DNV·GL

IKT-SIKKERHET – ROBUSTHET I PETROLEUMSSEKTOREN

Cyber security SIS og egensikre komponenter, kommunikasjonsprotokoller

Petroleumstilsynet

Rapport nr.: 2019-0826, Rev. 0
Dato: 2020-02-21

Prosjekt navn:	IKT-sikkerhet – Robusthet i petroleumssektoren	DNV GL AS
Rapport tittel:	Cyber security SIS og egensikre komponenter, kommunikasjonsprotokoller	Cyber Security Services Postboks 300
Kunde:	Petroleumstilsynet, P.O. Box 599 4003 Stavanger Norge	1322 Høvik Norway
Kontaktperson:	Arne Halvor Embergsrud	
Dato:	2020-02-21	
Prosjekt nr.:	10157212	
Organisation unit:	Cyber Security Services	
Rapport nr.:	2019-0826 Rev. 0	
Dokument nr.:		

Kontrakt for leveranse av denne rapport:

Kontrakt 06677 IKT-sikkerhet – Robusthet i petroleumssektoren - Prosjekt 992709

Hensikt:

Delleveransen vurderer IKT-sikkerhet i instrumenterte sikkerhetssystemer («Safety Instrumented System» (SIS)). Det er vurdert hvordan IKT-sikkerhet bygges inn i design av slike systemer fra en tidlig fase og hvordan dette ivaretas i bygging, igangsetting og drift.

Utarbeidet av:	Verifisert av:	Godkjent av:
Pål Børre Kristoffersen Principal Specialist	Boye Tranum Project Manager	Trond Solberg Head of Section Cyber Security Services
Knut Omberg Principal Engineer		

DNV GL Distribution:

☒ ÅPEN. Fri distribusjon, internt og eksternt

☐ INTERN. Fri distribusjon internt i DNV GL.

☐ KONFIDENSIELL. Distribusjon som angitt i distribusjonsliste.

☐ HEMMELIG. Kun autorisert tilgang.

☐

Keywords:

Cybersecurity, Security, Digital Vulnerabilities, Oil & Gas, Information Risk Management, Lysneutvalget

Rev. Nr.	Dato	Formål	Utarbeidet av	Verifisert av	Godkjent av
A	2019-11-30	Høringsutkast	Pål Kristoffersen	Boye Tranum	Trond Solberg
0	2020-02-21	Revidert etter høring	Pål Kristoffersen	Boye Tranum	Trond Solberg

INNHOLD

1 SAMMENDRAG

For å unngå eller begrense ulykker ved olje- og gassinstallasjoner, er det installert en rekke sikkerhetssystemer. Funksjonen til sikkerhetssystemer er å forhindre og ta kontroll i en uønsket hendelse når prosessen og anlegget ikke lenger opererer i en normal tilstand. Utblåsningssikring, nødavstengningssystemer og brann- og gass-systemer regnes som de mest vitale sikkerhetssystemene.

Tidligere var sikkerhetssystemer basert på mekaniske systemer eller de var isolerte systemer med egne kontrollsystemer. I dag er sikkerhetssystemene primært styrt av digitale komponenter og de er i mange tilfeller tilknyttet samme nett som prosesskontrollsystemer. Det betyr at sikkerhetssystemene har fått angrepsflate i forhold til IKT-sikkerhetshendelser.

Denne rapporten vurderer hvordan installerte og nyere sikkerhetssystemer sikres i forhold til IKT-sikkerhetshendelser gjennom:

Design

Systemer for utblåsningssikkerhet er designet for å operere isolert og totalt uavhengig av andre systemer. Noen systemer er tilkoblet datanett for overvåkning. De fleste operatører tillater ikke fjernvedlikehold av slike systemer. Kommunikasjon mellom ventilstyring og operatørstasjon er for nyere systemer basert på dedikerte feltbusser.

Nødavstengningssystemer er vanligvis designet for å styres og vedlikeholdes fra enheter delt med prosesskontroll. Et slikt konsept kan ha sårbarheter for ondsinnet kode som overtar kontroll av sikkerhetssystemet fra styresystem. For nyere enheter er det strengere krav til tilgangskontroll og programvareoppdatering av sikkerhetssystemene. Systemene er designet for å følge krav i IEC 61508/611. Det brukes dublerte lokalnett med rutbare protokoller mellom kontrollere og operatørstasjon.

Branndeteksjonssystemer er designet som isolerte systemer med lukkede sløyfer mot sensorer og brannmeldere. I oljesektoren er det vanlig at det er automasjonssystemene som viser status på branndeteksjon i kontrollrom, og branndeteksjon og automasjonssystemer er integrert.

Bygging

Først de senere årene har leverandøren innført systemer og rutiner for sikker programvareutvikling. Kun et fåtall har sertifiserte rutiner etter IEC 62443-4-1. Systemer designet etter IEC 61508/611 er ofte bygget og sertifisert etter denne standarden. Det er lite bruk av penetrasjonstesting etter bygging.

Igangsetting

De fleste leverandørene av sikkerhetssystemer har i dag rutiner for å verifisere herding, sikkerhetsoppdatering, kode integritet med mer under igangsetting. Det er økende bruk av penetrasjonstesting. Kun et fåtall har sertifisert organisasjon etter IEC 62443-2-4.

Drift

Intervjuene som er gjennomført viser at ca. halvparten av anleggene har vedlikeholdsavtale med leverandørene som inkluderer oppdatering av sikkerhetsrettelser. For disse systemene gjennomføres oppdatering opp til fire ganger årlig. For anleggene der dette ikke er inkludert i vedlikeholdsavtaler gjennomføres oppdatering primært knyttet til større revisjonsstans. Mange av sikkerhetssystemene er ikke oppdatert på flere år. Noen av anleggene har installert beskyttelse mot ondsinnet kode for sikkerhetssystemene. Det er økende fokus på styringssystem for informasjonssikkerhet innen operasjonelle systemer. De fleste operatørene har etablert eller har pågående prosjekter for å etablere rutiner opp mot ISO 27001, IEC 62443-2-1 eller Norsk olje og gass 104. Amerikanske selskap innfører styringssystem basert på NIST Cyber Security Framework.

Elkraft

Det er økende bruk av elektrisitetsforsyning fra land. Styring av elektriske substasjoner og omformerstasjoner utføres på systemer adskilt fra andre OT og IT systemer. Sikkerhetssystemer (vern) for elkraft er ikke adskilt fra andre elektriske komponenter. Nyere anlegg er basert på IEC 61850 primært for å sikre samtrafikk. Standarden IEC 62351 for å sikre denne kommunikasjonen er fersk og er foreløpig ikke tatt i bruk.

2 ENGLISH SUMMARY

To avoid or limit accidents in oil and gas installations, a number of safety systems have been installed. The function of safety systems is to prevent and mitigate an unwanted event when the process and the plant no longer operate in a normal state. Blow-out prevention, emergency shutdown systems and fire and gas systems are considered the most vital safety systems.

In the past, safety systems were based on mechanical devices or they were isolated self-contained systems with their own control systems. Today, the systems are primarily controlled by digital components and in many cases they are integrated with process control systems. This means that the safety systems have an attack-surface in relation to cyber security incidents.

This report considers how installed safety systems and new systems are secured towards cyber security incidents through:

Design

Blow-out prevention systems are designed to operate isolated. Some systems are connected to data networks for continuous monitoring. Most operators do not allow remote maintenance of such systems. Communication between valve control and user interface is for newer systems based on dedicated field buses.

For emergency shutdown systems and fire and gas systems, these are usually designed to be controlled and maintained from units shared with process control. Such a concept may be vulnerable to incidents where malware or an intruder takes control of the safety system from the control system. For newer devices, there are stricter access control requirements and software update security barriers. The systems are designed to comply with IEC 61508/611 requirements. Duplicated local area networks are used with routable protocols between controllers and user interfaces.

Construction

In the recent years suppliers have introduced systems and routines for secure software development. Only a few have certified development routines according to IEC 62443-4-1. Systems designed according to IEC 61508/611 are normally built and certified to this standard. There is little use of penetration testing of modules after construction.

Commissioning

Most safety system vendors today have routines to verify hardening, security updates and code integrity during commissioning. There is increasing use of penetration testing. Only a few have certified organizations according to IEC 62443-2-4.

Operation

The interviews conducted show that approximately half of the plants have a maintenance agreement with the suppliers including security patching. For these systems, security patches are updated up to four times a year. For the facilities without such agreements, updating is primarily carried out in connection with major revision-stops. Many of the safety systems have not been updated for several years. Some of the facilities have installed malicious code protection for the safety systems. There is an increasing focus on cyber security management systems in operational systems. Most operators have established or have ongoing projects to establish routines based on ISO 27001, IEC 62443-2-1 or Norwegian Oil and Gas Association 104. US companies establishes management system based on the NIST Cyber Security Framework.

Electrical control systems

There is increasing use of electricity supply from shore. Control of electrical substations and converter stations is performed on systems separate from other OT and IT systems. Electricity protection systems are not separate from other electrical components. Newer plants are based on IEC 61850 primarily to ensure interconnection. The IEC 62351 standard to secure this communication is new and is not in use.

3 INNLEDNING

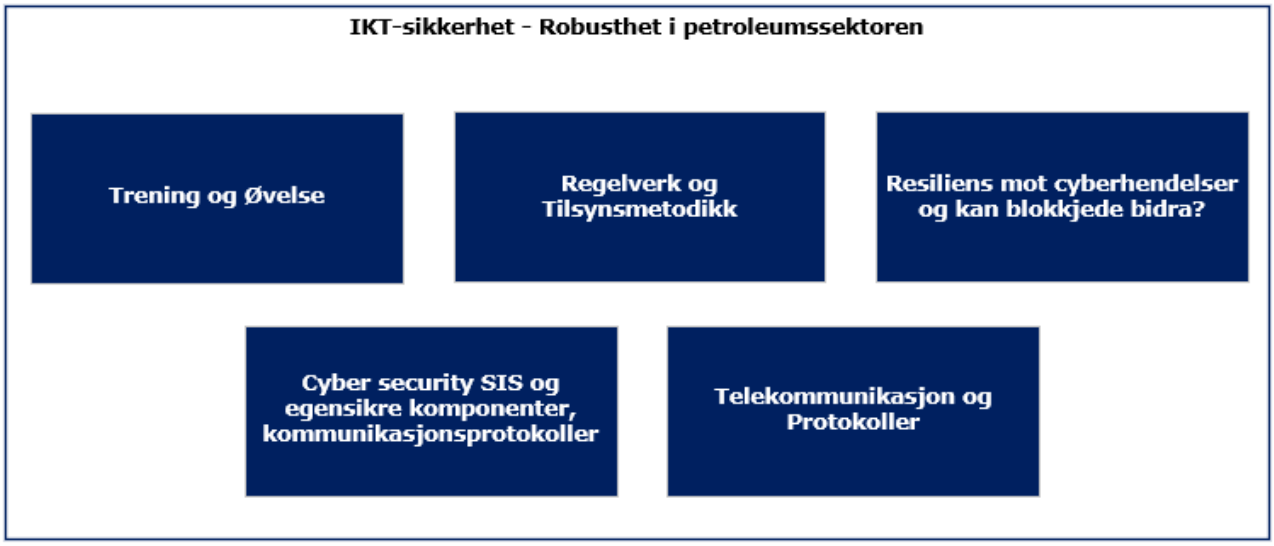
3.1 Bakgrunn

Digitalisering i olje- og gass-sektoren åpner opp for effektivisering, men gjør også sektoren mer sårbar for IKT-sikkerhetshendelser. Olje- og gass-sektoren er et mål for trusselaktører både på grunn av de store verdier sektoren representerer, og for aktivister med idealistisk eller politisk motivasjon.

