SINTEF

SINTEF IKT
Anvendt kybernetikk

SINTEF Teknologi og samfunn
Sikkerhet

Postadresse: 7465 Trondheim
Besøksadresse: O S Bragstads plass 2D
7034 Trondheim
Telefon: 73 59 30 00
Telefaks: 73 59 43 99

Foretaksregisteret: NO 948 007 029 MVA

SINTEF RAPPORT

TITTEL

Uavhengighet av sikkerhetssystemer

FORFATTER(E)

Stein Hauge, Stig Ole Johnsen, Tor Onshus

OPPDRAGSGIVER(E)

Petroleumstilsynet

RAPPORTNR.	GRADERING	OPPDRAGSGIVERS JFR.	
SINTEF A12626	Åpen	Torleif Husebø	
GRADER. DENNE SIDE	ISBN	PROSJEKTNR.	ANTALL SIDER OG BILAG
Åpen	978-82-14-04450-8	90G342.01	16
ELEKTRONISK ARKIVKODE		PROSJEKTLEDER (NAVN, SIGN.)	VERIFISERT AV (NAVN, SIGN.)
Uavhengighet-endelig.doc		Tor Onshus	Lars Bodsberg
ARKIVKODE	DATO	GODKJENT AV (NAVN, STILLING, SIGN.)	
	2009-09-16	Sture Holmstrøm, Forskningssjef	

SAMMENDRAG

Sikkerhetssystemene offshore blir stadig mer "koblede", for eksempel ved at samme produsent leverer styre- og sikkerhetssystemer, bruk av felles software og brukergrensesnitt i ulike systemer, felles hardware, økt signaloverføring mellom systemer, innføring av integrerte operasjoner, osv.

Med dette som bakgrunn har Petroleumstilsynet med assistanse fra SINTEF gjennomført et prosjekt hvor hovedmålsettingene har vært å:

1. vurdere hvor sikkerhetskritisk angitte koblinger og avhengigheter egentlig er
2. avdekke hvorvidt enkelte typiske avhengigheter er uakseptable og derfor bør flagges overfor bransjen generelt

Denne rapporten oppsummerer resultatene fra dette arbeidet.

STIKKORD	NORSK	ENGELSK
GRUPPE 1	Sikkerhet	Safety
GRUPPE 2	Offshore	Offshore
EGENVALGTE	Uavhengighet	Independence
	Tekniske sikkerhetssystemer	Technical safety systems
	Tilgang og sikring	Access and security

INNHOLDSFORTEGNELSE

1. Sammendrag, konklusjoner og forslag til tiltak

Basert på en kartlegging utført i 2007, er det i dette prosjektet gjennomført tilsyn hos tre operatører og tre leverandører av sikkerhetssystemer. Hovedformålet har vært å undersøke i hvilken grad Ptil sine krav til uavhengighet er oppfylt og videre vurdere hvor sikkerhetskritisk eventuelle koblinger og avhengigheter egentlig er. Det er i denne sammenheng fokusert på feil og hendelser som kan føre til farlige tilstander ved at sikkerhetsfunksjoner ikke fungerer ved behov. Dette betyr at regularitetsproblemer – som at et sikkerhetssystem stenger ned utilsiktet – her ikke er ansett som tilsvarende kritisk da sikker tilstand normalt er å stenge ned. Merk at for en del systemer og spesielt flytende installasjoner er dette ikke alltid tilfelle (dynamisk posisjonering, ballastering, brannpumper, etc.). Hyppige oppstarter kan dessuten i seg selv være et sikkerhetsmessig problem.

En del hovedfunn fra prosjektet er listet under. Merk at vi her har fokusert på de områdene der næringen har et forbedringspotensial. For mer utdypende beskrivelse av hvert punkt refereres det til kapittel 3:

a) Signaler fra underordnede til overordnede systemer er forholdsvis vanlig
b) Konsekvenser og aksjoner ved tap av datakommunikasjon til land er uklare
c) Risiko- og sårbarhetsanalyser (ROS) er generelt mangelfulle
d) Automatiseringssystemene er ikke sertifiserte for datatrafikk
e) Det er begrenset bruk av fjerntilgang
f) SIS og PCS nettverket kunne vært bedre segmentert
g) Implementering av sikkerhetskritiske funksjoner i styresystemet forekommer
h) Det er ingen spesifikk oppfølging av fellesfeilhendelser[1]
i) Dokumentasjon av tilstrekkelig uavhengighet mangler
j) Det mangler ofte formaliserte krav til kompetanse
k) Krav til ytelse for SIS og oppfølging av slike er mangelfulle
l) Det er flere eksempler på at styrende dokumentasjon ikke er oppdatert
m) Manglende beredskap og manglende prosedyrer for håndtering av virus og oppdateringer

Som en ser av listen over og nærmere beskrivelse i kapittel 3, er det flere punkter som i seg selv må sies å representere avvik fra Ptils krav om uavhengighet (jfr. styringsforskriftens § 1 og innretningsforskriftens § 31-33) - herunder spesielt punktene a), f), g) og i).

