-koden (ikke CG)
- det samhandler med et skip som ikke er omfattet av ISPS-koden
- servicefartøyer som omfattes av PFSP samhandler med stasjonære eller flyttbare plattformer eller borerigger

Havn 4 (Vedlegg 14)

Terminalens security-regime

Punkt 8: Har terminalen spesifisert kriterier for å kunne vurdere hvordan det enkelte security personale utfører sine oppgaver?

- Skal foreta internrevisjon i nær fremtid. Usikker på om det foreligger, men temmelig sikker på at her er det et avvik.

Punkt 11: Terminalen har ikke prosedyrer for fortløpende måling og revidering av effektiviteten vedrørende security-tiltakene.

Overvåkning av terminalen

Punkt 3: Følgende tiltak benyttes for å overvåke terminalen og adgangen til denne;

- Vaktpatruljer
- Overvåkningsutstyr

Punkt 6: Følgende tiltak er etablert for å øke security-tiltakene ved security-nivå 1 og 2;

- Øke intensitet og dekning av belysning og overvåkningsutstyr
- Øke intensiteten ved patruljering
- Tilkalle ekstra personell

Punkt 7: Etablerer PFSP prosedyrer og utstyr tilstrekkelig til at en er forsikret om at overvåkningsutstyret vil fungere kontinuerlig, uavhengig av værforhold og strømbrudd?

- Nei ingen nødstrøm

Kontroll av avgrensede områder

Punkt 10: Dersom automatiske overvåkningssystemer er installert, varsler de et kontrollsenter kapabel til å respondere på en slik alarm?

- Nei, kamera har kun visuell kontroll

Punkt 11: Følgende security-tiltak benyttes for å kontrollere adgang til avgrensede områder;

- Permanente eller midlertidige barrierer rundt det avgrensede område
- Vakthold ved adgangspunkter som er i bruk
- Adgangspunkter ikke i bruk kan avlåses
- Bruk av adgangskort
- Merking av kjøretøy
- Bruk av automatiske overvåkningssystemer
- Særskilt kontroll med kjøretøy som befinner seg i nærheten av skip

Punkt 12: Følgende tiltak er etablert for å øke security i avgrensede områder ved security nivå 2;

- Redusere antall adgangspunkter
- Styrke kontroll i adgangspunkter
- Kontroll av aktivitet inne på området
- Kontinuerlig overvåkning
- Øke hyppighet av patruljering
- Begrense adgang til områder nært skip

Kontroll av kommunikasjonsutstyr

Punkt 1: Terminalen har ikke tilgang til kommunikasjonsutstyr utover telefoner.

Punkt 2: Terminalen er ikke utstyrt med alternative kommunikasjonssystemer for intern og ekstern bruk som er raskt tilgjengelige uavhengig av security-nivå, værforhold eller strømbrudd på security-nivå 1 og 2.

Punkt 3: Personalet ved terminalen er ikke gitt tilstrekkelig opplæring i bruken av kommunikasjonsutstyret.

Punkt 5: Det forefinnes ikke prosedyrer for å forsikre at kommunikasjonsutstyret kontrolleres og vedlikeholdes.

Opplæring, drill og øvelser

Punkt 4: Det avholdes ikke security-driller minst hver tredje måned og security-øvelser minst en gang i året med ikke mer enn 18 mnd mellom hver øvelse.

Diverse

Punkt 2: Terminalen har etablert prosedyrer og gjennomført tiltak som kan benyttes dersom:

- det samhandler med et skip som kommer fra en stat som ikke har implementert ISPS-koden (ikke CG)
- det samhandler med et skip som ikke er omfattet av ISPS-koden
- servicefartøyer som omfattes av PFSP samhandler med stasjonære eller flyttbare plattformer eller borerigger

3.3 Grovanalyse

Resultatene er tatt direkte ut fra selve grovanalysen.

Havn 1, stor privat bedrift**:**

Tabell 9: Grovanalyse Havn 1

Fare	**Årsaker**	**Hovedeffekter**	**Konsekvens**	**Mulige Tiltak**
Uautorisert personell inne på området	Portløsning/gjerdet	Fare for at gjenstander / personer til terrorvirksomhet kan komme ombord	Terror	Rulleport
	Tilgangskontroll			Rundell Kortidentifisering
	Visuell kontroll (vakter)			Fast vaktoppsett ved ISPS anløp
	Video- overvåkning			Bevisstgjøring og opplæring
Ikke opplært ISPS personell	Økonomi	Ingen prioritering av opplæring	Kurs blir nedprioritert og personell får ingen kurstilbud	Legge kursing inn i budsjettet
	Manglende intern kursing	Manglende opplæring innen ISPS	Manglende kunnskap og forståelse for ISPS	Kursing, opplæring / informasjon, øvelser
Størrelsen på området	Smal port	Fri tilgang til området	Må flytte gjerder for å komme inn – området blir åpent	Rulleport Mer bruk av stor kran

Havn 2, mindre privat bedrift med hele bedriftsområdet som ISPS-havneterminal**:**

Tabell 10: Grovanalyse Havn 2

Fare	**Årsaker**	**Hovedeffekter**	**Konsekvens**	**Mulige Tiltak**
Uautorisert personell på havneterminal	Tilgang via naboeiendom	Fare for at ukjente gjenstander evt. personell til terrorvirksomhet kommer ombord. Uautorisert personell på området	Terror	Belysning
	Dårlig adgangskontroll			Informasjon til nabobedrifter
	Dårlig oversikt			Kursing, opplæring / informasjon, øvelser
	Vanskelig å kontrollere / ”vaske” området			Flere som foretar sikkerhetsklarering (kvalitets-kontroll)

Havn 3, kommunal havn**:**

Tabell 11: Grovanalyse Havn 3

Fare	**Årsaker**	**Hovedeffekter**	**Konsekvens**	**Mulige Tiltak**
Uautorisert personell / utstyr inne på området	Tilgangs kontroll	Fare for at personer / gjenstander til terrorvirksomhet kan komme ombord	Terror	Mer enn en på vakt.
				Videokontroll
	Bebyggelse			Bevisstgjøring og opplæring
		Stor trafikk av uautorisert personell	Forstyrrende elementer	Tydeligere merking med skilt når man nærmer seg området
Plassering av område	Oppbevaring av sikringsutstyr	Svekket barriere	Terror	Sikker oppbevaring