Utvinning, transport og distribusjon av hydrokarboner medfører en risiko for ulykker med konsekvenser for liv og helse, miljø og materielle verdier. For å redusere risiko for slike ulykker, er det installert en rekke sikkerhetssystemer. Mange av disse sikkerhetssystemene benytter IKT-teknologi og kan være sårbare for IKT-sikkerhetshendelser. Manglende eller feil funksjonalitet i sikkerhetssystemene kan få katastrofale konsekvenser. Det er et mål at IKT-sikkerhetshendelser ikke skal påvirke sikkerhetssystemene.

Petroleumstilsynet gjennomfører en satsing på IKT-sikkerhet i perioden 2018-2021. Målet er å gå i dybden på en del viktige områder, innhente kunnskap om den teknologiske utviklingen og vurdere hvordan dette påvirker risikobildet. Nylig er det publisert rapporter innen temaene «Kunnskap IKT-sikkerhet og CERT» /1/ og «Fjernarbeid og HMS» /2/. Videre pågår det en utredning om «Industriell IKT og IIoT».

Petroleumstilsynet utlyste en konkurranse for å utrede «IKT-sikkerhet – Robusthet i petroleumssektoren», som inneholder flere arbeidspakker og delleveranser, som illustrert i figuren under. Dette oppdraget ble tildelt DNV GL. Alle arbeidspakker har gjennomført intervjuer og innhentet informasjon fra aktørene i bransjen, samt innhentet erfaringer med tilsyn av IKT-sikkerhet i andre sektorer.



Figur 3-1: Delleveranser i prosjektet

Delleveransen «Cyber security SIS og egensikre komponenter, kommunikasjonsprotokoller» er dokumentert i denne rapporten.

3.2 Hensikt

Delleveransen vurderer IKT-sikkerhet i instrumenterte sikkerhetssystemer («Safety Instrumented System» (SIS)). Det er vurdert hvordan IKT-sikkerhet bygges inn i design av slike systemer fra en tidlig fase og hvordan dette ivaretas i bygging, igangsetting og drift. En viktig del av leveransen er å vurdere hvordan sikkerhetsprinsippene beskrevet i IEC 61508/511 /9/ /10/ og IEC 62443 /11/ /12/ /13/ /14/ blir ivaretatt.

Det er vurdert hvordan systemleverandører av SIS implementerer og ivaretar prinsipper for robust IKT-sikkerhet i sine systemer samt hvordan de gjennomfører prosesser for å kontinuerlig ivareta sårbarheter mot nye trusler og angrepsflater.

Videre inkluderer vurderingen systemer som helhet samt enkeltkomponenter som inngår i systemene. Enkeltkomponenter kan være software og hardware noder med tilhørende I/O kort og kommunikasjonsprotokoller. Det er tatt hensyn til vertikal og horisontal kommunikasjon mellom HMI, arbeidsstasjoner, node og I/O, samt node-node (internode) kommunikasjon.

Delleveransen beskriver også trender og utvikling innen industrielle IKT-systemer knyttet til nettverksbaserte komponenter.

IKT-sikkerhet i elektriske anlegg og bruk av IEC 61850 /23/ er vurdert. I dette inngår komponenter for vern og beskyttelse av elektroutstyr samt vertikal og horisontal kommunikasjon med tanke på IKT-sikkerhet i disse systemene.

3.3 Metodikk

For å utrede industriell IKT-sikkerhet i SIS systemene, er det gjennomført litteraturstudier og innhentet erfaringer. Det er gjennomført intervju med 11 aktører i sektoren. Dette inkluderer:

- Operatørselskap
- Leverandører av sikkerhetssystemer
- Teknisk tjenesteleverandør landanlegg
- Leverandører av industrielle kontroll- og sikkerhetssystemer
- Leverandør av landanlegg for forsyning av elektrisk kraft

Drøftinger, analyser og rapportskriving er basert på det innhentede materiale. En oversikt over hvilke aktører som har blitt intervjuet finnes i Appendix A, og intervjuguiden er vedlagt i Appendix B.

Basert på intervjuene er det laget diagrammer som viser fordelinger av sikkerhetstiltak. Antall intervjuer er ikke tilstrekkelig til at dette er representativt for hele sektoren.

Fakta for å belyse drøftingene og analysene er tatt med i egne faktabokser i rapporten.

3.4 Forkortelser og definisjoner

APS	Abandon Platform Shutdown
BOP	Blowout Preventer
CAP	Critical Action Panel
CERT™	Computer Emergency Response Team (Trademark Carnegie Mellon University)
DHSV	Down Hole Safety Valve
E/E/PES	Elektriske, Elektroniske, og Programmerbare Elektroniske Systemer
ESD	Emergency Shutdown
EWS	Engineering Work Station
FPSO	Floating Production Storage and Offloading
HAZOP	Hazard and Operability
HMI	Human Machine Interface
IIoT	Industrial Internet of Things
IKT	Informasjon- og kommunikasjonsteknologi
IKT-sikkerhet	Sikring av IKT systemer. (Engelsk: Cyber Security)
IMS	Information Management System
IOGP	International Oil and Gas Producers Association
IT	Informasjonsteknologi
IEC	International Electrotechnical Commission
NIST	National Institute of Standards and Technology
NSM	Nasjonal Sikkerhetsmyndighet
NVE	Norges vassdrags- og energidirektorat
OLE	Object Linking and Embedding
OPC	OLE for Process Control
OT	Operasjonsteknologi
PHA	Process Hazard Analysis
PLC	Programmable Logic Controller
PLS	Programmerbar Logisk Styring
Ptil	Petroleumstilsynet
RTU	Remote Terminal Unit
SANS	SysAdmin, Audit, Network and Security
SAS	Safety and Automation System
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SPR	Security PHA Review
TSP	Technical Service Provider
USB	Universal Serial Bus
WSUS	Windows Server Update Services

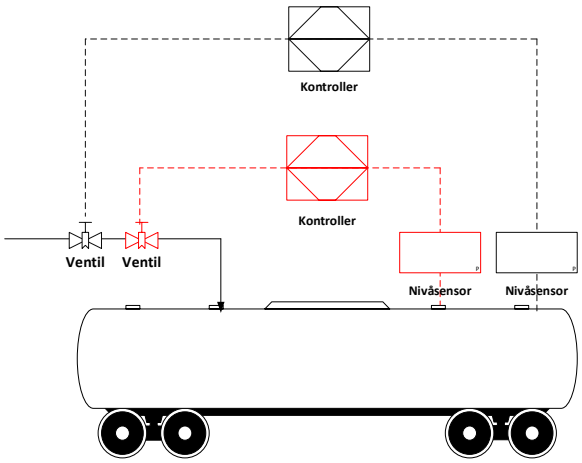
4 SIKKERHETSSYSTEMER I OLJE- OG GASS-SEKTOREN

I dette kapittelet gis en kort introduksjon til sikkerhetssystemer. Deretter gis en kort beskrivelse av vitale sikkerhetssystemer i olje- og gass-sektoren.

Hensikten med sikkerhetssystemer er å forhindre, kontrollere eller redusere konsekvensene av uønskede hendelser når prosessen og anlegget ikke lenger opererer i henhold til en definert normal driftstilstand.

4.1 Prinsipp for sikkerhetssystemer

Figur 4-1 viser et enkelt eksempel på et sikkerhetssystem. For å regulere nivået i en tank, installeres automatiseringssystem (sort) bestående av en nivåsensor, en kontroller (ofte en PLS) og en ventil. Dersom risiko for uhell grunnet for høyt nivå vurderes som uakseptabel, installeres et uavhengig sikkerhetssystem (rødt).



Figur 4-1: Prinsipp for sikkerhetssystem

Dersom automatiseringssystemet ikke evner å holde nivået i tanken under en definert verdi, vil sikkerhetssystemet stenge ventilen.

4.2 Funksjonell sikkerhet

Begrepet funksjonell sikkerhet («functional safety») brukes i standarden IEC 61508 om alle elektriske, elektroniske, og programmerbare elektroniske (E/E/PES) systemer som brukes til å utføre sikkerhetskritiske funksjoner.

IEC 61508 inneholder en generisk tilnærming for all typer av slike systemer i alle industrier, men et hovedpoeng med standarden er å fungere som morstandard for mer industri og produktspesifikke standarder. Typiske eksempler på slike avledede standarder er IEC 61511 (prosessindustri), EN 50126 (jernbane) og ISO 26262 (bilindustri).

I norsk olje- og gassvirksomheten benytter man IEC 61508 og IEC 61511, som begge er referert i Ptils regelverk, bl.a. i veiledningen til Styringsforskriftens /8/ § 5. IEC 61511 blir brukt på systemnivå som rammeverk for analyser, integrering av komponenter, verifikasjon og validering. IEC 61508 er innenfor olje og gass hovedsakelig brukt for utvikling, verifikasjon og validering av fysiske komponenter og programvarekomponenter. IEC 61511 stiller krav om at alle komponenter i en sikkerhetsfunksjon må være utviklet iht. til IEC 61508 og at applikasjonsprogramvaren skal kunne bygges fra slike godkjente programvarekomponenter.

Når man anvender disse standardene vil sikkerhetskritiske funksjoner i et system bli identifisert og allokert et integritetsnivå «Safety Integrity Level» (SIL) basert på risikoanalyser og risikoakseptkriterier.

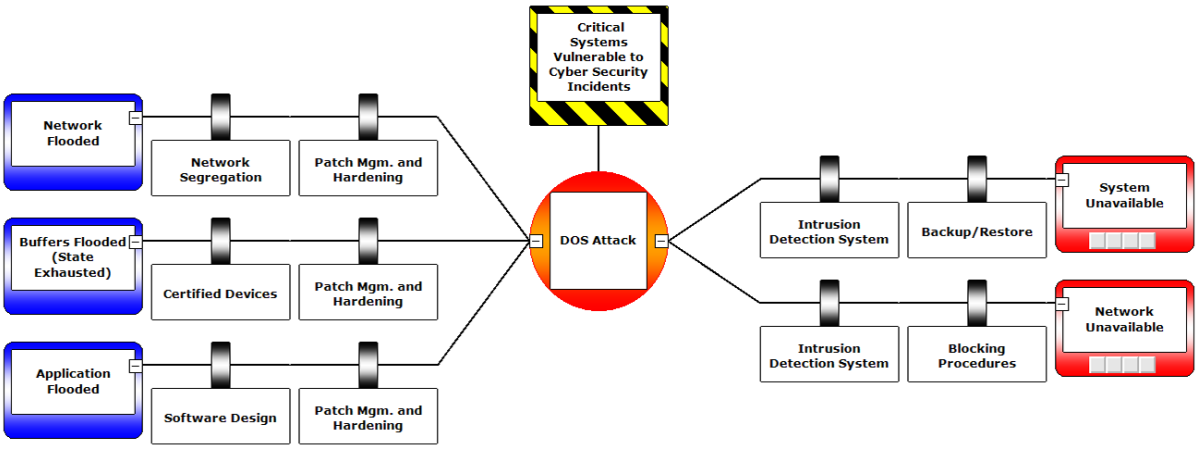
Veiledningsdokument nr. 070 /24/, er Norsk olje & gass sin veiledning til IEC 61511 og IEC61508. Denne veiledningen forenkler prosessen knyttet til bruken av disse standardene gjennom å definere hvilket SIL-nivå som er nødvendig for vanlige sikkerhetsfunksjoner innenfor olje- og gassvirksomheten. Disse SIL-kravene er uavhengige av hva slags risikoakseptkriterier den enkelte operatør måtte ha, samt hva som er risikobildet på det enkelte felt.