Når det gjelder *signaler i "feil retning"*, dvs. fra underordnet til overordnet system (slik som signaler fra PAS til NAS), representerer dette helt klart en uheldig design. Ved detaljert gjennomgang av en rekke slike signaler har vi imidlertid ikke konkret klart å påvise at noen er av en slik karakter at feil på underordnet system kan medføre sikkerhetskritiske feil i overordnet system.

Mangelfull segmentering av SIS og PCS nettverkene representerer også en utfordring i forhold til å påvise full uavhengighet mellom disse systemene.

Tilsvarende representerer *implementering av sikkerhetskritiske funksjoner i styresystemet* en svært uheldig design som klart kan svekke påliteligheten til de berørte sikkerhetsfunksjonene. Den utstrake bruken av signaler over nettverk fører også til at kompleksiteten øker og testing blir vanskelig.

[1] Fellesfeil: feil på to eller flere (redundante) komponenter som har samme årsak, og som skjer innenfor et begrenset tidsintervall, /2/

Når det gjelder *manglende dokumentasjon av tilstrekkelig uavhengighet* er dette et vanskelig tema siden begrepet *tilstrekkelig* slik det benyttes i forskriftene[2] krever videre tolkning. En kan i første omgang støtte seg på veiledning til styringsforskriften som sier at én enkelt feil eller enkelt hendelse ikke skal kunne "slå ut" flere systemer samtidig. Gitt dagens teknologiske virkelighet med økt integrasjon av IKT systemer og SAS, økt sammenkobling mellom systemer og installasjoner, bruk av felles nettverk og felles servere og brukergrensesnitt for SIS og PCS, og et generelt sammensatt risikobilde – med andre ord økt kompleksitet – blir en slik definisjon av hva som er *tilstrekkelig uavhengig* dessverre utilstrekkelig i seg selv. Industrien trenger derfor en tydeligere presisering av hva som ligger i begrepet *tilstrekklig uavhengig* og hva som kreves for å vise dette.

I CCPS boka "Guidelines for Safe and Reliable Instrumented Protection Systems" (Wiley, 2007), /10/, står følgende beskrivelse av uavhengighet som det kan være nyttig å vurdere dersom en ønsker å utdype veiledningsteksten videre:

> *"For a protection layer to be considered independent, its performance should not be affected by the occurrence of the initiating cause, its consequences, or by the failure of another protection function used to reduce the risk of the same hazardous event. The correct operation of the protection layer should not be conditional on any other layer and its separation from other layers should be unambiguous."*

Basert på ovenstående er SINTEFs hovedkonklusjoner som følger:

- I tråd med funn i tidligere studier kan det konkluderes med at industrien ikke arbeider systematisk med å påvise at systemer er uavhengige av hverandre og dermed ikke kan sies å ha full kontroll med dette;
- Uønskede IKT hendelser og trusler slik som virusangrep og nettstorm har så langt i all hovedsak ført til at systemer og installasjoner har stengt ned. Industrien kan imidlertid ikke sies å ha full kontroll ved hvorvidt slike trusler også kan medføre sikkerhetsmessige konsekvenser i framtida;
- En kan dermed konkludere med at risikobildet generelt er noe uklart og at bevisstheten derfor bør styrkes i form av økt bruk av risiko- og sårbarhetsanalyser, bedre samarbeid mellom fagdisipliner (IKT / prosess / automatisering /instrument / telekom.) og en generell kompetanseheving;
- De fleste installasjoner er ikke forberedt verken teknisk eller organisatorisk på fjerntilgang. Det mangler både analyser og tekniske tiltak før dette kan tas i bruk over alt. Det er i denne sammenheng verdt å henvise til OLF 104.
- Det er i denne rapporten trukket fram flere spesifikke avhengigheter som det bør arbeides videre med både via designmessige tiltak og ved økt bruk av ulike analyser;

Som et forsøk på å konkretisere hvilke krav som bør stilles overfor operatører/leverandører i forhold til å dokumentere uavhengighet, foreslår SINTEF følgende:

- Alle IO og koblinger via nett/kommunikasjon til/fra systemer skal dokumenteres inkludert en beskrivelse av hva signalene brukes til og hvorfor de ikke er kritiske;

[2] Ordlyden i styringsforskriftens §1 er "Der det er nødvendig med flere barrierer, skal det være tilstrekkelig uavhengighet mellom barrierene". Dette er i veiledning til forskrift utdypet med at "Kravet til uavhengighet innebærer at flere viktige barrierer ikke skal kunne svekkes eller settes ut av funksjon samtidig, blant annet som følge av en enkelt feil eller en enkelt hendelse"

- Det skal dokumenteres at nettstorm ikke kan føre til at funksjoner svikter i farlig tilstand men kun medfører at SIS går til sikker tilstand;

- Det skal dokumenteres at operatørgrensesnitt og andre enheter basert på standard operativsystemer ikke kan påvirke sikkerhetsfunksjonene negativt;

- Det skal dokumenteres at sikkerhetsfunksjoner der sikker tilstand ikke er av/stopp er operative etter en vilkårlig enkeltfeil (FMEA som for DP);

- Det skal dokumenteres at enkeltfeil på felleskomponenter (for eksempel nettverk, power, servere, OS) ikke skal kunne gi farlige feil på sikkerhetsfunksjoner;

- Det skal finnes en oppdatert analyse som tar for seg tap av datakommunikasjon til land og mulige konsekvenser av tapt kommunikasjon;

- Det skal være beredskap og prosedyrer på plass for håndtering av IKT relaterte angrep og trusler.