Havn 4, mellomstor privat bedrift**:**

Tabell 12: Grovanalyse Havn 4

Fare	**Årsaker**	**Hovedeffekter**	**Konsekvens**	**Mulige Tiltak**
Uautorisert personell / utstyr på havneterminal	Tilgangskontroll	Fare for at personer / gjenstander til terrorvirksomhet kan komme ombord	Terror	Rundell
	Usikrede utganger til havneterminal			Sikre dører og vinduer som mot ISPS området.
	Strømbrudd			Nødstrømsystem
Kommunikasjon	Manglende VHF	Ingen kommunikasjon	Informasjons-flyt/alarm	Ta i bruk VHF
Ikke opplært ISPS personell	Økonomi	Ingen prioritering av opplæring	Manglende kunnskap og forståelse for ISPS	Kursing, opplæring / informasjon, øvelser
	Manglende driller og øvelser	Manglende forutsetning for arbeidet som skal gjennomføres		

3.4 SWOT-analyse

SWOT-analysen er utarbeidet ut i fra de tre andre metodene (grovanalyse, egenkontrollskjema og intervju). Resultatene lister opp hovedmomentene fra analysen.

Havn 1:

Tabell 13: SWOT-analyse havn 1.

SWOT analyse operasjon:	
Styrker (hva er bra?)	**Svakheter (hva kan bli bedre?)**
Terminalen er et lite område, god oversikt for visuell kontroll, samt sikkerhetsklarering. Området er godt merket og avskjermet. System for Id-kontroll er under utarbeidelse.	Portløsningen er problematisk på grunn av størrelse, kan være en utfordring ved enkelte typer arbeide For lettvint tilgang for uautorisert personell på området Inngjerding av området Informasjonsflyten er mangelfull. Området er fritt ferdselsområde ved av-sertifisering.
Muligheter (er det noe vi bør satse mer på?)	**Trusler (finnes det noe som kan true våre mål?)**
Opplæring/kursing av personell, slik at de som jobber på kaien har ISPS opplæring Tilgangskontroll Informasjonsflyt – hvorfor ISPS Bruk av stor kran	Fare for uautorisert adgang fra sjøsiden Terror Uautorisert personell på området

Styrker:

- Lite område
- God oversikt - visuell kontroll - sikkerhetsklarering
- Id-kontroll
- God avskjerming og merking

Svakheter:

- Portløsning
- Adgang til område
- Informasjonsflyt
- Ferdselsområde ved av sertifisering

Muligheter:

- Opplæring/kursing av personell
- Tilgangskontroll

- Informasjonsflyt
- Kran

Trusler:

- Fare for uautorisert adgang fra sjøsiden
- Uautorisert personell på området

Havn 2:

Tabell 14: SWOT-analyse havn 2.

SWOT analyse operasjon:	
Styrker (hva er bra?)	**Svakheter (hva kan bli bedre?)**
Hele området blir ISPS-havneterminal ved anløp av skip. Naturlig avgrensing. God og tydelig merking både på land og fra sjø. Alle ansatte er ISPS klarerte. Adgangskontroll - dagtid	Dårlig oversikt pga lagring på kai, sikkerhetsklareringen kan bli en utfordring. Nærliggende industri.
Muligheter (er det noe vi bør satse mer på?)	**Trusler (finnes det noe som kan true våre mål?)**
Adgangskontroll – natt Lyssetting	Uautorisert personell inne på området. Fare for uautorisert adgang fra sjøsiden

Styrker:

- Hele bedriftsområdet ISPS sertifisert havneterminal
- Naturlig avgrensing
- God merking fra land og sjøsiden
- Alle ansatte er ISPS klarerte
- (Adgangskontroll – dagtid)

Svakhet:

- Dårlig oversikt – sikkerhetsklarering
- Nærliggende industri

Muligheter:

- Adgangskontroll – natt
- Lyssetting

Trusler:

- Uautorisert personell på området
- Fare for uautorisert adgang fra sjøsiden

Havn 3:

Tabell 15: SWOT-analyse havn 3.

SWOT analyse operasjon:	
Styrker (hva er bra?)	**Svakheter (hva kan bli bedre?)**
Oversiktlig og lite område med god plass. Lett å utføre sikkerhetsklarering. Området er godt merket fra land og sjø. Inngjerding og adgangskontroll er bra. Tilgang på ISPS klarert personell.	Oppbevaring av sikringsutstyr for område. Sterkt trafikkert havn (offentlig havn)
Muligheter (er det noe vi bør satse mer på?)	**Trusler (finnes det noe som kan true våre mål?)**
Finne en annen og sikrere oppbevaring av sikringsutstyr. Øvelser innen passasjertrafikk	Stor befolkningstetthet med mye trafikk av både fotgjengere, biler og båter. Når det ikke er ISPS-område er det et offentlig område med fri tilgang for befolkningen. Fare for uautorisert adgang fra sjøsiden

Styrker:

- God oversikt – sikkerhetsklarering – god plass
- God merking fra land og sjøsiden
- Inngjerding
- Adgangskontroll
- Tilgang på ISPS klarert personell

Svakheter:

- Oppbevaring av sikringsutstyr
- Sterkt trafikkert havn

Muligheter:

- Oppbevaring av sikringsutstyr
- Øvelser innen passasjertrafikk

Trusler:

- Offentlig område – høy befolkningstetthet
- Fare for uautorisert adgang fra sjøsiden

Havn 4:

Tabell 16: SWOT-analyse havn 4.