Utgave 2 av IEC 61511 fra 2016 har krav om at det skal utføres en IKT-sikkerhets risikoanalyse. Hvis risiko er uakseptabel skal det igangsettes tiltak for å beskytte mot disse truslene.

4.3 Barrierer

Styringsforskriften § 5 setter krav til barrierer som skal identifisere, redusere og begrense feil, fare og ulykkessituasjoner. Prinsipper for barrierestyring i petroleumsvirksomheten er beskrevet i Ptils Barrierenotat /6/. Visualisering av barrierer er også relevant for å visualisere mottiltak («countermeasures») innen IKT-sikkerhet.

Figur 4-2 viser eksempel på barrierer for et tjenestenektangrep («Denial Of Service Attack»).



Figur 4-2: Barrierer tjenestenektangrep

Det skal etableres barrierer som til enhver tid kan
a) identifisere tilstander som kan føre til feil, fare- og ulykkessituasjoner,
b) redusere muligheten for at feil, fare- og ulykkessituasjoner oppstår og utvikler seg,
c) begrense mulige skader og ulemper.

Der det er nødvendig med flere barrierer, skal det være tilstrekkelig uavhengighet mellom barrierene.

Operatøren eller den som står for driften av en innretning eller et landanlegg, skal fastsette de strategiene og prinsippene som skal legges til grunn for utforming, bruk og vedlikehold av barrierer, slik at barrierenes funksjon blir ivaretatt gjennom hele innretningens eller landanleggets levetid.

Det skal være kjent hvilke barrierer som er etablert og hvilken funksjon de skal ivareta, samt hvilke krav til ytelse som er satt til de konkrete tekniske, operasjonelle eller organisatoriske barriereelementene som er nødvendige for at den enkelte barrieren skal være effektiv.

Det skal være kjent hvilke barrierer og barriereelementer som er ute av funksjon eller er svekket.

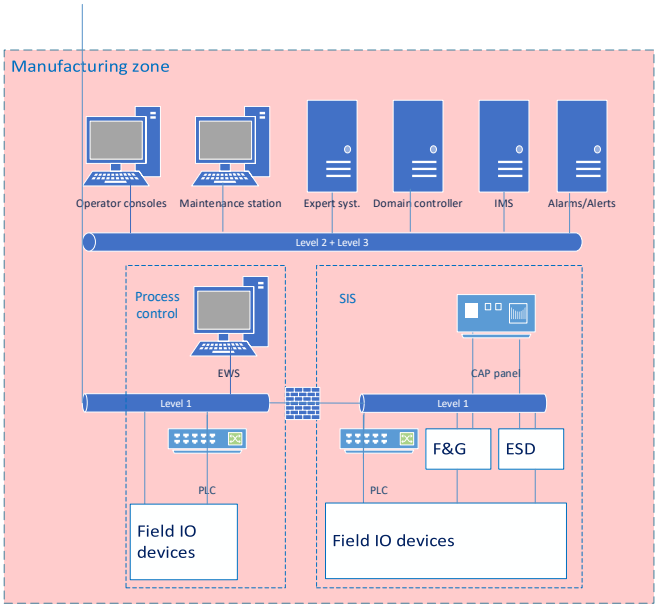
Det skal settes i verk nødvendige tiltak for å rette opp eller kompensere for manglende eller svekkede barrierer.

Faktaboks 1*: Styringsforskriften § 5 (uthevet skrift gjort av DNV GL)*

4.4 Separasjon av sikkerhetssystemer fra prosesskontroll

ISA TR-84.00.09 /18/ standarden beskriver fire prinsipper for å separere sikkerhetssystemer fra industrielle kontrollsystemer. Hensikten er å hindre at en IKT-sikkerhetshendelse som berører industrielle kontrollsystemer skal berøre sikkerhetssystemene:

- Luft-gap – Både logisk og fysisk separasjon. Tillater dedikert kabling for tilstandsovervåkning.
- Tilkoblet – Separat nett for PLS til PLS kommunikasjon. Tillater dedikert kabling for tilstandsovervåkning.
- Integrert 2 sone – To avskilte nett med brannvegg. Tillater kun les kommunikasjon fra sikkerhetssystem til kontrollsystem. Mulig å laste oppdateringer («pull») fra sikkerhetssystemer. Dette prinsippet er vist i *Figur 4-3*.
- Integrert 1 sone - Begge systemer på samme nett. Muliggjør felles operatørstasjon, arbeidsstasjon («EWS») mm. Krever andre tiltak for IKT-sikkerhet.



Figur 4-3: Separasjon av sikkerhetssystem og prosesskontroll: Integrert 2 sone

4.5 Sikkerhetssystemer uten IKT-sikkerhet angrepsflate

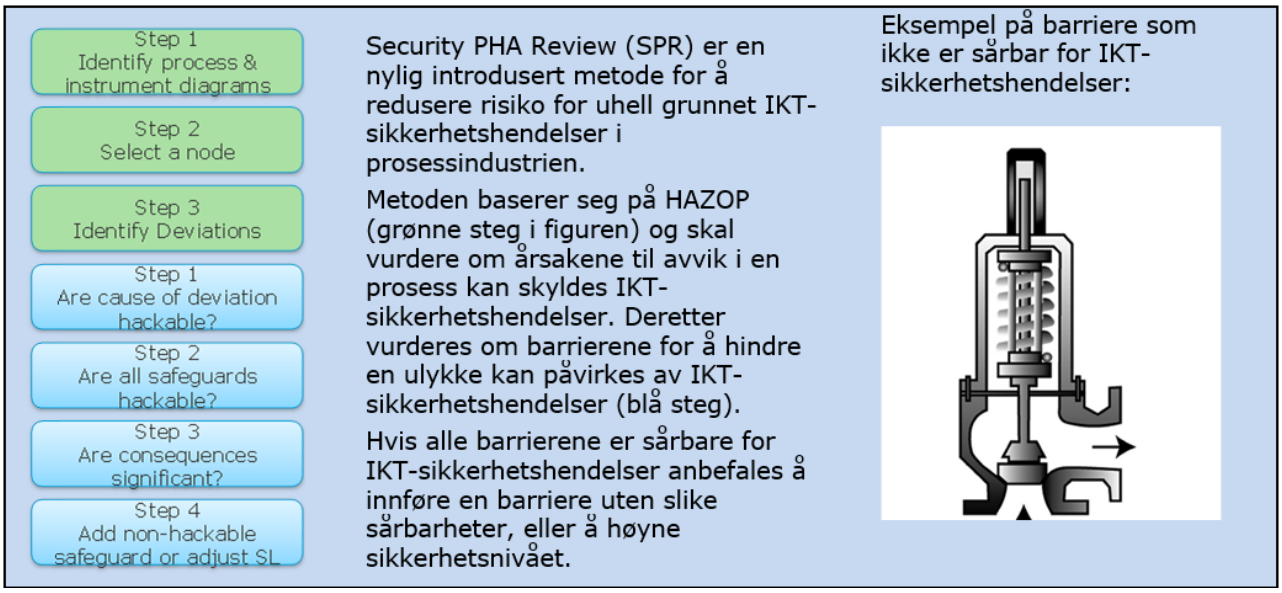
Innretningsforskriftens /7/ § 33 som omhandler nødavstengning beskriver krav til sikkerhetssystem uavhengig av programmerbare system:

> *«Fra bemannet kontrollsenter skal det være en manuell aktiveringsfunksjon som bringer innretningen til en sikker tilstand uavhengig av de programmerbare delene av systemet»*

Dette kravet er mulig å oppfylle fordi aktuatorer i sikkerhetsfunksjonen typisk er fjærbelastet eller trykkbelastet, og går til sikker tilstand dersom energien som virker mot fjær/trykk forsvinner. Dette gjør det mulig å aktivisere sikkerhetsfunksjonene ved å kutte strømmen til disse systemene.

Kravet om nødavstengning uavhengig av programmerbare system påvirker utformingen av «Critical Action Panel» (CAP) paneler i kontrollrom. Disse er direkte kablet («hard wired») til sikkerhetskontrollerne.

Det er introdusert risiko metodikker som baserer seg på HAZOP og som favoriserer bruk av sikkerhetssystem uten IKT-sikkerhet angrepsflate som et element i barrieresikringen (Se *Faktaboks* 2).



Faktaboks 2: Security PHA Review (SPR) /24/, metode for å redusere uhell forårsaket av sikkerhetshendelser

4.6 Instrumenterte sikkerhetssystem (SIS)

Et instrumentert sikkerhetssystem («Safety Instrumented System» (SIS)) er et system som brukes til å implementere en eller flere sikkerhetsfunksjoner ved å bruke elektriske, elektroniske eller programmerbare elektroniske teknologier sammen med andre aktive (f.eks. mekaniske) teknologier. Begrepet stammer fra IEC 61511 og brukes i praksis om nødsystemer som tar systemet til sikker tilstand ved behov, og som er utviklet iht. til denne standarden. Mange sikkerhetssystemer som brukes innenfor olje og gass er i praksis av typen SIS, og de viktigste av disse er beskrevet nedenfor. Som eksempler på sikkerhetssystemer som ikke er instrumenterte kan nevnes overtrykkssikringssystemet gjennom overtrykkssikringsventiler («pressure relief valve» (PSV)) eller sprengblekk samt dreneringssystem som samler og leder brennbar væske til sikkert område.

4.6.1 Utblåsningssikring

Under boreoperasjoner benyttes utblåsingssikring («blowout preventer» (BOP)). En BOP består av store spesialutviklede ventiler eller tilsvarende mekaniske innretninger som brukes til å kontrollere og om nødvendig forsegle olje- og gassbrønner for å unngå utblåsning. Dersom brønnen kommer helt ut av kontroll, kan BOP-en kutte borestrengen og forsegle brønnen.

En BOP kontrolleres primært fra en egen operatørstasjon (HMI) på plattformen. I dag er dette digitale systemer. Systemer for utblåsingssikring er adskilt fra andre systemer (se kapittel 4.4) og operatørselskapene tillater generelt ikke fjernvedlikehold.

Etter Deepwater Horizon ulykken (se *Faktaboks* 3) innførte amerikanske myndigheter krav om kontinuerlig overvåkning av systemet for utblåsingssikring. Dette medførte at BOP systemene ble tilkoblet datanett for å overføre informasjon om driftsstatus. Det finnes slike løsninger også på norsk sokkel.