2. Innledning

2.1 Bakgrunn

Petroleumstilsynet har de senere årene sett en økende grad av integrasjon og kobling mellom sikkerhets- og styresystemene. Samtidig inneholder regelverket krav om tilstrekkelig uavhengighet mellom sikkerhetsbarrierene (jfr. styringsforskriftens § 1) inkludert krav om at sikkerhetssystemene skal kunne utføre tiltenkte funksjoner uavhengig av andre systemer. (jfr. innretningsforskriftens § 31-33). Som en følge av teknologiutviklingen og økende bruk av integrerte systemer har Ptil stilt spørsmål ved hvorvidt kravene til uavhengighet og robusthet av barrierene er tilstrekkelig oppfylt.

Med dette som bakgrunn, har Ptil med assistanse fra SINTEF gjennomført et tilsyn med det formål å studere noen utvalgte installasjoner, systemer og koblinger i mer detalj. Fokus for tilsynet har vært uavhengigheten til sikkerhetssystemene gitt de koblinger som finnes mellom systemene i SAS og fra eksterne IKT systemer. Totalt ble det gjennomført tilsyn rettet mot fire installasjoner i form av møter med operatører samt leverandører av SAS. Det ble også gjennomført et offshore besøk for én av installasjonene.

Denne rapporten oppsummerer hovedresultatene fra dette tilsynet

2.2 Tidligere SINTEF arbeid innenfor området

SINTEF har tidligere utført flere prosjekter for Ptil og gjennom PDS, som er direkte eller indirekte er knyttet til temaet uavhengighet, herunder;

“The Impact of Common Cause Failures in Safety Systems”, PDS memo datert april 2004. Memoet er basert på en studie for Norsk Hydro hvor en, basert på arbeidsmøter og gjenomgang av Synergi rapporter, blant annet gir en rekke eksempler på typiske fellesfeil i instrumenterte sikkerhetssystemer og årsaker til disse.

”Trusler og muligheter knyttet til eDrift”. Åpen rapport til Ptil datert januar 2005. Formålet med dette prosjektet var å kartlegge trusler og muligheter knyttet til innføring av eDrift eller Integrerte Operasjoner, slik at risikobildet kunne komme klarere frem.

”Uavhengighet av sikkerhetssystemer offshore – status og utfordringer”. Rapport for Ptil datert januar 2006. I denne rapporten er det gitt en statusbeskrivelse av hvordan Ptil sitt krav til uavhengighet mellom tekniske barrierer er implementert på norsk sokkel, og diverse kjente avhengigheter mellom ulike sikkerhetssystemer er beskrevet og diskutert, basert på blant annet intervjuer med fagfolk.

”Uavhengighet mellom barrierer - metodikk for avhengighetsanalyse”. Draft notat for Ptil datert juni 2006. I dette notatet beskrives metoder for analyse av avhengige feil og det gis anbefalinger til hvordan Ptil kan forholde seg til slik metodikk i sitt tilsynsarbeid mot nye prosjekter.

”Oversikt over utvalgte kontroll- og sikkerhetssystemer (SAS) på sokkelen”. Rapport til Ptil datert november 2007. Formålet med dette prosjektet var å kartlegge status på utvalgte styre og sikkerhetssystemer og sikring av disse i forhold til uønsket tilgang og IKT angrep. Det ble utviklet et spørreskjema som ble distribuert til alle selskapene som er operatør for produksjonsinnretninger

på norsk kontinentalsokkel og rapporten oppsummerer resultatene fra spørreskjemaundersøkelsen. Bakgrunn for undersøkelsen var at Petroleumstilsynet ønsket å skaffe seg en oversikt over status på utvalgte styre og sikkerhetssystemer (SAS) og sikring av disse. Hovedkonklusjoner fra denne undersøkelsen, /4/, ligger i vedlegg A.

