SINTEF

SINTEF IKT

Postadresse: 7465 Trondheim
Besøksadresse: S P Andersens v 15
7031 Trondheim
Telefon: 73 59 30 00
Telefaks: 73 59 43 02

Foretaksregisteret: NO 948 007 029 MVA

SINTEF RAPPORT

TITTEL

Oppfølging av arbeidsseminar om IKT-sikkerhet i Integrerte Operasjoner

FORFATTER(E)

Martin Gilje Jaatun, Stig Ole Johnsen, Maria B. Line og Odd Helge Longva

OPPDRAGSGIVER(E)

Forskningsrådet, OLF

RAPPORTNR.	GRADERING	OPPDRAGSGIVERS REF.	
SINTEF A1550	Åpen		
GRADER. DENNE SIDE	ISBN	PROSJEKTNR.	ANTALL SIDER OG BILAG
Åpen	9788214040609	90D205	8
ELEKTRONISK ARKIVKODE		PROSJEKTLEDER (NAVN, SIGN.)	VERIFISERT AV (NAVN, SIGN.)
tiltak.doc		Martin Gilje Jaatun	Thor Myklebust
ARKIVKODE	DATO	GODKJENT AV (NAVN, STILLING, SIGN.)	
	2007-06-08	Eldfrid Ø. Øvstedal, forskningssjef	

SAMMENDRAG

Den 30/11-2006 ble det på initiativ fra SINTEF avholdt et arbeidsseminar om IKT-sikkerhet i integrerte operasjoner hos Oljedirektoratet (OD) og Petroleumstilsynet (Ptil) i Stavanger, hvor også Oljeindustriens Landsforening (OLF) og Statnett deltok i arrangementskomiteen.

Arbeidsseminaret tok opp til diskusjon en rekke strategisk viktige temaer. Resultatene fra gruppe-diskusjonene bør dermed få innvirkning på prosesser som OLFs videre arbeid med IKT-sikkerhet, ODs arbeid og Ptils utvikling av en strategi for forvaltning og oppfølging av IKT-sikkerhet i petroleums-virksomheten.

Vedlagte forslag til tiltak er basert på sluttrapporten fra arbeidsseminaret og etterfølgende diskusjoner med OLF.

STIKKORD	NORSK	ENGELSK
GRUPPE 1	Informasjonsteknologi	Information Technology
GRUPPE 2	Informasjonssikkerhet	Information Security
EGENVALGTE	Integrerte operasjoner	Integrated Operations

INNHOLDSFORTEGNELSE

1 Bakgrunn

Arbeidsseminaret om IKT-sikkerhet i integrerte operasjoner [1] ble avholdt den 30/11-2006 hos Oljedirektoratet og Petroleumstilsynet i Stavanger, i regi av Oljeindustriens Landsforening (OLF), Oljedirektoratet (OD), Petroleumstilsynet (Ptil) og SINTEF.

OLF, OD og Ptil spiller viktige roller som premissgivere for initiativer og policyutvikling mht ulike aspekter av IKT-sikkerhet. Samtidig må aktørene ut fra sine ulike ståsteder reagere og iverksette hensiktsmessige initiativer i forhold til den utvikling som skjer i industrien og i samfunnet for øvrig.

Målet for seminaret var å:

- Skape oppmerksomhet om informasjonssikkerhet i ulike miljøer (IKT, HMS, automasjon og drift) som er involvert i prosesskontroll- og boresystemer.
- Skape en arena for kunnskapsutveksling og nettverksbygging mellom relevante fag- og forskningsmiljøer
- Identifisere behov for tiltak, herunder forskning og kompetanseutvikling, industri- og myndighetstiltak

Seminaret fokuserte på systemer som benyttes til styring av integrerte operasjoner. Det omfatter generelle administrative IKT-systemer som er koplet opp mot kontroll og sikkerhetssystemer[1].

Seminaret samlet 46 deltakere fra olje- og gassindustrien (Statoil, Hydro, BP, ConocoPhillips, OLF), leverandørbedrifter (ABB, Kongsberg Maritime, Siemens), kraftbransjen (SKS, Statnett), offentlige etater (Ptil, OD, NSM/NorCERT) og forskningsmiljøer (HiA, HiG, FFI, IFE, DNV, IRIS, UiS, SINTEF).