SWOT analyse operasjon:	
Styrker (hva er bra?)	**Svakheter (hva kan bli bedre?)**
Lite område. Naturlig avgrensing. God og tydelig merking både på land og fra sjø.	Bygg naturlig "sperre". Sikring av vinduer
Muligheter (er det noe vi bør satse mer på?)	**Trusler (finnes det noe som kan true våre mål?)**
Kommunikasjonsutstyr Nødstrømsystem Samarbeid med nærliggende havneterminaler Intern revisjon	Uautorisert personell inne på området. Fare for uautorisert adgang fra sjøsiden

Styrker:

- Lite område – naturlig avgrensing – kupert terreng
- God merking fra land og sjøsiden

Svakheter:

- Bygg naturlig avgrensing - sikring av vinduer

Muligheter:

- Kommunikasjonsutstyr
- Nødstrømsystem
- Samarbeid med nærliggende havneterminaler
- Intern revisjon

Trusler:

- Uautorisert personell på området
- Fare for uautorisert adgang fra sjøsiden

4 Diskusjon

4.1 Intervju og ”egenkontrollskjema”

Resultatene fra intervjurundene kommer under den andre delen av oppgaveteksten som omhandler opplæring. Her er det intervjuobjektenes subjektive oppfatninger som vil være utgangspunktet for diskusjonen.
I egenkontrollskjema kommer utfordringer vedrørende opplæring og informasjon også frem. I tillegg vil andre momenter i forhold til regelverket bli tatt opp i diskusjonen.

Det er verdt å nevne at denne informasjonen ikke har blitt satt opp mot beskrivelsen i havneterminalenes PFSP, men at kravene i koden er kjent. Dette kan gjøre det mulig å vurdere om kravene er fulgt på grunnlag av intervjuobjektenes uttalelser og resultatene etter gjennomgangen av ”egenkontrollskjema”.

Del A i koden inneholder krav, Annex 1 forteller at PFSO, havnepersonell og annet personell som utfører oppgaver ved havneterminalen skal ha opplæring og trening med utgangspunkt i retningslinjene gitt i del B. Del B inneholder veiledninger til gjennomføring av kravene beskrevet i del A.

Havn 1

Det lagres LNG/LPG i nærhet av havneterminalen. Denne er bygget inn med diker og betongvegger. Dersom denne blir utsatt for sabotasje tilsier tankens størrelse sammen med dens barrierer, at det mest sannsynlig ikke vil skape noen direkte fare for personell og skip som befinner seg ved havneterminalen. Ved en eventuell hendelse kan muligens stråling fra B.L.E.V.E.[4] bli et problem.

Gjennomgangen av intervjuene og ”egenkontrollskjema” viser at det er en del utfordringer som går igjen. Havn 1 er en godkjent ISPS-havneterminal med bakgrunn i PFSP, men enkelte av sikringspersonellet ved havneterminalen føler ikke at de innehar nok kunnskap og opplæring i henhold bestemmelser og anbefalinger i koden. Dette kan bunne i at ISPS er en liten del av den daglige driften og dermed får lavere prioritet. Lav prioritet kan føre til en dårlig informasjonsflyt som i verste fall kan skape usikkerhet vedrørende viktigheten og

[4] Boiling Liquid Expanding Vapor Explotion/fireball

formålet med ISPS. I denne forbindelse sier koden tydelig at alle involverte parter skal inneha kunnskap om ISPS, (International Maritime Organization, 2003).
Punkt 7 under "Terminalens security-regime" i "egenkontrollskjema" omhandler opplæringskrav for security-personell. I henhold til koden skal dette være beskrevet i PFSP. PFSO sier dette står i PFSP, men gir uttrykk for usikkerhet vedrørende opplæring av personell som skal inn og gjøre en jobb av kort varighet (personell uten security-ansvar). Usikkerheten blir også uttrykt fra havnepersonell som har security-ansvar på havneterminalen. Del B punkt 18.3 i koden gir anbefalinger om hvilke emner personell uten security-ansvar skal ha i de tilfeller de må inn på terminalen og utføre et arbeidsoppdrag.
En stor del av personellet inne på havneterminalen utfører sporadisk oppdrag som ikke er security relatert. I henhold til koden bør derfor også disse ha kjennskap til relevante punkter i PFSP[5].

I tillegg til kravene i koden holder PFSO seg faglig oppdatert på egent initiativ. Mulighet for benyttelse av PFSO sine kunnskaper kan være positivt med tanke på intern opplæring. Samtidig mangler enkelte av sikringspersonellet kurs, opplæring, øvelse, driller eller en oppdatering av disse. Sikringspersonell som har gjennomført opplæring i henhold til koden savner personlig oppfølging og faglig påfyll. Koden setter krav til opplæring, øvelser og driller, men ikke til personlig oppfølging eller oppdatering (fornying av opplæringen). Havneterminalen er selv ansvarlig for at aktuelt personell innehar nødvendig kunnskap og kompetanse.

Del A i koden setter krav til at øvelser skal gjennomføres ved passende intervaller. Bedriften gjennomfører årlige fellesøvelser i samarbeid med andre ISPS-havneterminaler i distriktet. Dette kan ha positiv innvirkning med tanke på erfaringsoverføring. Bedriften setter ingen økonomiske begrensinger i forhold til opplæring, øvelser og driller. Pr. dags dato gjennomføres det ikke intern opplæring ved bedriften.

Prosedyrer og rutiner i forhold til oppgaver som skal utføres på havneterminalen skal stå beskrevet i PFSP. Alle som har arbeidsoppgaver inne på havneterminalen bør ha kjennskap til og delvis innsyn i denne planen. Enkelte av sikringspersonellet ved denne havneterminalen kjenner ikke til prosedyrer eller rutiner knyttet til egne arbeidsoppgaver

[5] Se denne rapport pkt 1.7

inne på området. Del A pkt 16.3 i koden setter minimumskrav til hvilke prosedyrer PFSP skal inneholde.

En annen utfordring bedriften opplever er utskiftning av personell samt manglende ressurser. Stor utskiftning av personell kan føre til usikkerhet knyttet til utførelse av arbeidsoppgaver ved havneterminalen, som igjen kan føre til uønskede hendelser. Mangel på ressurser kan bunne i lav prioritet i forbindelse med ISPS, noe som kan resultere i at sikringspersonellets arbeidsoppgaver ikke blir utført i henhold til kravene i koden.