2.3 Målsettinger

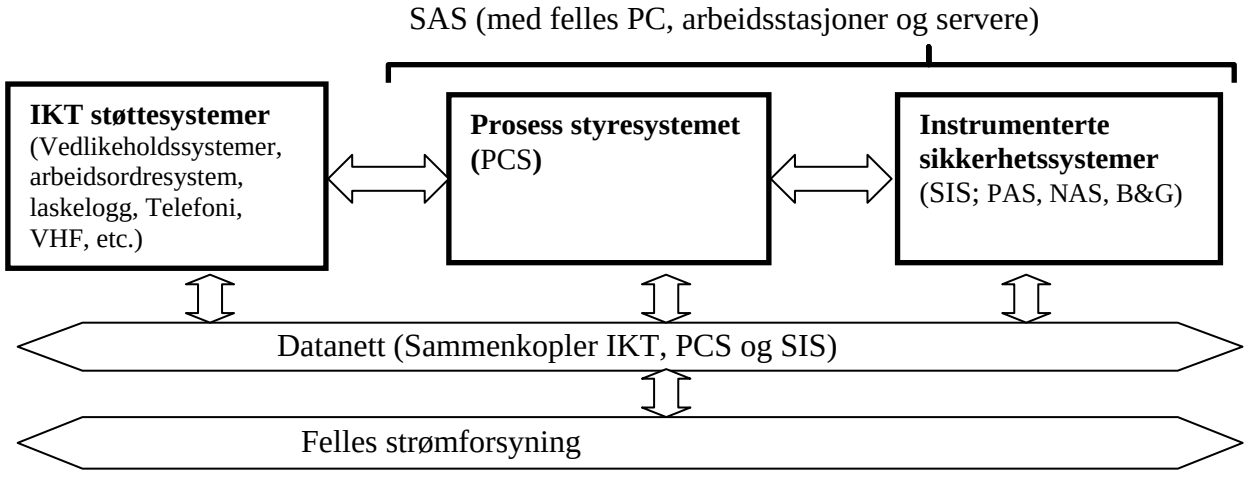
Hovedmålsettingene med dette prosjektet har vært følgende:

- å vurdere hvor sikkerhetskritisk angitte koblinger og avhengigheter egentlig er
- å avdekke hvorvidt enkelte typiske avhengigheter er uakseptable og derfor bør flagges overfor bransjen generelt

Eksempler på forhold som har blitt sett spesifikt på er felles nettverk, felles servere, felles infrastruktur, anvendte løsninger for å separere og beskytte systemene samt bakgrunnen for hvorfor en del signaler sendes i uønsket retning (for eksempel fra prosessavstengningssystemet til nødavstengningssystemet).

2.4 Omfang

Systemer som har vært inkludert i dette prosjektet har vært tekniske løsninger, datanett og IKT systemer, som er sammenkoplet rundt SAS systemene. Dette er forsøkt vist i figuren under. Hovedfokus har imidlertid vært avhengigheter i SAS og i koblinger mellom IKT systemene og SAS.



Figur 1: Anskueliggjøring av omfang

2.5 Forkortelser

B&G	-	Brann og gass
DFU	-	Definert Fare- og Ulykkeshendelse
DoS	-	Denial of Service
NAS	-	Nødavstengningssystem
OS	-	Operatørstasjon
PAS	-	Prosessavstengningssystem
PDS	-	Pålitelighet av Databaserte Sikkerhetssystemer
PCS	-	Process Control System
ROS	-	Risiko og sårbarhet
SAS	-	Safety and Automation System
SIS	-	Safety Instrumented System
VHF	-	Very High Frequency

3. Resultater

I dette kapittelet oppsummeres hovedresultater fra arbeidet knyttet til de fire gjennomførte tilsynene. Resultatene er forsøkt strukturert i forhold til hovedtemaer slik disse var definert i spørreundersøkelsen fra 2007. Det bør igjen understrekes av fokus har vært på områder hvor næringen har et forbedringspotensial.

3.1 Datatrafikk og datakommunikasjon

Sentralt her var å se nærmere på oppgitte koblinger mellom de forskjellige deler av SAS og mellom SAS og andre systemer, for på denne måten å kunne vurdere hvorvidt krav til uavhengighet er tilstrekkelig ivaretatt. Datakommunikasjon fra installasjon til land er også diskutert.

3.1.1 Signaler fra underordnet til overordnede systemer er forholdsvis vanlig

Det er funnet en rekke eksempler på at signaler går i ”feil retning” mellom systemer, for eksempel fra PCS til PAS og fra PAS til NAS ’(altså fra underordnet til overordnet system). Det er ikke tilstrekkelig dokumentert at disse signalene ikke kan gi negativ påvirkning på andre systemer.

3.1.2 Konsekvenser og aksjoner ved tap av datakommunikasjon til land er uklare

En har de seinere år sett en økt trend mot at offshore installasjonene bruker sentrale datasystemer på land som dermed faller bort ved tap av fiberkommunikasjon til land. Eksempler på dette kan være arbeidsordresystem, laskelogg, vedlikeholdssystem og hendelsesrapporteringssystem samt tap av datanett, telefon og VHF.

Basert på samtaler med personell på installasjonene virker det som en generelt ikke har full oversikt over hva en mister ved bortfall av kommunikasjon over fiber til land og hva mulige konsekvenser av dette kan være. Effekter og konsekvenser av tapt kommunikasjon til land bør derfor klarlegges og nødvendige aksjoner bør være definert på forhånd.