Den 20. april 2010 skjedde en utblåsing, eksplosjon og brann om bord på den flyttbare innretningen Deepwater Horizon i Mexicogolfen. Hendelsen utviklet seg umiddelbart til en katastrofe. Elleve av de som var om bord da ulykken inntraff, omkom, og flere fikk alvorlige skader. Innretningen sank etter to døgn. Mer enn fire millioner fat olje strømmet ukontrollert ut av brønnen før lekkasjen ble stoppet 87 dager senere etter omfattende forsøk på å tette brønnen og ved hjelp av avlastningsboring.

Deepwater Horizon var utstyrt med de mest moderne, databaserte sikkerhetssystemer relatert til overvåkning av brønn, avstengning av brønn, frakopling av rigg, kraftforsyning, deteksjon og varsling av mannskap. Under ulykken sviktet disse sikkerhetssystemene helt eller delvis.

Det ble i den påfølgende granskning påvist at det var kjent at flere av informasjonssystemene hadde feil og mangler og at dette var blitt ignorert og akseptert. Det var flere kjente programvarefeil på riggen. Datamaskinene som kontrollerte boreoperasjonene fungerte dårlig og noen av riggens alarmsystemer, inkludert riggens generelle alarmsystemer, var slått av. Dette medførte at selv om sensorer på riggen registrerte høye gassnivåer, giftig gass eller brann, og overførte disse signaler til brann- og gassvarslingssystemet, så ble ingen alarm aktivert.

Utblåsningssikringen (BOP) stengte ikke av brønnen slik den skulle gjøre. Det er uklart om den ble skadet under ulykken eller om den allerede var i ustand. Det var gjort observasjoner av lekkasjer fra BOP-ens hydrauliske kontrollsystem uten at man hadde gjort noe med dette. Myndighetene hadde krevd en resertifisering av BOP-en, men dette ville nødvendiggjøre en nedstengning i 90 dager, og var ikke utført.

Faktaboks 3: Deepwater Horizon ulykken

Utblåsningssikring for produserende brønner består av primære- og sekundære barriereelementer. I de primære barriereelementene inngår nedihullsventil («Down Hole Safety Valve», (DHSV)), som kontrolleres fra plattform. I de sekundære barriereelementene inngår ventiltre («juletre») som bl.a. inneholder øvre hovedventil og vingeventil som er hydraulisk opererte. Kuttes strømtilførsel, vil disse ventilene stenge.

4.6.2 Brann & Gass

Systemer for deteksjon av brann og gass, samt slukkesystemer, er installert på alle installasjoner.

Branndeteksjon utføres av dedikerte systemer med sensorer for røyk, varme og flamme, samt manuelle alarmbrytere. Slike enheter er koblet i redundante sløyfer. Branndeteksjonssystemene kommuniserer med egne brann og gass noder i det sentrale sikkerhetssystemet.

Sensorer for deteksjon av gass er normalt tilkoblet direkte til brann og gass noder i det sentrale sikkerhetssystemet.

Brann og gass nodene har som hovedoppgave å sikre hurtig og pålitelig deteksjon. Disse alarmene danner grunnlag for manuell aktivering av slukkesystemer samt de sendes til nødavstengingssystemet for automatisk avstenging av ventilasjon og isolering av tennkilder.

Innretninger skal ha et brann- og gassdeteksjonssystem som sikrer hurtig og pålitelig deteksjon av branntilløp, branner og gasslekkasjer. **Systemet skal kunne utføre tiltenkte funksjoner uavhengig av andre systemer.**

Ved brann- eller gassdeteksjon skal automatiske aksjoner begrense konsekvensene av brannen eller gasslekkasjen. Plassering av detektorer skal baseres på aktuelle scenarier og simuleringer eller tester.

Faktaboks 4: Innretningsforskriften § 32 (tekst uthevet av DNV GL)

4.6.3 Nødavstengningssystem (ESD)

Et nødavstengningssystem («Emergency Shutdown System», (ESD)) skal hindre utvikling av fare- og ulykkessituasjoner og begrense konsekvenser. Sikkerhetsfunksjoner som f.eks. avstenging av brønner og stigerør, trykkavlastning og nedstenging av elektrisk kraftsystemer utføres av ESD-systemet basert på manuell aktivering, eller automatisk basert på bekreftet brann/gass.

Sikkerhetsfunksjonene er klassifisert i et hierarki, der NORSOK S-001 /21/ definerer nivåene APS («Abandon Platform Shutdown»), ESD1, ESD2 og PSD («Process Shutdown System»). APS kan bare aktiveres manuelt og benyttes ved full evakuering av plattform.

Mindre nødavstengningssystemer kan være hydrauliske eller basert på releer (ikke programmerbare).

Landbaserte lagrings- og produksjonsanlegg kan ha store volumer av eksplosjonsfarlige stoffer som ikke raskt kan trykkavlastes i en nødsituasjon. Det anvendes derfor seksjonalisering i en nødsituasjon hvor trykkavlastning gjøres etter gitte sekvenser som er tilpasset dimensjoneringen av rørsystemer og faklingskapasitet. Dette medfører et mer komplekst nødavstengningssystem som må fungere over lengre tid.

Innretninger skal ha et nødavstengningssystem som kan hindre utvikling av fare- og ulykkessituasjoner og begrense konsekvensene av ulykker, jf. § 7. **Systemet skal kunne utføre tiltenkte funksjoner uavhengig av andre systemer.**

Nødavstengningssystemet skal utformes slik at det går til eller forblir i en sikker tilstand dersom det oppstår en feil som kan hindre systemet i å virke. Nødavstengningssystemet skal ha en enkel og entydig kommandostruktur. Systemet skal kunne utløses manuelt fra utløsningsstasjoner som er plassert på strategiske steder på innretningen. Fra bemannet kontrollsenter skal det være en manuell aktiveringsfunksjon som bringer innretningen til en sikker tilstand uavhengig av de programmerbare delene av systemet.

Det skal installeres nødavstengningsventiler som kan stanse hydrokarbon- og kjemikaliestrømmer til og fra innretningen og til og fra brønner, og som isolerer og/eller seksjonaliserer brannområdene på innretningen.

Faktaboks 5: Innretningsforskriften § 33 (tekst uthevet av DNV GL)

5 IKT-SIKKERHET I SIS SYSTEMER

I dette kapittel diskuteres hvordan sikkerhetssystemene som beskrevet i kapittel 4.6 er sikret mot ondsinnede hendelser der trusselaktøren benytter datamaskiner eller datanett. Kapittelet er delt opp i de forskjellige fasene til systemene i et livssyklus.

For å antyde hvilke angrepsflate for IKT-sikkerhetshendelser som har størst fokus innen OT og kontrollsystemer vises det til svarene fra SANS undersøkelsen i 2019 /19/. Disse tallene gjelder for alle industrier.

Tabell 5-1: De viktigste angrepsflater for IKT-sikkerhetshendelser innen OT/kontrollsystemer (Kilde SANS)

Viktige angrepsflater 2019	% Respons
Fysisk tilgang (USB stikker, direkte tilgang til utstyr)	56,3%
Fjerntilgang (utenfor tiltenkt bruk/arkitektur)	40,6%
Tiltrodd fjerntilgang (gjennom tiltenkt bruk/arkitektur)	37,5%
Tjenester for vedlikehold og service (endringer av konfigurasjon)	34,4%
Leveransekjede (endret HW og SW, oppgradering av «firmware», «patching», vedlikehold av verktøy/utstyr)	18,8%

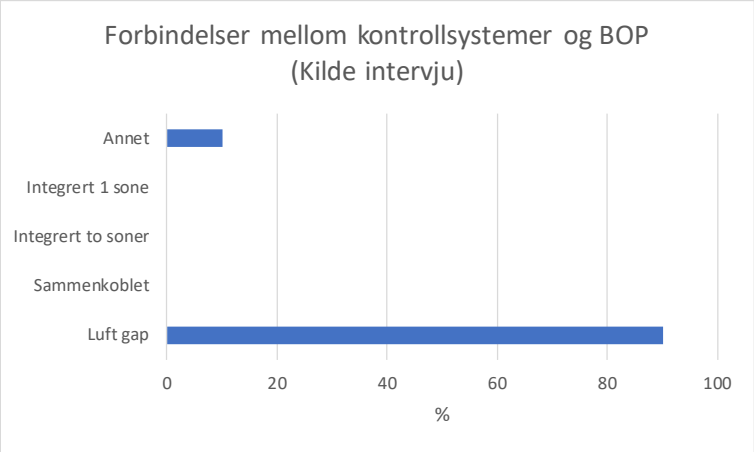
Flere av de intervjuede operatørene og leverandørene har vært aktiv i utvikling av et beste praksis dokument /5/ for bruk av 62443 standarden, og bruker denne for alle livssyklus fasene til systemene.

Utgave 2 av IEC 61511 fra 2016 har fått krav om å gjennomføre risikoanalyse i forhold til IKT sikkerhet (se kapittel 4.2). Videre skal det gjennomføres tiltak for å redusere slik risiko. Sikkerhetssystemer som sertifiseres eller legger disse standardene til grunn vil i måtte innarbeide ikt-sikkerhet i alle fasene.

5.1 Design

Majoriteten av sikkerhetssystemene i olje- og gassektoren er designet i en tid der det ikke var fokus på IKT-sikkerhetshendelser. Først i de seneste årene har leverandørene utarbeidet rutiner for å innarbeide IKT-sikkerhetskrav i design. For BOP-er (se kapittel 4.6.1) som er utviklet i USA blir NIST krav /15/ lagt til grunn, mens de europeiske SAS («Safety and Automation Systems») leverandørene i økende grad benytter IEC 62443. Nasjonale myndighetskrav og veiledninger gir føringer for design. F.eks. Innretningsforskriften §32 og §33 gir klare føringer til uavhengighet mellom sikkerhetssystemer og andre systemer. Det er en tendens til at leverandører ikke innfører IKT-sikkerhetsløsninger med mindre operatørene krever det samtidig som at mindre operatører ikke innfører IKT-sikkerhetsløsninger med mindre myndighetene setter krav.

Det finnes både BOP-systemer (se kapittel 4.6.1) sertifisert etter IEC 61511/508 og systemer som ikke er designet etter denne standarden. BOP-systemene er i hovedsak designet adskilt fra kontrollsystemer med luft-gap (se kapittel 4.4). Det er under intervjuene referert til et fåtall boreskip der det er åpnet for fjernvedlikehold og installasjoner der tilstanden på systemene kommuniseres til eksterne systemer, se *Figur 5-1* (se kapittel 3.3 om det statistiske grunnlaget for tallene).