Havneterminalen er liten og oversiktlig, noe som kan gjøre sikkerhetsklareringen enklere. Det er to adgangspunkter, en for større gjenstander som skal fraktes inn/ut av havneterminalen (port) og en annen for personell (rundell). Porten oppleves i noen tilfeller som utfordrende med tanke på størrelsen. Til tider er det store gjenstander som skal transporteres inn/ut av havneterminalen. I disse tilfellene må porten og deler av gjerdet demonteres. Dette kan resultere i uønskede hendelser. Havneterminalen har tilgang til en større kran som kan brukes ved tunge løft, og muligens ikke krever demontering av port og gjerder.

Rundellen er under utvikling. Pr dags dato har alle ansatte ved bedriften tilgang til området med sitt personlige adgangskort. Egne adgangskort for personell som har opplæring i henhold til PFSP er under utarbeidelse. Dette kan bidra til å gjøre adgangskontrollen bedre og mer oversiktlig.

I de tilfeller havneterminalen er av-sertifisert brukes dokkporten som ferdselsvei til andre områder på bedriften. Ved på-sertifisering oppstår det derfor frustrasjon og irritasjon. Dette kan bunne i blant annet manglende informasjon til ansatte vedrørende kodens intensjon og dens praktiske gjennomføring ved bedriften.

Bedriften har ingen spesielle tiltak for intern kommunikasjon utover bruk av mobiltelefon. Det foreligger heller ikke prosedyrer for beskyttelse av radio- og telekommunikasjonsutstyr. Ved svikt i primærkommunikasjonsmidler kan kommunikasjon mellom security-personell og skip bli en utfordring.

Havn 2

Det er ikke etablert prosedyrer for fortløpende måling og revidering av effektiviteten vedrørende security-tiltakene. Kodens del B punkt 16.8.7. anbefaler dette. Slike prosedyrer kan være med på å skille ut hvilke security-tiltak som er effektive.

Havneterminalen samarbeider med andre ISPS-havneterminaler i forhold til øvelser m.v. Et slik samarbeid kan bidra til blant annet bedre erfaringsoverføring mellom havneterminalene. Opplæring, øvelser og driller er i henhold til koden, og det gis personlig oppfølging, noe som kan sikre god informasjonsflyt vedrørende ISPS ved bedriften. Likevel ses det forbedringspotensial.
PFSO ved bedriften har ønske om at alt personell som berøres av koden skal få muligheten til å delta på kurs utviklet i samarbeid med RSO. Den praktiske gjennomføringen med tanke på administrative og økonomiske konsekvenser, kan bli en utfordring for bedriften. Sikringspersonell ønsker en mer differensiert opplæring i forhold til koden, og videre bedre informasjon om kodens formål. Dette ulike behovet kan bunne i svekket oppfølging av enkeltpersonell om hvilket opplæringsbehov disse har.

Nærliggende bedrifter kan skape utfordringer med tanke på områdesikring grunnet manglende forståelse og kunnskap om ISPS, selv om hele området er tydelig merket. Del A pkt. 16.3.2 i koden stiller krav til områdesikring. Hvis det oppstår tilfeller hvor denne blir utilstrekkelig, er det bedriftens ansvar å iverksette tiltak for å opprettholde sikringen i henhold til koden.

Havneterminalens sikringspersonell opplever ISPS-terminalen oversiktlig. Området er relativt stort med en del lagret metall. Da det er lagret mye i høyden kan belysning være en utfordring med tanke på visuell kontroll. Skjema for egenkontroll viser at havneterminalen bruker videoovervåkning. Dårlig belysning kan redusere effekten av videoovervåkingen.

Havneterminalen har ett adgangspunkt med bemannet adgangskontroll på dagtid. Ved nattestid leveres portnøkkelen til skipets sikringsansvarlig. Dette kan oppfattes som uansvarlig og skape usikkerhet blant sikringspersonellet. Denne løsningen er sannsynligvis beskrevet i PFSP og regulert i DoS, men likevel reagerer personellet ved havneterminalen på ordningen. Dersom det skulle oppstå en uønsket hendelse i forbindelse med denne ordringen, er det havnen som står ansvarlig.

Etter etablering av ISPS-havneterminal har bedriften merket nedgang i svinn og fått bedre kontroll med varestrømmen. Dette kan relateres til områdesikring og økt kontroll.

Havn 3

Det kommer frem at opplæring, driller og øvelser er i henhold til koden bestemmelser, og PFSO opplever den personlige oppfølgingen som god.
Pr. dags dato mangler havneterminalen øvelser og driller som omfatter passasjertrafikk. Likevel gis det ikke uttrykk for at det forefinnes noen økonomiske begrensninger i forbindelse med opplæring, driller og øvelser.
Havneterminalen har god samhandling med lignende terminaler for å få erfaringer som de selv kan dra nytte av.

PFSO har eneansvar på havneterminalen. Dette kan medføre stort ansvarsområde, og til tider mangel på personell. Gjennom samarbeid med nærliggende ISPS havneterminaler er det mulighet for å få hjelp fra godkjent personell ved behov. I forkant av anløp er det ikke alltid like lett å vite hvilke ressurser som trengs
ISPS-havneterminalen oppleves som tungvint å etablere da beliggenheten er i sentrum, med trafikk av mennesker og kjøretøy. Informasjon ut til befolkningen kan være en utfordring da ISPS ikke er allmenn kjent, og publikum ikke har forståelse for avstengingen.
Ved opprettelse av havneterminalen har PFSO mulighet til å tilkalle ekstra mannskaper fra andre kommunale organisasjoner. Disse har faste arbeidsoppdrag og oppdrag som krever umiddelbar innsats. Dette kan være utfordrende med tanke på at personellet ikke nødvendigvis er tilgjengelig ved behov.

Internt i bedriften oppleves informasjonsflyten som god. I forhold til interaksjon mellom båt og havn kan kommunikasjonen oppleves som en utfordring, da forståelsen for hverandres ansvarsområder ikke alltid er like god.Kommunikasjon mellom skip og havn er viktig. Lite fokus og forståelse for ansvarsområder kan resultere i uønskede hendelser.