3.2 Tilgang til og sikring av SAS

Dette omfatter sikring av systemene knyttet til lokal tilgang, fjernaksess, osv. Dessuten hva som gjøres av uttesting og analyser for å verifisere systemenes godhet.

3.2.1 Risiko- og sårbarhetsanalyser (ROS) er generelt mangelfulle eller har feil fokus

Generelt ser en at installasjonene får stadig nye IKT løsninger som utvikler seg over tid og som en bli mer og mer avhengig av. Hvorvidt det utføres ROS analyser av disse IKT systemene og av sammenkoblingen mellom IKT og SAS systemene synes å variere mellom operatørene og mellom installasjonene. I den grad slike analyser er utført er det en generell observasjon at disse ofte utføres på delsystemnivå, mens det synes å mangle overordnede analyser som tar for seg totaliteten, ser analysene i sammenheng og vurderer grensesnittene mellom systemene. En annen observasjon er at effekten på produksjonen (oppetid) ofte er fokus for analysene. Analysene bør, i tillegg, på en systematisk måte se på hvilke effekter IKT relaterte feil kan ha på sikkerheten.

3.2.2 Automatiseringssystemene er ikke sertifiserte for datatrafikk

En ser ofte at automatiseringssystemene ikke har blitt sertifisert eller testet med de nye belastningene (eksempel nettstorm) som kan skje med økt bruk av PC teknologi og økt bruk av datanettverk. Dette er derfor en problemstilling som bør vurderes. Det finnes i dag kommersielle verktøy som kan avsløre eventuelle sårbarheter.

3.2.3 Det er begrenset bruk av fjerntilgang.

Ingen av selskapene la for eksempel opp til at leverandørene skulle kunne sitte hos seg selv å gjøre endringer på systemene.

3.3 Uavhengighet mellom systemer

3.3.1 SIS og PCS nettverket kunne vært bedre segmentert

I forbindelse med tilsynene ble det avdekket at PCS og SIS som regel var realisert på samme nettverk og struktur uten segmentering (oppdeling), annet enn ved hjelp av switcher. Trafikk fra PCS kan da påvirke SIS. Det er dokumentert at dette kan lede til problemer, eksempel har vi bl.a. fra kjernekraftindustrien fra Browns Ferry – hvor det ble dokumentert at nettverkene var følsomme for uplanlagt PC trafikk. Hvorvidt slik trafikk kan være sikkerhetskritisk på en offshore installasjon er usikkert, men det motsatte bør i hvert fall dokumenteres.

3.3.2 Implementering av sikkerhetskritiske funksjoner i styresystemet forekommer

Det ble i forbindelse med tilsynene registrert at sikkerhetskritiske funksjoner kan være implementert i styresystemet. Eksempler er brannspjeld og brannpumper implementert i PCS noder og NAS funksjon som benytter seg av PCS transmitter.

En slik design må anses som avvik fra Ptil sitt generelle krav om uavhengighet mellom styre- og sikkerhetssystemer. Det er dessuten generelt mindre fokus ute på oppfølging av styresystemene i forhold til oppfølging av sikkerhetssystemene, noe som tilsier at slike løsninger er uheldig.

3.3.3 Det er ingen spesifikk oppfølging av fellesfeilhendelser

På spørsmål om selskapene hadde egne systemer eller rutiner for oppfølging av fellesfeilhendelser svarte alle selskapene negativt. Det er heller ingen spesifikk registrering av slike hendelser.

I forbindelse med årlige gjennomganger av sikkerhetskritiske feil som SINTEF har deltatt på, er det en generell observasjon at hendelser hvor flere komponenter feiler samtidig pga felles årsak, ikke er uvanlig. Det er derfor viktig at bransjen tar tak i dette og at en på sikt vurderer å bygge opp en slags sjekkliste eller database over fellesfeilhendelser som kan anvendes i framtidig forbedringsarbeid.

3.4 Generell styring og oppfølging

3.4.1 Dokumentasjon av tilstrekkelig uavhengighet mangler

En generell konklusjon er at selskapene har en lite systematisk tilnærming til uavhengighetsprinsippet. Det mangler akseptkriterier for hva som er ”tilstrekklig uavhengig” og det mangler en systematisk tilnærming i forhold til å påvise tilstrekkelig uavhengighet.

Dette er i tråd med funn fra tidligere studier som blant annet viste at selskapene i liten eller ingen grad utfører spesifikke analyser for å påvise at systemene er funksjonelt uavhengige.

3.4.2 Det mangler ofte formaliserte krav til kompetanse

En generell observasjon er at flere selskaper og leverandører ikke har formaliserte krav til kompetanse for personell som vedlikeholder og modifiserer de instrumenterte sikkerhetssystemene på installasjonene. Det er også eksempler på at selskap har systemer på dette, men at disse systemene ikke blir tilstrekkelig fulgt opp i praksis.