Arbeidsseminaret tok opp til diskusjon en rekke strategisk viktige temaer. Resultatene fra gruppediskusjonene bør dermed få innvirkning på prosesser som OLFs videre arbeid med IKT-sikkerhet, ODs arbeid og Ptils utvikling av en strategi for forvaltning og oppfølging av IKT-sikkerhet i petroleumsvirksomheten.

Vedlagte forslag til tiltak er basert på sluttrapporten og diskusjoner i OLFs arbeidsgruppe for informasjonssikkerhet på møtet 15/3-2007.

2 Prosessen i arbeidsseminaret

Seminaret startet med innlegg fra Gunnar Berge (Oljedirektoratet) og Thore Langeland (OLF), fulgt av foredrag om SCADA systemer. Deltakerne ble deretter delt i fem grupper for diskusjoner av utvalgte utfordringer fram til lunsj (gruppearbeid I). Temaene var:

- Kommunikasjonsgap – forskjellig kultur, holdninger og kunnskap
- Indikatorer for oppfølging og måling av sikkerheten
- Hendelseshåndtering og definering og klassifisering av IKT-hendelser
- Sikkerhet innbygget i systemarkitektur

[1] I Norge brukes forkortelsen SAS (Safety and Automation Systems) som en samlebetegnelse på kontroll- og sikkerhetssystemene, det samme omtales ofte som SCADA (Supervisory Control and Data Acquisition) internasjonalt. For sikkerhetssystemene brukes ofte forkortelsen SIS som står for Safety Instrumented System.

- Sikkerhet ved informasjonsdeling i nett

Basert på diskusjonene i gruppene, framkom det forslag til nye tema (gruppearbeid II), som skulle ende opp i forslag til tiltak og videre arbeid.

2.1 Gruppearbeid I – Forslag til videre tema etter første gruppearbeid

Under er listet opp forslagene fra gruppearbeid I til tema for gruppearbeid II. Etter avstemning blant deltakerne ble følgende tema valgt for behandling i gruppearbeid II:

1. Tiltak for å redusere kommunikasjonsgap, eks. prosessforståelse og opplæring. Økende krav til flerfaglighet – forståelse for "hvorfor?"
2. Hvordan håndtere gamle eksisterende systemer og konverteringer. (How to handle legacy systems and migration path)
3. Hva skal til for å nå fase 2 i IO?
4. Hvordan få til rapportering av uønskede IKT-hendelser?
5. Kategorisering av (IKT/SCADA) systemer

De tema som ikke samlet nok støtte til videre utdyping var:

- Integrering av web-tjenester og sikkerhetsstandarder i en overordnet systemarkitektur
- Utarbeid en felles tillitsarkitektur (m/myndighet) for å muliggjøre adgangskontroll og rollebasert informasjonsdeling på tvers av organisasjoner
- Interessekonflikt eller samarbeid mellom ulike miljøer
- Indikatorer I: Videre arbeid med self-assessment skjema for sikkerhet i SCADA og måling av sikkerhetskultur
- Indikatorer II: Etablering av erfaringsdatabaser ved tekniske målinger på SCADA-systemer ved sikkerhetsbrudd
- Indikatorer III: Indikatorer/måleparametre for konsekvenser av sikkerhetsbrudd i SCADA-systemer
- Risikomodellering – proaktive modeller

2.2 Gruppearbeid II – Oppsummering av konklusjoner fra arbeidsseminaret

Under er oppsummert konklusjonene (som korte nøkkelfraser) som kom fram som referat fra gruppearbeid II.

1. Det må trenes og folk må møtes sosialt for å bygge tillit – trene på kommunikasjon mellom typer mennesker og fag/profesjoner/roller.
2. Vi trenger flere ingeniører som snakker både prosesstyring og IT! Dette er en utfordring til utdanningsinstitusjonene.
3. Definere hva som er god praksis. Man ønsker praktiske løsninger og svar på spørsmålet: Hva er den anbefalte måten oljebransjen gjør dette på? Dette må spres slik at man kan få kommentarer.
4. Fortsette arbeid med begrepsapparat. Man legger forskjellig betydning i ordene. Ønsker forskningsprosjekter støttet av EU for å få på plass ontologi.
5. Kjør flere pilotprosjekter. Man opplever motvilje – mange er redde for at ting skal gå galt. Pilotprosjekter kan vise at det fungerer.
6. Skape en kultur for rapportering
7. Opplysning om hendelser/erfaringslæring
8. Samle inn god praksis med hensyn på rapportering og håndtering av hendelser.
9. Risikovurderinger på tjeneste/funksjonsnivå
10. Referansearkitektur for å sette krav til komponenter/delsystemer
11. Referansemodeller for grenseflatene mot andre systemer
12. Sertifisering som en del av kategorisering
13. Myndighetene må sette klarere krav (tre-partssamarbeidet)

SINTEF har tatt tak i alle disse konklusjonene og andre momenter og forslag som kom fram i løpet av arbeidsseminaret. SINTEF har, basert på sluttrapporten [1], laget en mer strukturert og systematisk liste over anbefalte tiltak som presenteres i det følgende.