Havn 4

Havneterminalens beliggenhet ut mot sjøsiden kan oppleves som utfordrende med tanke på anløpene. I forhold til uvedkommende kan dette være en naturlig hindring, noe som igjen kan gjøre sikkerheten ved havneterminalen bedre samt enklere å vedlikeholde.

Bedriften har etablert en øvelsesplan som er i henhold til PFSP, men praktiske årsaker gjør at denne ikke alltid er like lett å følge. Dette til tross for at det ikke foreligger noen økonomiske begrensinger i forhold til opplæring, driller og øvelser. En årsak til manglende oppfølging av øvelsesplanen kan bunne i lav prioritering da ISPS kun er en liten del av PFSO sine daglige arbeidsoppgaver. Lav prioritering kan føre til dårlig informasjonsflyt, som igjen kan skape usikkerhet vedrørende viktigheten og formålet av ISPS.

Havneterminalen har hatt en fellesøvelse med andre nærliggende havneterminaler i distriktet, men PFSO opplever ikke dette som god nok samhandling med andre havneterminaler. Samarbeid mellom havneterminaler kan gi erfaringsoverføring og bedre forståelsen for viktigheten av ISPS. Selv om det ved denne bedriften ikke foreligger noen økonomiske begrensinger i forhold til ISPS, vil et samarbeid i tillegg til faglig også gi økonomisk gevinst.

PFSO opplever bemanningsløsningen som god. Bedriften har en fast gruppe med godkjent personell som ivaretar havneterminalen i henhold til PFSP. Med bedre samhandling med andre havneterminaler kan løsningen videreføres til disse. En stabil gruppe kan gjøre personellet tryggere på at de utfører arbeidsoppgavene på havneterminalen i henhold til gjeldende regelverk.

Kriterier vedrørende vurdering av security-personalets utføring av sine oppgaver er ikke etablert. Bedriften skal foreta en internrevisjon i nær framtid for å få dette på plass. Kodens del B punkt 16.8.2 anbefaler at dette blir gjennomført. Manglende oppfølging av personellet og deres utførelse av arbeidsoppgaver, kan skape usikkerhet med tanke på om arbeidsoppgavene blir utført i henhold til kodens bestemmelser og anbefalinger. Det kan også skape usikkerhet med hensyn på om personellet er trygge i utførelsen av sine arbeidsoppgaver. En slik rutine kan gi grunnlag for kontinuerlig forbedring av sikkerheten ved havneterminalen.

4.2 Grovanalyse

Havn 1

Det foreligger muligheter for at uautorisert personell kan komme inn på havneterminalen, dette med hensyn på visuell og fysisk kontroll. I de tilfeller der større gjenstander skal inn på området må gjerdet demonteres, og den fysiske kontrollen blir av den grunn ikke tilstrekkelig. Pr. dags dato har alle på bedriften tilgang til terminalen med det eksisterende id-kortet. Dette skal forbedres i nær fremtid da ISPS-sikringspersonell skal ha egne kort som kun gir dem adgang til terminalen i de tilfeller ISPS-skip ligger til kai. Det nye systemet er under utvikling og skal effektueres i nær fremtid.

Den visuelle kontrollen foregår primært med videoovervåking, og personell står Securitas for. Denne kontrollen er avhengig av årvåkenheten til den ansatte som er satt til å betjene denne, og det er mange moment som kan spille inn i forhold til effekten av overvåkingen. Dette er en liten del av arbeidsoppgavene Securitas-personellet gjennomfører på bedriften. Andre oppgaver kan flytte fokuset bort fra ISPS-havneterminalen.

Det er personell som utfører sikkerhetsrelaterte oppdrag på ISPS-havneterminalen som ikke føler de har god nok opplæring i forhold til kodens bestemmelser. Årsaken til dette kan være økonomiske forhold og manglende intern kursing og opplæring. ISPS er en liten del av den daglige driften, og dette kan være en av grunnene til manglende fokusering på dette. Dette kan skape usikkerhet blant de ansatte vedrørende formålet med og viktigheten av ISPS.

Havn 2

Bedriften ligger i nær tilknytning til andre bedrifter som ikke har noe forhold til ISPS. Dette kan skape problemer i de tilfeller nabobedrifter lagrer materialer langs muren som skiller havneterminalen og de omliggende bedriftene. I de tilfelle slike problemer oppstår, kan dette bli en juridisk utfordring for de involverte partene.
Da det er lagret store mengder metall på området kan dette gi utfordringer i forhold til sikkerhetskontroll av området ved anløp av ISPS-skip. Mengden metall gir også begrensninger i forhold til oversikt og generell visuell kontroll.
På kveld og natt er ikke sikringspersonell fra havneterminalen til stede, og tilgangskontroll er pr. definisjon overført til skipets mannskap. Nøkkel til port blir utlevert SSO. Skipets mannskap er da selv ansvarlige for sikring av havneterminal og skip. Dette kan være en utfordring da det sannsynligvis er forskjeller i effektuering av security-tiltak for havn og skip.

Havn 3

Dette er en kommunal havn med beliggenhet nær sentrum. Effekten av dette er stor trafikk av biler og personer med liten eller ingen forståelse for ISPS. Nedstenging av området kan derfor skape irritasjon. Når havneterminalen etableres opprettes kontrollpunkt med 24 timers bemanning. Dette kan være med på å minske faren for at uautorisert personell tar seg inn på det sertifiserte området.

Det etableres ett adgangspunkt ved på-sertifisering. Denne plasseres i sørenden av havneterminalen. Selve det sertifiserte området er langt, og visuell kontroll ved nordenden kan derfor bli en utfordring.

Sikringsutstyret som brukes til blant annet områdesikring ved havneterminalen oppbevares på offentlig område uten kontinuerlig tilsyn. Dette kan skape mulighet for hærverk og annet form for sabotasje, noe som kan føre til svekket barriere.