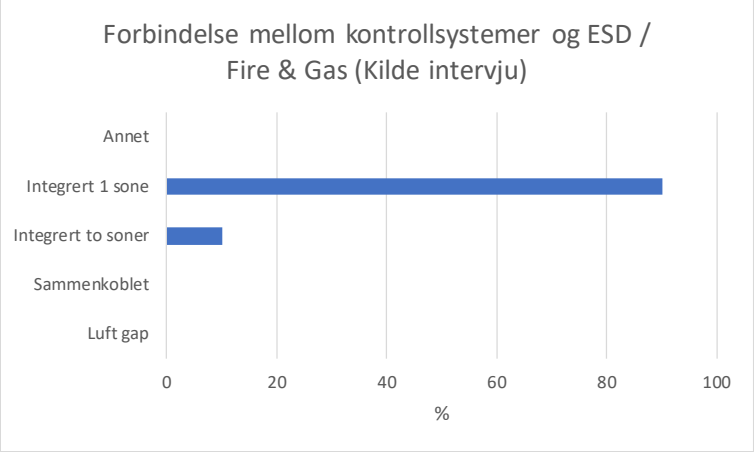


Figur 5-1: Forbindelser mellom kontrollsystemer og BOP (Kilde intervju)

Nødavstengningssystemer (se kapittel 4.6.3) og brann- og gass-systemer (se kapittel 4.6.2), har lagt IEC 61511/508 standardene til grunn i design, bygging og igangsetting. Under intervjuene ble det for det meste identifisert nødavstengningssystemer og sentrale deler av brann og gass-systemer som var designet på samme nett som kontrollsystemene («Integrert 1 sone») (se kapittel 4.4). Dette for å kunne benytte felles operatørstasjon og arbeidsstasjoner («Engineering Work Station» (EWS)) samt for å forenkle datainnsamling. Det var et fåtall installasjoner der operatør har krevd adskilte systemer, se *Figur 5-2* (se kapittel 3.3 om det statistiske grunnlaget for tallene).

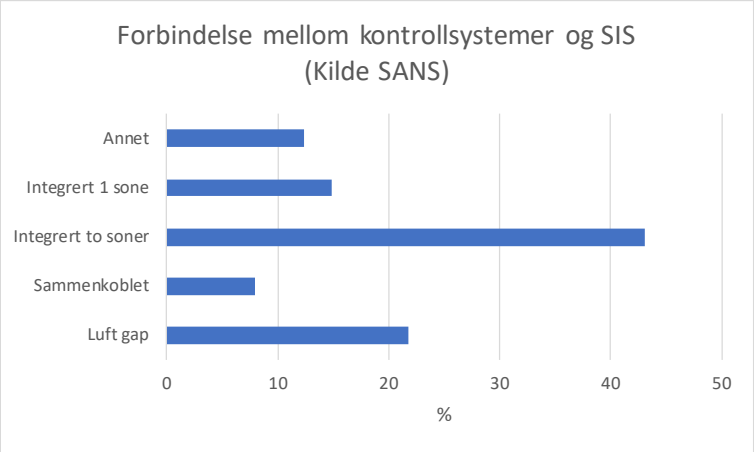
Dersom et sikkerhetssystem styres eller vedlikeholdes fra en operatørstasjon eller en arbeidsstasjon (EWS) tilknyttet felles nett, kan en slike stasjoner benyttes til målrettede angrep mot sikkerhetsfunksjonen (Se *Faktaboks* 6). Leverandørene mente at protokoller mellom sikkerhetssystemer og operatørstasjon hadde mekanismer for å sikre integritet, men det er ikke benyttet kryptering eller digitale sertifikat for autentisering av endepunkter. Det forventes at det vil bli økt fokus på sikkerhet i slike protokoller (se kapittel 6.2).

Branndeteksjonssystemer er integrert med brann & gass-systemene vanligvis med dedikerte nett.



Figur 5-2: Forbindelser mellom kontrollsystemer og ESD / Brann og Gass (Kilde intervju)

Praksisen i olje- og gassindustrien med å koble ESD og Brann og gass til samme nett som andre kontrollsystemer avviker fra praksis i annen industri. SANS undersøkelse innen OT/kontrollsystemer 2019 /19/ viser praksis for separasjon av sikkerhetssystemer og kontrollsystemer i annen industri, se *Figur 5-3*.



Figur 5-3: Forbindelser mellom kontrollsystemer og SIS (Kilde SANS)

STUXNET fra ca. 2010 var en øye-åpner for at industrielle kontrollsystemerer er sårbare for ondsinnet-kode. På samme måte var skadevaren TRITON i 2017 en øyeåpner for at sikkerhetssystemer er sårbare. TRITON var antakelig den første ondsinnede koden som var laget for å skade et sikkerhetssystem.

Det ble oppdaget etter et angrep mot et energiselskap i Midtøsten der en angriper fikk tilgang til en «engineering workstation» for et sikkerhetssystem og plantet skadevaren. Til alt hell, var det feil i koden slik at systemet stengte ned før angrepet gjorde omfattende skade.

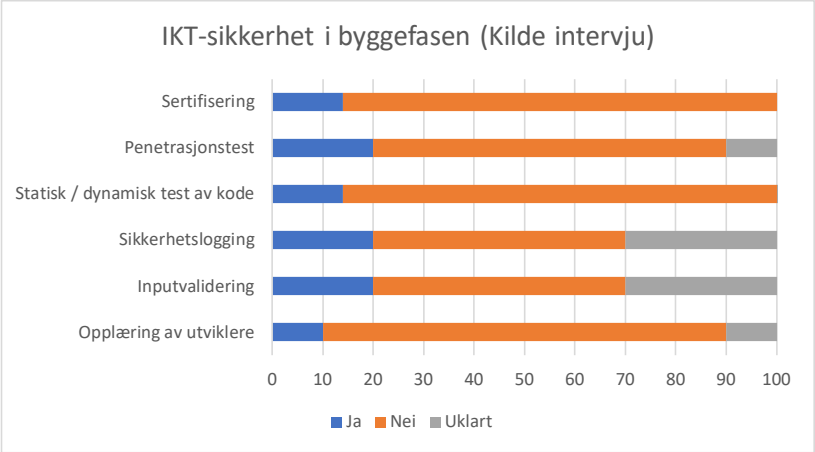
TRITON (også kalt TRISIS) er et rammeverk utviklet for å angripe Triconex Safety Instrumented System (SIS) kontrollere fra Schneider Electric. Det benytter Tristation protokollen for å sende kommandoer, lese minne og omprogrammere. Det kan eksempelvis stoppe enheten med en «halt» kommando.

Faktaboks 6: Skadevaren Triton og angrep på SIS

5.2 Bygging

Toneangivende leverandører av programvare innen IT har etablert regimer for sikker programvareutvikling (Se *Faktaboks* 7). Leverandørene av sikkerhetssystemer har i liten grad tatt i bruk regimer for sikker programvareutvikling, men det er sterkt økende fokus på dette. Kun en av de intervjuede leverandørene var sertifisert etter IEC 62443-4-1. En av BOP produsentene benyttet verktøy for statisk kildekodeanalyse, og et fåtall benyttet standardbiblioteker for inputvalidering. De fleste systemene hadde løsninger for felles sikkerhetslogging.

Figur 5-4 viser leverandørenes svar på sikker programvareutvikling under byggefasen (se kapittel 3.3 om det statistiske grunnlaget for tallene).



Figur 5-4: IKT-sikkerhet programvareutvikling SIS (Kilde Intervju)

Det er utviklet flere rammeverk for å styre sikkerhet og personvern gjennom alle fasene av programvareutvikling. Kjente rammeverk er Microsoft SDL («Software Development Lifecycle») og OWASP S-SDLC («Secure Software Development Lifecycle Project»). ISO 27001 standarden setter overordnede krav til sikker programvareutvikling mens IEC 62443-4-1 setter detaljerte krav til sikkerhet både i design og programvareutvikling. Elementer som inngår i et slikt rammeverk vil bl.a. være:

- Opplæring
- Inputvalidering
- Sikkerhetsrelatert logging
- Bruk av kryptografi og signering
- Bruk av verktøy og sikkerhetsbibliotek
- Statisk og dynamisk test av kode
- Penetrasjonstesting

Faktaboks 7: Rammeverk for sikker programvareutvikling

5.3 Leveransekjede

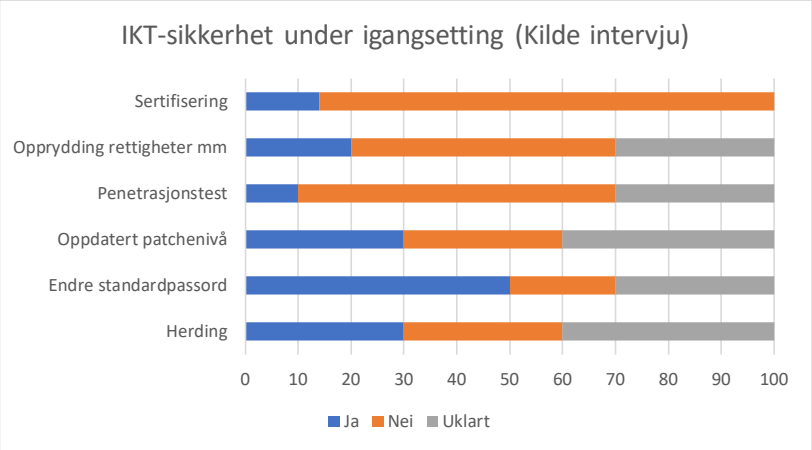
Det er bekymring knyttet til om programvare i sikkerhetssystemer kan endres av ondsinnede aktører etter at den er utviklet av produsent og frem til produktet settes i drift. Mens det tidligere var vanlig å levere produktene med preinstallert programvare, er det i dag vanlig at leverandøren laster ned programvare over nettet under igangsetting.

Det er lite bruk av digital signering for å sikre integritet på programvaren. Noen leverandører har manuelle rutiner for å verifisere integritet basert på en sjekksum.

5.4 Igangsetting

Under sikkerhetsverifikasjon og test av sikkerhetsløsninger er det avdekket at flere av sårbarhetene skyldes manglende rutiner under igangsetting («Commissioning»). Det har i de siste årene vært økende fokus på dette, og både produktleverandører og systemintegratorer («Engineering and Procurement Construction» (EPC)) er i ferd med å etablere rutiner. Kun en av de intervjuede leverandørene var sertifisert etter IEC 62443-2-4. Denne standarden setter krav til funksjoner som herding av komponenter, endring av standardpassord, oppdatering av sikkerhetsrettelser («patching») og sikkerhetstesting av løsningen. Det siste er spesielt viktig fordi det under igangsettingsfasen vil være mange personer som har hatt tilgang til systemene og det kan være gjort temporære åpninger i brannvegger mm. Oppryddingsrutiner og testing skal lukke slike avvik.

Figur 5-5 viser leverandørene svar på sikkerhetstiltak under igangsettingsfasen (se kapittel 3.3 om det statistiske grunnlaget for tallene).



Figur 5-5: IKT-sikkerhet under igangsetting av SIS (Kilde Intervju)

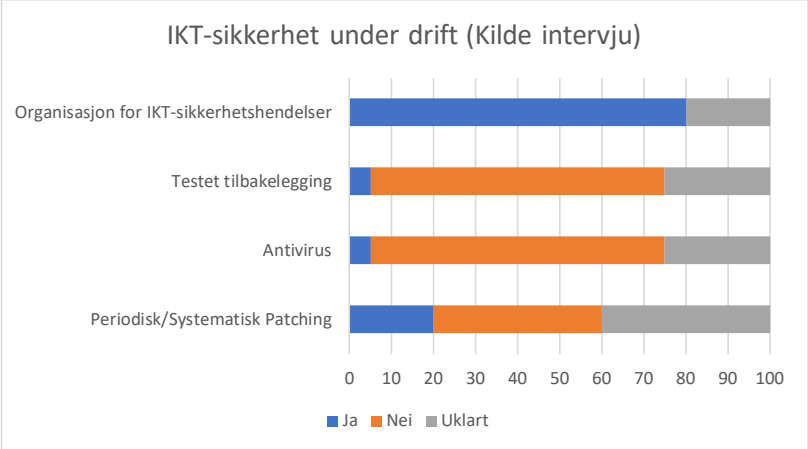
5.5 Overlevering til drift

Det er utfordringer knyttet til overlevering av løsninger fra en utbygger-organisasjon til en driftsorganisasjon. Sikkerhetsløsningene må overvåkes og vedlikeholdes fra dag en i drift. Generelt er det rom for forbedringer både knyttet til dokumentasjon og opplæring.