3 Anbefalte tiltak

Konkret arbeid med sikkerhet i gruppene ble godt mottatt, og vi ser behovet for periodiske samlinger med fokus på å etablere god praksis og enes om tiltak som kan forbedre sikkerheten i bransjen. Våre forslag til videre arbeid er listet opp under. Dette ble også presentert i møte med OLFs arbeidsgruppe for informasjonssikkerhet den 15/3 2007.

3.1 Tiltak som initieres av SINTEF

I det følgende identifiseres tiltak som SINTEF vil initiere og gjennomføre i regi av eksisterende eller nye forskningsprosjekter i samarbeid med bransjen. Det er imidlertid viktig at også industrien bidrar til disse prosjektene, for å sikre den nødvendige forankring og implementering av resultater.

3.1.1 God praksis for rapportering av IKT-hendelser

En ønsker å skape en kultur for rapportering av uønskede IKT-hendelser som kan støtte erfaringslæring i bransjen. Viktige aktiviteter som er foreslått for å styrke rapporteringskulturen er å samle god praksis for rapportering og håndtering av uønskede IKT-hendelser, i tillegg til å lage beskrivelser av uønskede IKT-hendelser, gode historier og opplysning om hendelser for å få styrket forståelsen av hva som kan gå galt. Forskningsrådsprosjektet IRMA er allerede i gang med innsamling av god praksis, og vil lage en håndbok basert på dette i 2007. Det vil i samme periode vurderes om det er grunnlag for å definere ett (eller flere) oppfølgerprosjekt(er) til IRMA som kan ta dette videre.

3.1.2 Indikatorer for oppfølging av informasjonssikkerhet

Vi ser et behov for å etablere felles måleparametere for informasjonssikkerhet i bransjen. Hensikten er å kunne følge opp hvordan ulike tiltak påvirker sikkerhetsnivået, hvilke tiltak som har størst lønnsomhet, og hvilke konsekvenser sikkerhetsbrudd i SCADA-systemer fører til. Per i dag er bruken av slike indikatorer lite utbredt, men det er interesse i bransjen for å se nærmere på dette. OLF har laget et sett av (prosess) indikatorer, i forbindelse med innføring av OLF retningslinje 104 – ISBR, et "self assessment tool". SINTEF har publisert artikler om indikatorer [2], vi har blitt invitert til internasjonale konferanser for å fortelle om vår erfaring, og ønsker å bearbeide dette ytterligere gjennom forskning i samarbeid med næringen.

3.1.3 Sikkerhet og semantisk web

Semantisk web vil bli viktig i arbeidet med å få integrerte operasjoner på plass, og en bør være i forkant med å analysere de sikkerhetsmessige utfordringene knyttet til dette. Samling av informasjon/data ved hjelp av semantisk søking/semantisk web innebærer bl.a.

- at data/dokumenter gjøres tilgjengelige og søkbare
- at relasjoner mellom data beskrives og er søkbare
- at dette gjøres dels innen egen organisasjon, dels i lukkede nett med andre organisasjoner, dels åpent på internett
- at det må etableres et informasjonssikkerhetsregime som ivaretar informasjonssikkerhet, dvs konfidensialitet, integritet og tilgjengelighet i tillegg til sikkerhet
- at rettigheter i form av tilgang til og bruk av dokumenter/data må ivaretas

- at informasjonssikkerhetsnivået/rettighetsnivået for kombinasjoner av data/dokumenter ivaretas, inklusive deres innbyrdes og eksterne relasjoner. Dette må ivaretas både for de enkelte elementer og for ensemblet. Det kan for eksempel bety at en samling av åpne dokumenter til sammen må gis spesielle rettigheter og høyere sikkerhetsgradering enn hvert enkelt dokument.

SINTEF ønsker å initiere et forskningsprosjekt innen dette området, og er i ferd med å sondere terrenget for å etablere et konsortium som kan søke penger fra Petromaksprogrammet i Forskningsrådet.