Havn 4

Havneterminalen har beliggenhet inne på et sikret bedriftsområde. Havneterminalens områdesikring består blant annet av to bygg som er en naturlig hindring. Dette kan gjøre adgangskontrollen vanskelig med tanke på usikkerheten knyttet til sikring av vinduer.

Terminalen er videoovervåket, men bedriften har ikke nødstrøm tilknyttet havneterminalen. Ved strømbrudd vil videoovervåkningen falle bort, da vil den visuelle kontrollen bli betydelig redusert.

Sikringspersonell kommuniserer ved bruk av mobiltelefoner internt og eksternt. Det foreligger ingen alternative kommunikasjonssystemer som eksempelvis VHF. Dersom mobilnettet har problemer kan dette føre til betydelige utfordringer knyttet til kommunikasjon.
Som tidligere nevnt så har ikke havneterminalen noen utstrakt form for samarbeid med andre terminaler. Dette kan påvirke gjennomføringen av driller og øvelser ved terminalen, noe som igjen kan resultere i nedprioritering av disse. Et samarbeid mellom ISPS-havneterminaler kan gjøre det lettere for de respektive terminalene å gjennomføre de pålagte driller og øvelser.

5 Konklusjon

Det er ikke egne regler for praktiseringen av ”av-på” havneterminaler. Dette er en tolking av regelverket, og samme krav stilles til denne praktiseringen som til faste ISPS-havneterminaler.[6]
Det er en del felles utfordringer som tas opp hos de respektive havneterminalene. Dette går spesielt på opplæring. Fellestrekk ved de fire havneterminalene er at ISPS er en liten del av den daglige driften. Prioritering av opplæring, inkludert driller og øvelser, blir påvirket av dette. Det er viktig å få frem at sårbarhetsvurderingen er individuell, basert på de faktiske forholdene ved havneterminalen.

Havn 1

Oppbevaringen av LPG/LNG nær havneterminalen er godt sikret og vil sannsynligvis ikke være noen fare for havneterminalen.

Intervju, ”egenkontrollskjema” og grovanalysen viser at utfordringene hos havneterminalen er spesielt knyttet til opplæring og informasjon til sikringspersonell. Det kommer frem at dette skaper usikkerhet hos personellet om hvor vidt de utfører oppdragene i forhold til krav og anbefalinger i regelverket.

ISPS er en liten del av PFSO sin arbeidsdag og får av den grunn liten prioritet. Dette blir videreført nedover i systemet og resulterer i at sikringspersonell ikke oppfatter kodens formål eller tar ISPS på alvor.

En stor del av aktiviteten inne på havneterminalen er av ansatte uten security-ansvar. Disse skal ha informasjon om kodens formål og delvis innsyn i PFSP, (International Maritime Organization, 2003). Dette gjennomføres ikke ved denne bedriften. Personell med security-ansvar påpeker blant annet dette.

Det er stor utskiftning av security-personell, noe som vanskeliggjør muligheten for fast personell med faste rutiner som er trygge på den jobben de er satt til å utføre.

[6] Samtale Sveinung Hustoft 8.4.2011

Problematikken i forhold til store gjenstander som skal inn og ut av ISPS-området er en utfordring bedriften bør løse. Porten er i noen tilfeller for liten og må demonteres ved inn- og uttransportering av større utstyr. Dette svekker terminalens barriere og av den grunn reduseres sikkerheten.

Bedriften har selv oppfattet problematikken rundt adgangskontrollen for personell (rundellen). Her er det iverksatt tiltak for å bedre denne. Når denne løsningen er effektuert vil adgangskontroll med tanke på personell komme opp på et akseptabelt nivå.

Når havneterminalen er av-sertifisert brukes område (dokkporten) som ferdselsvei for mange av de ansatte ved bedriften. Ved på-sertifisering skaper dette irritasjon hos de ansatte. Dette er det vanskelig å gjøre noe med, men med utstrakt informasjon om ISPS så vil forståelsen for nedstengingen bli bedre.

Bedriften har videoovervåking som betjenes av Securitas-personell i hovedvakta. Det er sporadisk visuell kontroll av monitorer, men med tanke få anløp er det ikke formålstjenlig å ha kontinuerlig videoovervåking av havneterminalen. Dagens løsning er adekvat da havneterminalen er liten og svært oversiktlig, noe som er med på å forenkle blant annet sikkerhetsklareringen i forkant av anløp. I tillegg er området godt merket fra land og sjø.

Havn 2

Samarbeidet med andre ISPS havneterminaler gir stor mulighet for faglig oppdatering og kompetanseoverføring. Utfordringer en terminal opplever vil sannsynligvis gå igjen også hos andre havneterminaler.

Informasjonsflyten ved bedriften er god. Det er viktig at dette får videre fokus for å kontinuerlig vedlikeholde kunnskapen hos de ansatte vedrørende ISPS.

De ansatte er fornøyde med opplæringen, men ønsker en mer differensiert opplæring. PFSO vil ha lik opplæring på alle sine ansatte. Dette viser at det foreligger ulik oppfatning av behovet for opplæring i henhold til koden.

Det kommer frem at bedriften har vanskeligheter med å få nærliggende bedrifter til å forstå formålet med ISPS og områdesikringen. Informasjon vedrørende ISPS eksternt bør bli bedre.

En styrke er at hele bedriftsområdet stenges ned ved på-sertifisering. Dette fører ikke til misforståelser internt i forbindelse med nedstengingen, da alle ansatte har opplæring i ISPS koden. Området er også godt merket fra land og sjø.

Sikringspersonellet opplever området som oversiktlig selv om det er lagret store mengder metall på området. Grunnet store mengder metall kan bedriftsområdet oppfattes som uoversiktlig, men sikringspersonellet er godt kjent på sin arbeidsplass og føler seg trygge på at sikkerheten er i henhold til koden. Grunnet stort lager av metall blir belysningen negativt påvirket og det oppleves at belysningen ikke er tilstrekkelig. Maksimalt utbytte av videoovervåkning er avhengig av god belysning.