3.4.3 Krav til ytelse for SIS og oppfølging av slike er mangelfulle

Krav til ytelse for de instrumenterte sikkerhetssystemene synes ofte å mangle og/eller de er ikke kjent i driftsorganisasjonen. I andre tilfeller ser en at slike krav finnes, men at de ikke følges opp i drift.

Dette medfører at selskapene ikke fullt ut kan sies å ha kontroll med barrierene, dvs. kontroll med hvorvidt disse oppfører seg i drift slik det er forutsatt i design at de skal.

3.4.4 Det er flere eksempler på at styrende dokumentasjon ikke er oppdatert

I forbindelse med tilsynene ble det avdekket flere eksempler på at systembeskrivelser i sentral dokumentasjon ikke var oppdatert i henhold til hvordan systemene per i dag er implementert.

Det ble også registrert at sentrale krav og forutsetninger fra designfasen, som kan påvirke sikker operasjon av de instrumenterte sikkerhetssystemene, ikke overføres til driftsdokumentasjon på en konsistent og systematisk måte.

3.4.5 Manglende beredskap og manglende prosedyrer for håndtering av virus og oppdateringer

I forbindelse med tilsynene ble det avdekket manglende rutiner for håndtering av virus i systemer og manglende beredskapsrutiner. Manglende virusbeskyttelse og rutiner kan medføre at en har manglende barrierer for sårbarheter som kan påvirke IKT, PCS og SIS systemene. En annen observasjon er at sikkerhetsoppdateringer av Windows (på operatørstasjoner) sjelden gjennomføres.

4. Referanser

/1/ Petroleumstilsynets regelverk med veiledninger.

/2/ PDS Notat: “The Impact of Common Cause Failures in Safety Systems”, April 2004

/3/ ”Uavhengighet av sikkerhetssystemer offshore – status og utfordringer”, SINTEF rapport STF50 A06011, Januar 2006

/4/ ”Oversikt over utvalgte kontroll- og sikkerhetssystemer (SAS) på sokkelen og sikring av disse”, SINTEF rapport F3905, April 2007 (*fortrolig*)

/5/ ISA99 - International Society for Automation, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program, ANSI/ISA-99.02.01-2009, Research Triangle Park, North Carolina, 2009.

/6/ S. Luders, CERN tests reveal security flaws with industrial networked devices, The Industrial Ethernet Book, GGH Marketing Communications, Titchfield, United Kingdom, pp. 12–23, November 2006.

/7/ Nuclear Regulatory Commission, The effects of Ethernet-based, non- safety-related controls on the safe and continued operation of nu-clear power stations, NRC Information Notice 2007-15, Washington, DC (www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/2007/in200715.pdf), 2007.

/8/ OLF 104 Information security baseline requirements, retrieved from http://www.olf.no/guidelines/ at 28/7-2009.

/9/ K. Stouffer, J. Falco and K. Kent, Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security, NIST Special Publication 800-82, Initial Public Draft, National Institute of Standards and Technology, Gaithersburg, Maryland, 2006.

/10/ Center for Chemical Process Safety (CCPS): *Guidelines for safe and reliable instrumented protective systems*, Wiley, 2007

VEDLEGG A – Sammendrag av spørreundersøkelsen fra 2007, /4/

Bakgrunnen for prosjektet var at Petroleumstilsynet (Ptil) ønsket å skaffe seg en oversikt over status på utvalgte kontroll og sikkerhetssystemer (SAS) og sikring av disse. For å belyse denne problemstillingen utviklet SINTEF i samarbeid med Ptil et spørreskjema som ble distribuert til alle selskapene som er operatør for produksjonsinnretninger på norsk kontinentalsokkel. Dette spørreskjemaet ble sendt ut i slutten av mars 2007.

På basis av de innsamlete spørreskjemaene ble det utarbeidet en fortrolig rapport og følgende sammendrag er hentet fra denne (jfr. /4/).

Resultater og observasjoner

De viktigste resultatene fra spørreundersøkelsen er:

- Det synes å være avhengighet mellom SIS (de instrumenterte sikkerhetssystemene) og PCS (prosess styring), ut fra at systemene har felles komponenter og ofte ligger på felles nett.
- SAS systemene er ikke testet for å tåle all mulig IKT trafikk. I forbindelse med innføring av Integrerte Operasjoner vil integrasjon mellom IKT og SAS øke. I slike integrerte systemer er det viktig å unngå feil på sikkerhetssystemer på grunn av datatrafikk.
- Rutiner for å lære av uønskede IKT hendelser kan forbedres. Det mangler DFU'er og systematisk scenariotrening.
- SAS systemene kan være dårlig beskyttet mot bevisste angrep; robusthet kan forbedres ved at man deler god praksis for nettdesign, teknisk sikring og arbeidspraksis.