5.6 Drift

Det er normalt operatørene som drifter faste installasjoner på norsk sokkel. Flytende produksjonsenheter (FPSO) kan også driftes av eierorganisasjon og boreinstallasjoner driftes av boreoperatør. Landanlegg som betjener leveranser fra flere operatører driftes av «Technical Service Provider» (TSP).

I denne sammenheng er det sett på driftsoppgaver som påvirker sikkerhetssystemene i forhold til IKT-sikkerhetshendelser. *Figur 5-6* viser driftsorganisasjonenes svar på sikkerhetstiltak under drift (se kapittel 3.3 om det statistiske grunnlaget for tallene).



Figur 5-6: IKT-sikkerhet under drifting av SIS (Kilde Intervju)

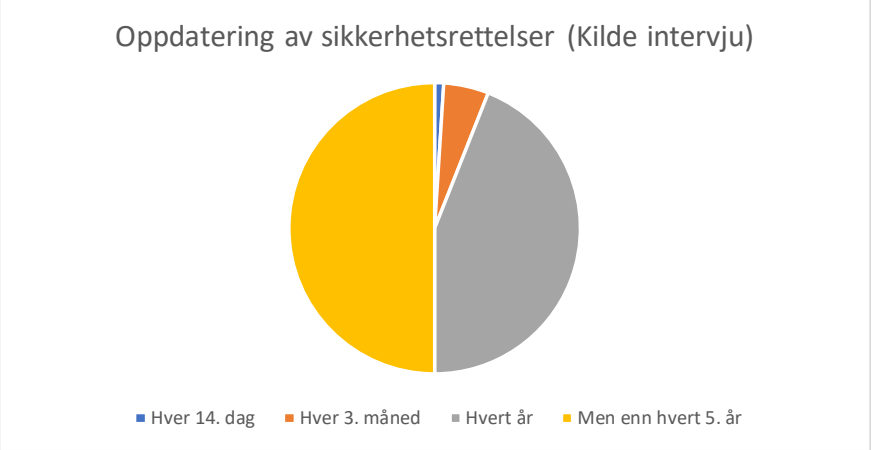
Det er økende fokus på styringssystem for informasjonssikkerhet innen industrielle systemer. De fleste operatørene har etablert eller har pågående prosjekter for å etablere rutiner basert på standarder utledet av ISO 27001 /4/ som IEC 62443-2-1 og Norsk olje & gass 104 /3/. Noen selskap baserer rutinene for driftsfasen på NIST Cyber Security Framework /15/.

5.6.1 Oppdatering av sikkerhetsrettelser

Sikkerhetshendelser er ofte grunnet i svakheter i programvare hvor det allerede finnes rettelser utarbeidet og distribuert av leverandørene. Det er derfor et ønske om å installere relevante rettelser så ofte som mulig. Her oppleves ofte et dilemma for industrielle installasjoner, og spesielt sikkerhetssystemer. Oppetid for disse systemene er kritisk, og alle endringer kan påvirke oppetid. Rettelsene må derfor være godkjent av alle berørte leverandører og de må være testet på produksjonslike anlegg før de utføres på produksjonsanlegget. Dette medfører at det er stor variasjon på hvor ofte sikkerhetssystemene blir oppdatert. Installasjoner som automatisk henter godkjente oppdatering fra leverandørene til en lokal server (f.eks. WSUS server) er hyppigere oppdatert enn installasjoner der nedlasting og godkjenning utføres manuelt. Windows operativsystem krever hyppigere oppdateringer enn programvare i kontrollere.

Ca. halvparten av anleggene har vedlikeholdsavtale med leverandørene som inkluderer oppdatering av sikkerhetsrettelser. For disse systemene gjennomføres oppdatering opp til fire ganger årlig. For anleggene der dette ikke er inkludert i vedlikeholdsavtaler gjennomføres oppdatering primært knyttet til større revisjonsstans. Mange av sikkerhetssystemene er ikke oppdatert på flere år.

Oppdateringsintervallene for sikkerhetssystemene er angitt i *Figur 5-7* basert på tilbakemeldinger i intervjuene (se kapittel 3.3 om det statistiske grunnlaget for tallene).



Figur 5-7: Oppdatering av sikkerhetsrettelser på SIS (Kilde Intervju)

5.6.2 Oppdatering av antivirus programvare

Det er varierende bruk av antivirusbeskyttelse på sikkerhetssystemer. Dette skyldes at leverandørene ikke godkjenner slik programvare, at operatørene er redd for tidsforsinkelser grunnet antivirus prosessen og at det har vært tilfeller av at systemene feiler («blå-skjerm») etter oppgradering av signaturfiler. Manglende antivirusbeskyttelse på systemene kompenseres for mange installasjoner med rutiner og utstyr for virusvask av portable media samt at løsninger for filoverføring til systemene har antivirus kontroll.

5.6.3 Sikkerhetskopiering og tilbakelegging

Det er utarbeidet planer for beredskap («Disaster recovery») og det tas sikkerhetskopier av operativsystem, programvare og konfigurasjon. Etter hendelsene med løsepengevirus (se *Faktaboks* 8) har det blitt økt fokus på sikkerhetskopiering («back-up») på media som ikke påvirkes av viruset og test av tilbakelegging («restore») på tomme systemer («from scratch»). Noen av installasjoner har hatt hendelser/feilsituasjoner slik at man har fått praktisert tilbakelegging, men det er i liten grad identifisert planlagte og gjennomførte tester av tilbakelegging. Flere leverandører har tjenester der de oppbevarer kopier av både operativsystem, programvare og konfigurasjon/innstillinger. Disse kopiene kan være utdatert og ikke inneholde oppdatert konfigurasjon og innstillinger.

Løsepengevirus er en type ondsinnet programvare som truer med å publisere eller å blokkere tilgang til data med mindre det innbetales løsepenger. Løsepengene skal vanligvis innbetales i kryptovaluta («bitcoin») for at mottaker ikke skal kunne identifiseres. Data blokkeres vanligvis ved at de krypteres og ved innbetaling av løsepenger, skal det gis tilgang til krypteringsnøkkel.

Den ondsinnede programvaren NotPetya rammet en rekke industrielle installasjoner inklusive olje- og gassektoren i 2017. Windows baserte systemer stoppet og måtte reinstalleres. Boreinstallasjonene til Maersk var bl.a. utilgjengelig i 6 dager; noe som medførte vesentlige økonomiske tap og tap av omdømme. NotPetya viste seg å være en sletteorm («Wiperware») ettersom innbetaling av løsepengene ikke medførte at data kunne gjenskapes. LockerGoga er et løsepengevirus som angrep Hydro i 2019.

Faktaboks 8*: Løsepengevirus*

5.6.4 Håndtering av sikkerhetshendelser

De fleste operatører på norsk sokkel har etablert rutiner og ansvarsforhold for å håndtere sikkerhetshendelser. Omfanget av disse rutinene er varierende. De intervjuede operatørene hadde også gjennomført øvelser.

Internasjonale standarder som ISO/IEC 27035 /16/ og NIST SP 800-61 /17/ er ofte lagt til grunn for arbeidet, men det er ikke identifisert noen sertifiseringer eller verifikasjon av samsvar med standardene.

Det er lite bruk av «Intrusion Detection System» (IDS) eller annet utstyr som kan detektere ulovlig/ondsinnet datatrafikk på nett tilknyttet sikkerhetssystemer.

5.7 Håndtering av nye trusler og angrepsflater («Lifecycle security management»)

De store operatørselskapene har etablert egne respons grupper («Computer Emergency Response Team» (CERT™)) som holder seg oppdatert på trusselsituasjonen. Noen mindre operatører har tilknyttet seg eller vurderer å tilknytte seg KraftCERT (Se *Faktaboks* 10).

Flesteparten av leverandørene av sikkerhetssystemer tilbyr tjenester for drift og overvåkning av produktene. Sentralt i disse løsningene er tjeneste for å utvikle og oppdatere sikkerhetsrettelser. Ettersom oppdatering av sikkerhetsrettelser er ressurskrevende, er det viktig å kun installere kun relevante rettelser. For å følge med på trusselbildet har leverandørene egne respons grupper, eller de

baserer seg på eksisterende varslingstjenester som CISA («Cybersecurity and Infrastructure Security Agency») (Se *Faktaboks* 9) og nett-tjenester med oversikt over sårbarheter («Vulnerability databases»).

CISA er en organisasjon i USA under Department of Homeland Security.

CISA er landets rådgiver innen IKT-sikkerhet, og arbeider med flere partnere for å beskytte landet mot dagens trusler, og samarbeider for å bygge en sikrere og mer motstandsdyktig infrastruktur for å kunne stå imot fremtidige trusler.

CISAs har bl.a. varsling av trusler og sårbarheter for industrielle kontrollsystemer.

Faktaboks 9*: Cybersecurity and Infrastructure Security Agency (CISA)*

KraftCERT har til formål å overvåke energiselskapers IT-systemer og håndtere uønskede IKT-sikkerhetshendelser, og skal bistå andre aktører i kraftbransjen i Norge (kraftprodusenter og nettselskaper) med håndtering og forebygging av angrep på IKT-systemer.

KraftCERT jobber for bedre sikring i prosesskontroll-systemer ved å bistå kraftbransjen slik at de skal være oppdatert om relevante sårbarheter og trusler, og at de skal være i stand til å detektere og motvirke digitale angrep.

KraftCERT bistår også i håndtering av digitale sikkerhetshendelser og er med i den nasjonale beredskapsorganisasjonen.

KraftCERT er et norsk aksjeselskap, etablert av Statnett, Statkraft og Hafslund Nett, etter initiativ fra NorCERT og Norges Vassdrags- og energidirektorat (NVE)

Faktaboks 10*: KraftCERT – Kraftsektorens Computer Emergency Response Team*

6 TRENDER OG UTVIKLING

6.1 Safety 4.0

Termen Safety 4.0 er innført som en visjon om oppgradering av sikkerhet for å støtte opp under «den fjerde industrielle revolusjon» - Industry 4.0 eller «Industrial Internet». Industry 4.0 skal muliggjøre ett tett samspill mellom intelligente enheter («cyber physical systems»), avanserte analyse og mennesker.

Innen norsk olje og gassektor er det igangsatt er Safety 4.0 prosjekt som skal adresserer behovet for et felles rammeverk og en metode som kan demonstrere sikkerhet for ny teknologi som avviker fra gjeldende praksis. Prosjektet fokuserer på undervannsteknologi ettersom det forventes at ca. 3 av 4 funn på norsk kontinentalsokkel vil bli utviklet ved hjelp av undervannsløsninger.