Adgangskontroll på dagtid fungerer bra. Ved kveld/natt blir nøkkelen til porten utlevert til skipets mannskap. Dette oppleves som utilstrekkelig i henhold til ISPS-koden. Denne løsningen blir avtalt i en DoS. En slik avtale er i hovedsak mest formålstjenlig for skipet.

Havn 3

Opplæring, driller og øvelser er i henhold til kodens bestemmelser, men det er ønske om øvelse og driller rettet mot passasjertrafikk.
Havneterminalen har en god samhandling med lignende terminaler. Samtidig gjennomføres det øvelser og driller i samarbeid med nærliggende ISPS havneterminaler.

PFSO har eneansvar ved anløp på terminalen. Dette oppleves i noen tilfeller som svært utfordrende for PFSO. Selv om han har tilgang på godkjent personell ved behov, er det ikke alltid mulig å vite på forhånd hvilke ressurser som er nødvendig.

Beliggenheten er i mange tilfeller en utfordring når ISPS-havneterminalen skal etableres. Havneterminalen er lang og adgangspunktet blir plassert på den ene enden. Dette vanskeliggjør visuell kontroll ved den andre enden av terminalen. Likevel er det svært oversiktlig da det ikke lagres noe på området. Sikkerhetsklarering i forkant av anløp blir dermed lettere. Samtidig er området godt merket fra land og sjø.

Befolkningens forståelse for avstenging av området er liten selv om området er godt merket. Årsaken til dette er at ISPS ikke er allment kjent. Uautorisert personell som befinner seg rundt/utenfor havneterminalen er det lite å gjøre noe med da havnen er offentlig.
Sikringsutstyret er lagret på offentlig sted, noe som gjør det utsatt for skadeverk. Denne løsningen bør revurderes.

Intern informasjonsflyt i bedriften er god, men kommunikasjon mellom havn og skip har forbedringspotensial.

Havn 4

Havneterminalens beliggenhet er god med tanke på naturlige barrierer og at hele bedriftsområdet er sikret med faste gjerder. Dette opprettholder sikringen rundt havneterminalen på en god måte. Områder er godt merket fra land og sjø. En del av områdesikringen rundt havneterminalen består av faste bygg. Dette er en god løsning dersom en ser bort fra usikrede vinduer. Dette bør utbedres.

Øvelsesplanen beskrevet i PFSP blir ikke alltid fulgt. Dette resulterer i at sikringspersonell ikke får nødvendig øvelse i viktige momenter knyttet til ISPS. Årsaken til dette er lav prioritering vedrørende ISPS, da dette er en liten del av den daglige driften.

Havneterminalen har et forbedringspotensial med tanke på samarbeid med andre havneterminaler i forbindelse med øvelser og erfaringsoverføring.
Bedriften har en stabil gruppe av personell med security-ansvar og formell opplæring. Dette er positivt for bedriften og for de ansatte.

Rutiner vedrørende oppfølging av security-personell er ikke etablert, men bedriften skal gjennomføre en intern revisjon for å få dette på plass.

Bedriften har videoovervåking, noe som gjør den visuelle kontrollen god. Ved brudd på strømnettet vil videoovervåkningen kuttes, da det ikke foreligger noen form for nødstrøm. Den visuelle kontrollen vil da bli betydelig redusert.

Bedriften benytter kun mobiltelefon ved intern og ekstern kommunikasjon. Det forefinnes ikke noen form for sekundære kommunikasjonsmidler, som for eksempel VHF. Ved svikt i mobilnettet vil kommunikasjonen bli redusert.

6 Tiltak

Gjennom denne prosessen har det kommet frem at flere av haveterminalene opplever felles utfordringer. Dette i forhold til opplæring og informasjon til ansatte som ikke har direkte security-ansvar på havneterminalen. Et generelt tiltak til dette kan være å innføre informasjon om ISPS i eksisterende HMS opplæringsplan og HMS-håndbok.

Selv om koden ikke sier noe spesifikt om hvor ofte det bør gjennomføres oppfriskning av kunnskaper vedrørende ISPS, anbefales det å beskrive dette i opplæringsplanen. Skjema utgitt av IMO (IMO International Maritime Organization, 2010) er i godt hjelpemiddel i så henseende.

Foreslåtte tiltak må hver havneterminal sette opp mot eksisterende PFSP og PFSA for å vurdere om de er relevante i forhold til disse. I denen prosessen kan en handlingsplan være til god hjelp.

Handlingsplan for havneterminal xxxxxxx					
Prioritet	Objekt/Operasjon/Infrastruktur	Tiltak	Antatt kostnad	Tidsfrist	Ansvar

Figur 4: Handlingsplan i forhold til ISPS.
Plan for iverksetting av tiltak.
(Det Norske Veritas, 2004)

Havn 1

Bedriften bør gjennomgå PFSP grundig i forhold til opplæring, driller, øvelser og informasjon. Opplæring av personell som utfører oppdrag av kort varighet skal stå beskrevet i PFSP. Planen skal beskrive opplæring i forhold til personell uten security ansvar. Personell som utfører oppdrag av kort varighet kommer inn under denne kategorien. Det som står beskrevet i planen må gjennomføres.
Et alternativ kan være å implementere informasjon vedrørende ISPS i den generelle HMS opplæringen og HMS-håndboken ved bedriften. I så tilfelle må dette beskrives i PFSP. Problematikken rundt ferdselsvei vil også bli bedret ved å innføre informasjon om ISPS i HMS opplæringen og HMS-håndboken.
Videre har det kommet fram at PFSO holder seg godt faglig oppdatert, og innehar betydelig kompetanse relatert til ISPS. Det anbefales å benytte PFSO til intern opplæring i større grad.
Et annet tiltak kan være å utarbeide arbeidslister over personell som skal inn på havneterminalen og gjøre en jobb av kort varighet. Dette vil forenkle security-personellets arbeid med tanke på oversikt over hvem som skal befinne seg på havneterminalen.

Personell med security-ansvar har gitt uttrykk for at de ikke innehar nok kunnskap eller kompetanse vedrørende koden. Koden sier ikke noe om hvor ofte en bør oppdatere opplæringen, men underforstått stilles det krav til at personell skal ha oppdatert kunnskap om ISPS. Det anbefales derfor å utarbeide en ny opplæringsplan i samarbeid med security-personellet. Dette for å sikre at opplæringen er i henhold til regelverket, og at alle parter med security-ansvar er innforstått med hva som står beskrevet i PFSP.