Viktige observasjoner fra gjennomgangen av spørreskjemaene (tematisk) er:

- *Generelt – det er stor spredning i svar;* Samme operatør gir til dels svært forskjellige svar avhengig av den spesifikke installasjonen, dvs. det synes som om det for enkelte operatører er begrenset standardisering og koordinering på tvers av installasjonene.

- *Tema 2 – Informasjon om SAS systemene;* Det er stor spredning mellom valgte SAS systemer hos samme operatør. Samme operatør har ofte valgt forskjellige leverandører og forskjellige tekniske løsninger på samme installasjon. Dette kan gi utfordringer for datakommunikasjon og oppkopling siden forskjellige løsninger må testes ut og integreres

  Ser en på framtidige integrerte operasjoner og fjernstyring, øker dette også kompleksiteten siden de som skal stå for fjernstøtte må forholde seg til mange ulike løsninger. Imidlertid vil forskjellige løsninger kunne øke robustheten for felles hendelser, da systemene har ulik teknisk implementering. For eksempel vil et virusangrep kunne ramme færre systemer totalt sett.

  Når SAS systemene kommer fra en og samme leverandør, gir dette tilsynelatende større integrasjon og avhengigheter mellom SAS systemene enn der det er valgt ulike leverandører. Det synes som om enkelte systemer er integrert på en slik måte at PCS/PAS og NAS inneholder felles komponenter som datanett, servere og operatørgrensesnitt, og dermed kan være avhengige. Slike avhengigheter mellom kritiske systemer hvor disse er nødvendig for å komme til sikker tilstand kan *i verste fall* medføre svikt av flere barrierer.

- *Tema 3 – Informasjon om andre systemer;* De fleste installasjonene har gått over til en eller annen form for Windows på operatørstasjonene og flertallet av nyere installasjoner benytter

også Ethernet (TCP/IP) for å utveksle informasjon mellom SAS og andre systemer. Bruk av kommersielt tilgjengelig software og standardiserte løsninger åpner for problemer med virusangrep både for PCS og SIS og medfører sårbarheter knyttet til bevisste hacker angrep. God eller beste praksis for sikring av systemene bør derfor i større grad spres mellom installasjonene.

- *Tema 4 - Informasjon om datatrafikk;* Formålet med dette temaet var å kartlegge koblinger mellom de forskjellige deler av SAS og mellom SAS og andre systemer, for på denne måten å kunne vurdere hvorvidt krav til uavhengighet mellom systemer er ivaretatt. Det framkom av svarene at mange installasjoner har signaler fra PCS til PAS og fra PAS til NAS. Med andre ord går flere signaler i "feil retning" fra underordnet til overordnet system. Det er imidlertid vanskelig å tolke årsakene til dette uten at en utfører en mer utdypende kartlegging.

- *Tema 5 – Tilgang til og sikring av SAS;* Det synes å være mange forskjellige løsninger som er implementert for sikring av SAS systemene. Generelt er det implementert enkle brannmurer bare mellom IKT og PCS systemet og ingen brannmur/barrierer mellom SIS og PCS, noe som *kan* være en for lite robust og sikker løsning. På den annen side skal det bemerkes at SIS systemene er designet slik at det er lagt sterke begrensninger på hvilke type signaler som kan sendes inn til systemene og hvilken informasjon som faktisk påvirker systemene.

  Nettene for PCS og SIS er på noen installasjoner felles, mens de på andre er separate. Dette kan lede til avhengighet mellom systemene; dersom for eksempel PCS nettet rammes vil også SIS nettet kunne rammes. På en del installasjoner er det felles nett for PAS og PCS og felles nett for de andre SIS systemene.

- *Tema 6 – Uavhengighet mellom systemene;* De som har svart oppgir generelt få avhengigheter mellom systemene, samtidig som det nevnes at nettene for PCS og SIS er felles. Det nevnes ofte felles operatørstasjon for tilgang til PCS og SIS. SAS systemene har ofte samme underliggende tekniske infrastruktur, noe som bør vurderes opp mot kravet om uavhengighet. Det er for eksempel ikke klart om en feil på en komponent i ett system kan spre seg til et annet system når samme underliggende tekniske infrastruktur er benyttet.

  I forbindelse med arbeidet med rapporten " *Uavhengighet av sikkerhetssystemer offshore – status og utfordringer*", ref. /3/, ble det avdekket flere avhengigheter mellom systemer som ikke framkommer på noen av svarskjemaene. Dette kan tyde på at enkelte avhengigheter ikke nødvendigvis er kjent for alle respondentene (eller de er "glemt" under utfylling av skjemaene).

- *Tema 7 - Generell styring og oppfølging;* Det finnes generelt mange ulike krav og retningslinjer som gjelder for IKT sikkerhetstiltak. I enkelte tilfeller ramses det opp så mange ulike dokumenter og retningslinjer at det er grunn til å tro at omfanget i seg selv vil være en utfordring i forhold til å få en ensartet og god praksis. I enkelte tilfeller opplyses det at man ikke kjenner til gjeldende retningslinjer.