Prosjektet utreder undervannsinstallasjoner der alt styres og sikres av elektriske system «all-electric subsea». Slike «all-electric subsea» installasjoner har vært prøvet ut på nederlandsk sektor siden 2008, men de første installasjonene har hatt tradisjonelle hydrauliske sikkerhetsventiler. Industrien ønsker å videreutvikle konseptet og gå bort fra fjærbelastede ventiler. Det betyr i så fall at man går bort fra kravet i PTILs regelverk om å kunne kjøre nødstengning uten bruk av programmerbare systemer, og man vil bli avhengig av et programmerbart safety systemet subsea for å få stengt. I dag har man ikke noe programmerbart safety system subsea, man kutter bare strømmen topside, og så går alt subsea til sikker tilstand elektromekanisk. Dermed er man også robust mot en cyber hendelse.

Prosjektet bringer sammen eksperter innen sikkerhet og undervannsteknologi fra myndigheter, olje- og gass-industrien, og to av Norges ledende akademiske forskningsgrupper innen sikkerhet for å sikre samsvar mellom behovene både fra myndigheter samt en solid vitenskapelig basis.

6.2 Sikre industrielle nett og protokoller

Å sikre sikkerhetssystemer ved å koble dem på egne nett (soner) bak barrierer som brannvegger har utfordringer. Drift og vedlikehold blir omfattende, og verdien av barrierene blir redusert dersom det åpnes for mange eksterne forbindelser(«conduits»). Antall eksterne forbindelser øker ved at det skal tillates dataoverføring til beslutningsstøtte, prosessoptimalisering, tilstandsbasert vedlikehold mm. samt at programvareoppdateringer skal skje via nett. Et alternativ eller supplement er å benytte sikkerhetsfunksjonalitet i nett og protokoller. Slike løsninger er lansert for trådløse industrielle nett, og innen kraftindustrien har det begynt å komme industrielle komponenter som støtter IEC 62351 /24/ standarden. Denne standarden muliggjør bl.a. kryptering og integritetskontroll under overføring, og autentisering av endepunkter. Triton skadevaren (Se *Faktaboks* 6) viser at det er behov for å autentisere endepunkter mellom HMI og sikkerhetssystemer slik at sikkerhetssystemet ikke aksepterer kommandoer fra ondsinnet kode i operatørstasjonen. Kontrollere utstyres med egen maskinvare for kryptering slik at krypteringen ikke skal påvirke sanntidsegenskaper.

6.3 Data-dioder

Andre kritiske bransjer som f.eks. atomkraftindustrien har tatt i bruk datadioder for transport av data i en retning fra kritiske systemer til løsninger for beslutningsstøtte, prosessoptimalisering, tilstandsbasert vedlikehold mm. Operatører på norsk sokkel har begynt å vurdere tilsvarende løsninger. Nye leverandører har etablert seg i markedet, og prisen på enheter har gått ned. Bruk av standardkomponenter for fiberoptiske nett har også gitt rimeligere enheter. Samtidig har enhetene fått utvidet protokollstøtte og støtter bl.a. protokoller brukt for informasjonsinnhenting (OPC). Dette gjør enhetene velegnet i olje- og gass-sektoren. For kommunikasjon inn til de industrielle systemene (f.eks. fjernvedlikehold) må det benyttes andre sikkerhetsløsninger.

6.4 Kontrollrom på land

Noen operatører har etablert eller er i ferd med å etablere hovedkontrollrom for offshore operasjoner på land. Det er også installasjoner som har etablert sekundært kontrollrom på land, men de driftes fra kontrollrom på plattform. Kontrollrom for mindre installasjoner som kompressorstasjoner er ofte lagt på naboplattform eller på land.

Nettverkene for kontrollere og kontrollrom «forlenges» til fjerntliggende kontrollrom med krypterte tuneller. Slike tuneller kan sikre konfidensialitet og integritet, men ikke tilgjengelighet. Det må etableres tilstrekkelig redundante forbindelser.

Slike landbaserte kontrollrom medfører nye og andre sikkerhetsaspekter, også for SIS systemer. Rutiner dersom nettverksforbindelse går ned må etableres. Det er omdiskutert om det skal være CAP («critical action panel») på fjerntliggende kontrollrom. Dersom dette skal etableres, er det en god praksis å ha nøkkellåser som krever at både ansvarlig på plattform og ansvarlig på fjerntliggende kontrollrom åpner for bruk av et slikt CAP.

7 IKT SIKKERHET I ELEKTRISKE ANLEGG

I denne sammenheng er det utredet IKT-sikkerhet knyttet til elektrisitetsforsyning fra land. Det er vurdert hvordan sikkerhetssystemer, primært vern (Se *Faktaboks* 11), er sikret.

Troll A plattformen har helt siden den ble satt i produksjon i 1996 operert med strømforsyning fra land. Opprinnelig var det en vekselstrømkabel på 20 megawatt. Senere er denne erstattet av 2 likestrømskabler og en 3-fase vekselstrømskabel. Strømmen forsynes fra en omformerstasjon ved Kollsnes anlegget. Valhall og Goliat har strømforsyning fra land. Nylig startet produksjon på Johan

Sverdrup med strømforsyning fra Kollsnes, og nye felt som Martin Linge vil gå i produksjon med strømforsyning fra land.

Et vern («protection device») er et system eller en enhet som skal detektere en unormal tilstand og aktivere en «strømbryter» (circuit breaker) når en feil detekteres.

Tidligere var dette elektromekaniske releer eller «solid state» releer, men fra omkring 1980 er det installert digitale releer. Slike enheter overvåkes og kan styres fra SCADA systemer. I tillegg kan slike intelligente vern kommunisere med hverandre for å oppnå en koordinert respons ved unormale hendelser slik at utkoblingen ikke blir mer omfattende enn nødvendig. For linje-vern kommuniserer flere vern knyttet til linjen basert på dedikerte fiberforbindelser.

De første digitale vern kommuniserte på lokalnett med proprietære protokoller, mens IEC 61850 standarden muliggjør i dag samtrafikk mellom vern fra forskjellige leverandører. Noen moderne vern støtter IEC 62351 standarden som bl.a. spesifiserer sikkerhetsprotokoller for bruk over IEC 61850.

Faktaboks 11*: Vern i kraftforsyningen*

Ondsinnede handlinger kan medføre tap av strømforsyning ved at f.eks. høyspent strømbrytere («circuit breakers») slås av («trippes»). Dette gir primært økonomiske tap ettersom innretningene har nødstrøm for sikkerhetsfunksjoner og ved at vitale sikkerhetssystemer vil gå i sikker tilstand ved strømtap. Det er store bekymringer for at ondsinnede handlinger skal medføre varmgang eller gnister i elektriske komponenter i områder med hydrokarboner.

7.1 Design

Det er ikke identifisert vern-systemer i olje og gass-sektoren som er designet ut ifra IKT-sikkerhetskrav. Styresystemer for elektriske anlegg på land kan være isolerte systemer, mens de på offshore innretninger er integrert med andre automatisering- og sikkerhetssystemer. Det er ofte muligheter for fjern-vedlikehold og nedlasting av ny programvare over nett.

Først i senere tid har noen leverandører annonsert vern-systemer som er designet basert på sikkerhetsstandarden IEC 62351. Disse systemene har forbedrede sikkerhetsmekanismer for autentisering av brukere og noder, de sikrer kommunikasjon med kryptering/integritetskontroll og de sikrer nedlasting av ny programvare. Det er mindre skepsis for bruk av kryptering og digitale sertifikat innen elektriske komponenter enn innen andre prosesskontrollsystemer. Noen moderne vern-systemer har egen maskinvare for kryptering slik at krypteringen ikke skal påvirke sanntidsegenskaper.

I desember 2015, rapporterte regionale kraftselskap i Ukraina om utfall av kraftforsyning. 225.000 kunder mistet strømforsyning. 7 stk. 110KV og 23 stk. 35kV substasjoner var koblet ut. Det kom senere uttalelser om at utfallet skyltes at en ondsinnet aktør hadde kontrollert styresystemet. Ukrainske myndigheter, private firmaer og amerikanske myndigheter har etterforsket hendelsen. Rapporten konkluderte med at angriperen hadde benyttet en kombinasjon av «spear phishing», varianter av BlackEnergy 3 ondsinnet kode og de hadde manipulert Microsoft Office dokument for å få tilgang til IT miljø. Deretter fikk angriper tilgang til brukerkontoer som ga tilgang til OT miljø. Fra en operatørstasjon i OT kunne strømbryter («Circuit breakers») slås av. Andre aktiviteter ble gjennomført for å skjule spor og hindre gjenoppretting.

I 2016 ble strømforsyningen i deler av Kiev koblet ut av ondsinnede aktører. Angrepet benyttet antakelig den ondsinnede programvaren Industroyer. Denne koden er senere analysert, og det er avdekket at den kan bruke industrielle protokoller som 60870-5-101, IEC 60870-5-104, IEC 61850, and «OLE for Process Control Data Access» (OPC DA).

Faktaboks 12 *Angrep på kraftforsyningen i Ukraina*

7.2 Bygging

Kun noen nyere enheter er bygget etter krav til IKT-sikkerhet. Kun en leverandør har sertifisert bygge-rutiner etter IEC 62443-4-1. Denne leverandøren penetrasjonstester all ny programvare.

7.3 Leveransekjede

Nyere systemer har gode løsninger for å verifisere at kode har riktig opphav. Det benyttes elektronisk signatur eller manuell inspeksjon av sjekksummer.

7.4 Igangsetting

Kraftbransjen er konservativ i forhold til oppgradering av programvare. Dette gjelder også under igangsettingsfasen. Nye installasjoner er i noen tilfeller satt i drift uten at systemene er oppdatert.

Under bygge-fasen har mange aktører vært involvert og mange personer har hatt tilgang til installasjonene. Det er bekymringer knyttet til sletting av rettigheter og at mange «Service PCer» har vært tilkoblet med mulighet for spredning av ondsinnet kode.

7.5 Drift

Landbaserte anlegg for kraftforsyning driftes normalt av egent personell fra eget utstyr i kontrollrom. På installasjoner er drift mer integrert.

Under intervjuene kom det fram at styresystemer for elkraft i større grad er utdatert enn for annen prosesskontroll. Det er ikke uvanlig med systemer som ikke er oppdatert de siste 10 årene. En omformerstasjon kan fort ha et 30-talls enheter som må oppdateres og slike oppdateringer er ressurskrevende.

For å sikre stabil strømforsyning til olje- og gass-sektoren kreves samspill mellom drift av sentralnett (Statnett), drift av lokale kraftselskaper (f.eks. BKK og Hammerfest Energi), landbaserte omformerstasjoner og installasjoner på innretninger. Uklare ansvarsforhold og manglende rutiner i dette samarbeidet kan medføre unødvendig nedetid. Det er gjennomført lokale initiativ for å forbedre dette samarbeidet. Det er ikke uvanlig at en aktør kan styre komponenter hos en annen aktør (f.eks. koble ut vern). Dette krever sammenkoblinger som kan være sårbare for IKT-sikkerhetshendelser.