Gruppen av ansatte som har security-ansvar med tilhørende opplæring i henhold til koden er for liten. Med tanke på stor utskiftning bør denne gruppen utvides for å sikre at det alltid er opplært personell som utfører oppdrag inne på havneterminalen.

Porten er i mange tilfeller lite hensiktsmessig. Det bør vurderes å bytte ut den eksisterende porten med en stor rulleport. En slik løsning vil opprettholde barrieren på en bedre måte. Hyppigere bruk av kran kan løse noen av utfordringene knyttet til dette.

Bedriftsområdet er stort og det bør være mulighet for kommunikasjonsutstyr som primært brukes til kommunikasjon mellom security-personell og eventuelt anløpende skip. Her kan VHF være en god løsning.

Havn 2

Det anbefales å opprettholde og videreutvikle samarbeidet med ISPS havneterminaler i nærområdet.

Bedriften bør i samarbeid med de ansatte kartlegge behovet for opplæring i ISPS, dette med tanke på de ansattes ønske om differensiert opplæring. Det anbefales å forsette å fokusere på den gode interne informasjonsflyten ved bedriften.

Informasjonen til omliggende bedrifter bør bedres for å øke deres forståelse vedrørende områdesikring og ISPS. Det anbefales å opprette en god dialog vedrørende ISPS slik at problemer med tanke på områdesikring m.v. ikke oppstår.

Belysningen på området bør bedres. Dette vil gi større effekt av blant annet videoovervåkningen.

Rutiner i forbindelse med utlevering av nøkkel til port oppleves som utilstrekkelig og bør forbedres. Det anbefales å undersøke mer om hva DoS regulerer og hvilket utbytte havneterminalen får gjennom denne.

Havn 3

Det anbefales å utarbeide en plan for øvelser og driller rettet mot passasjertrafikk i samarbeid med lignende havneterminaler. Eksisterende praksis med tanke på samarbeid med nærliggende havneterminaler bør opprettholdes.

Kommunikasjon mellom havn og skip bør bedres. Ved bedre kommunikasjon med anløpende skip vil PFSO i større grad se behovet for personell og andre nødvendige ressurser.

Adgangspunktets plassering bør vurderes. Det vil være mer formålstjenlig dersom dette blir plassert midt på terminalen da visuell kontroll vil bli bedre.

På grunn av fare for skadeverk på sikringsutstyret bør dette sikres på en bedre måte. Et alternativ kan være å låse utstyret inn i en bod på kaiområdet.

Havn 4

Det anbefales å gjennomføre sikring av vinduer som vender ut mot havneterminalen. Hvilken løsning som passer best, eller om dette er nødvendig, bør bedriften selv vurdere opp i mot PFSA.

Bedriften bør iverksette utstrakt samarbeid med andre nærliggende havneterminaler i forhold til øvelser. Dette vil bidra til å gjøre det enklere å følge øvelsesplanen i PFSP.

Planlagt internrevisjon bør effektueres snarest mulig. Dette for å sikre blant annet oppfølging av security-personell.

Vedrørende videoovervåkning og nødstrøm bør bedriften vurdere nødvendigheten av dette opp mot PFSA.

For å sikre god kommunikasjon bør bedriften vurdere behov for VHF. Et slik kommunikasjonsutstyr vil sikre kommunikasjonen mellom havn og skip også ved evt. brudd i mobilnett.

Referanser

Det Norske Veritas. (2004). *Håndbok til innføring av ISPS*. Ålesund: Kystverket.

Stortingsmelding Nr.14

På Den Sikre Siden-Sjøsikkerhet Og Oljevernberedskap, (2005).

HSH Lederhuset. (2009). *Swot-analyse.* Retrieved 01/15, 2011, from http://www.lederhuset.no/eway/default.aspx?pid=279&trg=Content_6448&Content_6448=6469:0:10,2048:1:0:0:::0:0

Guidelines on Security-Related Training and Familiarization for Port Facility Personell, (2010).

International Maritime Organization. (2003). *ISPS cod*e (2003rd ed.). London: International Maritime Organization.

KYSTDIREKTORATET MINIMUMSKRAV TIL SIKRINGSTILTAK VED NORSKE ISPS-HAVNETERMINALER, (2005).

Vedlegg

Vedlegg 1 Intervju PFSO havn 1

Vedlegg 2 Intervju Havn 1 havnearbeider 1

Vedlegg 3 Intervju Havn 1 havnearbeider 2

Vedlegg 4 Intervju Havn 1 havnearbeider 3

Vedlegg 5 Intervju PFSO havn 2

Vedlegg 6 Intervju Havnearbeider havn 2

Vedlegg 7 Intervju PFSO havn 3

Vedlegg 8 Intervju PFSO havn 4

Vedlegg 9 Samtale med Bodhild Bang, Politiet 310111

Vedlegg 10 Samtale med Sveinung Hustoft, Kystverket

Vedlegg 11 EGENKONTROLL AV SECURITY VED EN HAVNETERMINAL havn 1

Vedlegg 12 EGENKONTROLL AV SECURITY VED EN HAVNETERMINAL havn 2

Vedlegg 13 EGENKONTROLL AV SECURITY VED EN HAVNETERMINAL havn 3

Vedlegg 14 EGENKONTROLL AV SECURITY VED EN HAVNETERMINAL havn 4

Vedlegg 15 Grovanalyser

Vedlegg 16 Swotanalyser

Vedlegg 17 Veiledning Morten Lossius 13012011

Vedlegg 18 Veiledning Morten Lossius 03022011

Vedlegg 19 Veiledning Morten Lossius 030311

Vedlegg 20 Veiledning Morten Lossius 31032011

Vedlegg 21 Veiledning Morten Lossius 15042011

Vedlegg 22 Møte Kystverket 07022011

Vedlegg 23 Gannt diagram