3.1.4 Risikovurderinger av systemene og kategorisering (klassifisering)

Den finnes metoder for risikovurderinger, men de har en lang rekke svakheter når man skal vurdere sikkerheten ved Integrerte Operasjoner (IO). IO innebærer løpende endringer med innføring av ny teknologi, fjernarbeide, samarbeid mellom forskjellige organisasjoner opp mot sikkerhetskritiske prosesser med eksplosive gasser/væsker. Dagens metoder integrerer ikke godt nok et MTO helhetssyn, eller bruk av ikke-liniære ulykkesmodeller og resilience, ref [3]. Prosjektet IOSafe ved NTNU/SINTEF/IFE ønsker å jobbe med dette i samarbeid med industrien.

Vi ønsker også å arbeide konkret med eksisterende metoder for risikovurderinger av sikkerhet på tjeneste-/funksjonsnivå som er egnet for bruk i petroleumssektoren, hvor vi utnytter nye og eksisterende modeller. Det er etablert flere prosjekter som støtter dette bl.a. ved NTNU og ved IO-senteret hvor prosjektet IOSafe foreslår å lage "Top ten vulnerabilities of SCADA and ICT systems" i samarbeid med industrien. SINTEF ønsker også å etablere "Normer for kategorisering og klassifisering av systemer" i samarbeid med OLF.

3.2 Tiltak som bør initieres av andre

Følgende tiltak er det ikke naturlig at SINTEF initierer, men SINTEF kan bidra i større eller mindre grad. SINTEF kan rimeligvis ikke pålegge noen aktører å ta ansvar for slike tiltak, så i det følgende indikeres det hvilken aktør SINTEF mener det *er naturlig* at tar ansvar for det enkelte tiltak.

3.2.1 Etablere DFU (Definerte Fare og Ulykkeshendelser) for IKT

Vi ser et klart behov for å skape bedre risikoforståelse (proaktivt) og forståelse av hvilke konsekvenser (reaktivt) en uønsket IKT-hendelse kan få for HMS. Vårt forslag er at bransjen lager en DFU hvor uønskede IKT-hendelser inngår, eventuelt i kombinasjon med andre forhold slik at vi kan trene på en situasjon som kan utvikle seg til en storulykke. Vi foreslår at man benytter STEP-metoden for å dokumentere scenarier. SINTEF vil bemerke at scenarier beskrevet via STEP med uønskede IKT-hendelser er planlagt til å inngå i neste versjon av CRIOP, se [4].

Ansvar: OLF, spesifikt OLFs arbeidsgruppe om informasjonssikkerhet. SINTEF vil bidra.

3.2.2 Sertifisering

Vi ser et klart behov for å etablere rutiner for testing og sertifisering av SCADA-systemer, slik at en dokumenterer sikkerhetsnivået når man i forbindelse med integrerte operasjoner øker graden av sammenkopling mellom SCADA-systemer og den generelle IKT-infrastrukturen. Mange gamle SCADA-systemer kan låse seg eller stoppe opp dersom de blir utsatt for høy trafikkbelastning fra IKT-nettet. SCADA-systemene synes å være lite robuste for trafikkbelastning som kommer fra IKT-nett, eller de kan være sårbare for tjenestenektangrep (DoS – Denial of Service), se [5] for

dokumentasjon. Det er verdt å merke seg at standarden IEC 61508 (som omhandler teknisk sikkerhet) ikke dekker informasjonssikkerhet, heller ikke i den nye versjonen som er på trappene.

Ansvar: Ansvarsplassering må diskuteres – det kan være en offentlig etat via Ptil, OLF eller en oppgave som settes bort til DNV eller andre anerkjente aktører som arbeider med sertifisering. Dette kan også startes opp som en forskningsoppgave i samarbeid med operatører og leverandører av SCADA- systemer, hvor en kan teste ut problemstillingen på norsk sokkel og identifisere mulige tiltak. SINTEF kan bidra, både i forbindelse med IEC 61508 (se www.sintef.no/iec61508), vårt medlemskap i Standard Norge komité K 171 - IT Sikkerhetssystemer og internasjonalt via vårt medlemskap i IFIP "Working Group 11.10 on Critical Infrastructure Protection."