  Systematiske Risiko og Sårbarhetsanalyser (ROS) utføres i begrenset grad og de forskjellige fagdisipliner er ikke alltid (formelt) involvert i denne type analyser. Det foretas sjelden risikoanalyse av integrasjonen mellom SAS systemene og IKT systemene. Det er variabelt om det finnes oppdatert nettverksdiagram for PCS/SIS/IKT systemene.

  Det benyttes ulike administrative systemer for å rapportere uønskede PCS/SIS/IKT hendelser. Generelt kan det synes som om det ikke er gode nok rutiner for rapportering eller læring av uønskede IKT løsninger.

Ved svikt eller stopp i IKT/SAS systemene foreligger ikke alltid tydelige beredskapsløsninger.

Videre bearbeiding av funn fra spørreundersøkelsen

Det ble forut for de fire tilsynene utarbeidet en liste som nærmere oppsummerte en del av funnene fra spørreundersøkelsen:

1. **Manglende felles risiko og sårbarhetsvurderinger av koplingene mellom IKT og PCS:** Spørreundersøkelsen avdekket at bare 5 av de 46 installasjonene hadde gjennomført risikoanalyser knyttet til sammenkopling mellom IKT og PCS systemer.

2. **Separate faggrupper (siloer) for systemene med lite samhandling mellom telekom., prosess og IKT:** Prosess- og IKT-miljøene hadde samarbeidet på 8 av de 46 installasjonene. Vi ønsket å se på helheten av systemene og så da på Prosesstyringssystemene (PCS), med IKT komponenter som skjermer/servere, datanettet (lokalt og med koplinger til land) og evt. relevante IKT systemer (lokalt og å land). Systemene var styrt av forskjellige fagmiljø (som prosess, telekom., IKT) og det manglet ofte et samlet bilde og oversikt over alle systemene. Det var ofte lite samarbeid mellom fagmiljøene – miljøene jobbet i forskjellige fagsiloer.

3. **PCS og IKT systemer manglet sertifisering:** PCS systemene hadde ikke blitt sertifisert til å takle uønsket datatrafikk og kunne derfor stoppe eller oppføre seg uventet. IKT komponenter koples i økt grad opp mot PCS systemene. Slik sertifisering er tilgjengelig fra kommersielle aktører (for eksempel Achilles fra Wurldtech Security, ISA er i ferd med å utvikle standarder for dette). På 17 av de 46 installasjonene ble datatrafikken i PCS overvåket.

4. **Mulighet for fellesfeil – PCS og SIS har felles komponenter:** PCS og SIS har ofte felles strømforsyning, arbeidsstasjoner og nettverk som øker sannsynligheten for fellesfeil. PCS og SIS fra samme leverandører hadde flere felleskomponenter. Det er ikke rapportert at SIS har feilet eller blitt påvirket av datatrafikk eller feil oppsett i fm. integrasjon mellom IKT og SIS – men tester har avdekket sårbarheter i SIS som gjør at systemet kan stoppe opp (disse feilsituasjonene er meldt inn til leverandørene).

5. **Manglende nettverksbarrierer og segmentering av datanett:** Det var få/ingen barrierer mellom PCS og SIS, etablert via brannmur eller via segmentering av nettet. En fulgte i liten grad forslag til standarder fra ISA eks. “Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program”, ANSI/ISA-99.02.01-2009.. Dersom nettet ikke struktureres kan det lede til at PCS eller SIS blir belastet og påvirket av uønsket nett-trafikk – noe som gjør at systemene kan feile og stoppe opp.

6. **Ett standard sett av retningslinjer mangler:** 3 installasjoner benyttet ikke retningslinjer for sikkerhet/sikring for sammenkopling av IKT og prosessystemer. På 20 installasjoner var mange forskjellige retningslinjer referert. IKT og prosess bruker forskjellige standarder som utgangspunkt for sine vurderinger. IKT baserer seg på ISO/IEC 27002, mens prosess benytter IEC 61508. Det var generelt mangel på kjennskap til standarder og retningslinjer for sammenkopling mellom IKT og PCS som er etablert, som f.eks. fra ISA (International Society for Automation) “Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program”,

ANSI/ISA-99.02.01-2009.

7. **Rapportering, "awareness" og deling av uønskede hendelser kan forbedres:** To installasjoner hadde ikke rutiner for rapportering av uønskede hendelser knyttet til IKT/PCS. En organisasjon brukte 3 forskjellige rapporteringssystemer. Det ble ikke kjørt systematiske kurs for å øke "awareness". Det synes som om det var lite kjennskap til uønskede hendelser som kunne påvirke IKT, PCS og andre systemer. Det er ikke etablert DFUer (Definert Fare- og Ulykkeshendelser) knyttet til tap av datanett, PCS eller tilsvarende.

8. **Manglende distribusjon av Patcher.:** Distribusjon av Patcher varierte – noen steder ble patcher distribuert systematisk, mens andre steder ble patcher distribuert usystematisk eller de manglet helt.