3.2.3 Følge opp (implementere) og videreutvikle ISBR og andre bransjestandarder

Følge opp og videreutvikle bransjenormer for informasjonssikkerhet i integrerte operasjoner. Et eksempel på slike standarder er ISBR fra OLF, men det bør også utvikles krav til leverandører, dokumenteres hva som er god praksis og hva som er "sikkert nok". Næringen bør kunne få råd om hva som er god praksis innen forskjellige områder. Industrien bør sørge for at god praksis for sikkerhet skal kunne deles åpent mellom alle aktørene.

Myndighetene må sette klarere krav (trekant myndigheter, selskaper, ansatte) og bygge på det IO-relaterte arbeidet som allerede er gjort med støtte fra industri og forskningsråd, som f.eks. IRMA (se www.sintef.no/irma), CRIOP [4] eller CheckIT, se www.checkit.sintef.no.

Status på bruk av standarder og forbedring av informasjonssikkerheten kan følges opp via systematisk bruk av indikatorer, som kan gi en indikasjon på sikkerhetsnivået og hvordan det utvikler seg over tid (se punkt 3.1.2 Indikatorer).

Ansvar: OLF og myndighetene ved Ptil bør ta ansvar.

3.2.4 Utvikle kompetanse

Forbedre og bygge ut kompetanse knyttet til teknisk sikring av SCADA- og IKT-systemer og bygge ut tverrfaglig relevant kompetanse. Felles opplæring og felles krav til opplæring bør komme sterkere. Det må trenes på kommunikasjon og folk må møtes sosialt for å bygge tillit – trene på kommunikasjon mellom ulike typer mennesker og fag/profesjoner/roller. Vi trenger flere ingeniører som "snakker" både prosesstyring og IT.

Ansvar: Et initiativ om kompetanseutbygging bør komme fra oljebransjen, eksempelvis via OLF. Deretter kan det konkretiseres av universiteter og høgskoler, eksempelvis NTNU via IO-senteret, som har et spesielt fokus på integrerte operasjoner. IO-senteret har i samarbeid med industrien, ref HFC-forum (se www.hfc.sintef.no), planer om å tilby flere relevante kurs, bl.a. et kurs i Human Factors (HF) fra 2007/2008.

3.2.5 God praksis for tekniske løsninger/referansearkitektur

Etablere og spre god praksis for tekniske løsninger raskere, for eksempel fjerntilgang (felles oppsett), HUB for autentisering av ansatte. Man ønsker praktiske løsninger og svar på spørsmålet: Hva er den anbefalte måten for oljebransjen å gjøre dette på? Dette må spres slik at man kan få en enhetlig tilnærming i hele bransjen. Andre viktige områder er referansearkitekturer, for å inkludere legacy-systemer og for å sette krav til komponenter/delsystemer og referansemodeller

for grenseflatene mot andre systemer. Et konkret forslag er også å lage god praksis (beste praksis) for nettverk som integrerer IKT-systemer med SCADA-systemer.

Ansvar: Her bør OLF ta en rolle, slik at man bl.a. definerer hva som man ønsker å spre åpent.

Forkortelser

IKT	Informasjons- og Kommunikasjons-Teknologi
IO	Integrerte Operasjoner
ISBR	Information Security Baseline Requirements (OLF guideline 104)
IT	Informasjons-Teknologi
NTNU	Norges Teknisk-Naturvitenskaplige Universitet
OD	Oljedirektoratet
OLF	Oljeindustriens LandsForening
Ptil	Petroleumstilsynet
SAS	Safety and Automation System
SCADA	Supervisory Control And Data Acquisition
SIS	Safety Instrumented Systems

Referanser

[1] M. G. Jaatun (red.), "Arbeidsseminar om IKT-sikkerhet i Integrerte Operasjoner: Referat " 2007, http://www.sintef.no/upload/10977/sluttrapport.pdf.

[2] M. B. Line, et al., "Monitoring of Incident Response Management Performance," in *International Conference on IT-Incident Management & IT-Forensics (IMF 2006)*. Stuttgart, Germany 2006.

[3] E. Hollnagel, D. D. Woods, and N. Leveson, *Resilience Engineering - Concepts and Precepts*: Ashgate, 2006.

[4] S. O. Johnsen, et al., "CRIOP®: A scenario method for Crisis Intervention and Operability analysis.," SINTEF 2004, Se www.criop.sintef.no.

[5] S. Lüders, "CERN tests reveal security flaws with industrial networked devices," 2006, http://ethernet.industrial-networking.com/articles/articledisplay.asp?id=1490.