8 REFERANSER

/1/ SINTEF, 2018: *Kunnskapsprosjekt IKT-sikkerhet; Industrielle kontroll- og sikkerhetssystemer i petroleumsvirksomheten*: https://www.ptil.no/fagstoff/utforsk-fagstoff/prosjektrapporter/prosjektrapporter-2019/industrielle-kontroll--og-sikkerhetssystemer-i-petroleumsvirksomheten/

/2/ SINTEF, 2019: *IKT-sikkerhet - Fjernarbeid og HMS*: https://www.ptil.no/fagstoff/utforsk-fagstoff/prosjektrapporter/prosjektrapporter-2019/intervjustudie-i-ikt-sikkerhet-fjernarbeid-og-hms/

/3/ Norsk olje & gass, 2016: 104 Anbefalte retningslinjer krav til informasjonssikkerhetsnivå i IKT-baserte prosesskontroll-, sikkerhets- og støttesystemer: https://www.norskoljeoggass.no/arbeidsliv/retningslinjer/integrerte-operasjoner/104-anbefalte-retningslinjer-krav-til-informasjonssikkerhetsniva-i-ikt-baserte-prosesskontroll--sikkerhets--og-stottesystemer-ny-revisjon-pr-05.12.2016/

/4/ ISO/IEC 27001, 2013: Information technology - Security techniques - Information security management systems - Requirements. International Organization for Standardization.

/5/ DNVGL-RP-G108, 2017: Cyber security in the oil and gas industry based on IEC 62443 2013: https://www.dnvgl.com/oilgas/download/dnvgl-rp-g108-cyber-security-in-the-oil-and-gas-industry-based-on-IEC-62443.html

/6/ Petroleumstilsynet, 2017: Prinsipper for barrierestyring i petroleumsvirksomheten – Barrierenotat 2017: https://www.ptil.no/contentassets/43fc402b97e64a7cbabdf91c64b349cb/barrierenotat--2017.pdf

/7/ Innretningsforskriften, 2010: Forskrift om utforming og utrustning av innretninger med mer i petroleumsvirksomheten. Petroleumstilsynet.

/8/ Styringsforskriften, 2010: Forskrift om styring og opplysningsplikt i petroleumsvirksomheten og på enkelte landanlegg. Petroleumstilsynet.

/9/ IEC 61508, 2019. *Functional safety of electrical/electronic/programmable electronic safety-related systems.* International Electrotechnical Commission.

/10/ IEC 61511, 2016. *Functional safety - Safety instrumented systems for the process industry sector.* International Electrotechnical Commission.

/11/ IEC 62443-2-1, Draft 2015. *Security for Industrial Automation and Control Systems, Establishing an industrial automation and control system security program.* International Electrotechnical Commission.

/12/ IEC 62443-2-4, 2015. *Security for Industrial Automation and Control Systems, Security program requirements for IACS service providers.* International Electrotechnical Commission.

/13/ IEC 62443-3-3, 2013. *Security for Industrial Automation and Control Systems, System Security Requirements and Security Levels.* International Electrotechnical Commission.

/14/ IEC 62443-4-1, 2018. *Security for Industrial Automation and Control Systems, Secure product development lifecycle requirements.* International Electrotechnical Commission.

/15/ NIST, 2014: Framework for Improving Critical Infrastructure Cybersecurity: https://www.nist.gov/cyberframework

/16/ ISO/IEC 27035, 2016, Information security incident management. International Organization for Standardization.

/17/ NIST SP 800-61 Rev. 2, 2012 Computer Security Incident Handling Guide

/18/ ISA-TR84.00.09, 2013. Security Countermeasures Related to Safety Instrumented Systems (SIS)

/19/ SANS, 2019. SANS 2019 State of IT/ICS Cybersecurity Survey

/20/ Norsk olje & gass, 2018: *070 Application of IEC 61508 and IEC 61511 in the Norwegian petroleum Industry (Recommended SIL requirements)*

/21/ NORSOK S001, 2018: Technical Safety

/22/ ISA, 2019; Security PHA Review for Consequence-Based Cybersecurity

/23/ IEC 61850, 2019. *Communication networks and systems for power utility automation.* International Electrotechnical Commission.

/24/ IEC 62351, 2018. *Power systems management and associated information exchange - Data and communications security.* International Electrotechnical Commission.

APPENDIX A - INTERVJUKANDIDATER

Det er foretatt intervju med følgende aktører i olje- og gass-sektoren:

- ABB
- ABB Elkraft
- Aker BP
- Autronica
- Baker Hughes
- Equinor
- Kongsberg Maritime
- Lundin Norway
- Schlumberger (Cameron)
- Siemens
- Siemens Elkraft

APPENDIX B - INTERVJUGUIDE

DNV·GL

Intervjuguide Cyber security SIS

Intervjuobjekt (navn, funksjon): _____ *Organisasjon/sted:* _____

Intervjuere: _____ *Dato* (dd.mm.åååå): _____

#	Tema og spørsmål	Ref.	Kommentar / svar
1	**Rammesetting (ca. 5 min)** • Ønske velkommen, presentasjon		
2	**Informasjon (ca. 10 min)** • Si litt om temaet for samtalen (bakgrunn, formål) • Forklar hva intervjuet skal brukes til, nevn taushetsplikt og anonymitet • Forklar rollene til personene fra DNV GL • Spør om noe er uklart og om respondenten har noen spørsmål		
3	**Ansvar / rolle (5 min)** • Fortell litt om ditt arbeid og din rolle i organisasjonen? • Hva slags erfaringer har du med Industriell IKT og SIS? • Hvilken fase i livssyklusen til SIS system er du involvert i? • Kan person eller organisasjon refereres i rapport?		
4	**Livssyklus (ca. 50 min)**		

DNV GL Headquarters, Veritasveien 1, P.O.Box 300, 1322 Høvik, Norway. Tel: +47 67 57 99 00. www.dnvgl.com

#	Tema og spørsmål	Ref.	Kommentar / svar
4.1	**Design** • Hvilke krav og prinsipper (i forhold til cyber security) er lagt til grunn for design av produktet? • Hvordan er sikkerhetssystemer adskilt fra prosesskontroll? (Ref ISA TR84.00.09) • Hvordan vurderer du fordelingen mellom de 4 modellene i ISA TR84.00.09? (i %. Vis skisser av modellene) • Gitt at systemene er adskilt, hvordan sikres HMI, EWS, Oppdateringer, Status informasjon til kontrollrom/andre systemer? • Hvilke krav er satt til omkringliggende systemer? (sonemodell, ekstern brannvegg….) • Hvilke standarder er lagt til grunn? (IEC61508/511, IEC 62443, NIST, IADC…)		Air Gap: ____Interlaced:____Integrated 2 zone:____Integrated 1 zone:____
4.2	**Bygging** • Benyttes rammeverk for sikker programvareutvikling (SSDLC)? • Er utviklere kurset/trenet i sikker koding? • Benyttes bibliotek/produkter for inputvalidering? • Gjøres sikkerhetsrelatert logging, og er det samling av logger (SIEM)? • Benyttes produkter for statisk kodeanalyse? • Hvilke standarder legges til grunn? (IEC 62443-4-1, OWASP,		

#	Tema og spørsmål	Ref.	Kommentar / svar
	SANS…)		
4.3	**Transport / lagring** • Hvordan sikres integritet på programvare under transport/lagring? (Er koden signert?)		
4.4	**Igangsetting** • Er det definert krav til herding av systemet? • Er det rutiner for endring av standardpassord? • Verifiseres at produktet har oppdatert patchnivå før overlevering? • Utføres sikkerhetstesting? (Penetrasjonstest) • Hvordan sikres at løsningen som overleveres til drift ikke har svakheter fra implementasjonsfasen? (udokumentert/testet rettelser, temporære brannveggsåpninger, Virus…)		
4.5	**Overlevering til drift** • Er det definert krav til dokumentasjon av løsningen? (SW + HW inventory, systemdokumentasjon, nettverksskisser…) • Gis det opplæring til driftsorganisasjon i forhold til cyber security? • Utføres risikoanalyse iht. IEC61511-1:2016 (8.2.4)?		
4.6	**Drift**		

#	Tema og spørsmål	Ref.	Kommentar / svar
	• Hvor ofte oppdateres løsningen med sikkerhetsrettelser? • Hvor mange % av installasjonene er oppdatert) • Hvordan sikres integritet på oppdateringer (Er de signert av leverandør?) • Støttes bruk av antivirusprogramvare, og hvor ofte oppdateres denne? • Hvor mange % av SIS systemene har antivirus beskyttelse? • Hvor ofte oppdateres antivirus beskytelse? • Hvordan sikres oppdatering i forhold til nye trusler og angrepsflaer? • Er det testet tilbakelegging («restore») (fra scratch)? • Hvor mange % av SIS systemene har testet tilbakelegging fra scratch? • Sikres integritet på sikkerhetskopier? • Er det definert rutiner for håndtering av sikkerhetshendelser? • Er det øvet rutiner for sikkerhetshendelser? • Hvilke standarder legges til grunn?		Hver måned:____Hvert år:____Hvert 10 år:____ Oppdateres ikke:____ ____% Hver måned:____Hvert år:____Hvert 10 år:____ Oppdateres ikke:____ ____%
5	**Kommunikasjonsprotokoller (ca. 10 min)** • Hvilke nettverksløsninger benyttes for ekstern kommunikasjon? (Feltbuss, Ethernet…) • Hvilke kommunikasjonsprotokoller benyttes for ekstern		

#	Tema og spørsmål	Ref.	Kommentar / svar
	kommunikasjon? • Er denne protokollen routbar? (TCP/IP?) • Hvor mange % av SIS systemene kommuniserer TCP/IP?		 ____%
6	**Trender og utvikling (ca. 10 min)** • Vil dagens systemer eksistere om 10 år? • Hva vil være typiske trender • Hva er status/planer om bruk av enheter med IIoT egenskaper? • Vil det åpnes for optimalisering/styring fra skytjenester?		
7	**Elektriske anlegg (ca. 20 min)** • Hvilke prinsipper er lagt til grunn for å sikre prosesskontroll og sikkerhetssystemer? • Hvordan er sikkerhetssystemer adskilt fra prosesskontroll? (Ref ISA TR84.00.09) • Hvordan vurderer du fordelingen mellom de 4 modellene i ISA TR84.00.09? (i %. Vis skisser av modellene) • Hvilke prinsipper gjelder for sikring av vern? • Hvilke standarder legges til grunn? (IEC 61850, IEC 62351…)		Air Gap: ____Interlaced:____Integrated 2 zone:____Integrated 1 zone:____
8	**Oppsummering (ca. 10 min)** • Oppsummere funn		

#	Tema og spørsmål	Ref.	Kommentar / svar
	• Har jeg forstått deg riktig? • Er det noe du vil legge til? Nye intervjuobjekter, nye dokumenter?		

APPENDIX C - OPPSUMMERING AV FUNN

#	Vurdering	DNV GL Anbefaling	Kapittel
1	Det er en tendens til at leverandører ikke innfører IKT-sikkerhetsløsninger med mindre operatørene krever det samtidig som at mindre operatører ikke innfører IKT-sikkerhetsløsninger med mindre myndighetene setter krav	**Krav til IKT-sikkerhet for sikkerhetssystemer:** Tilsynsmyndighet bør sette strengere krav til IKT-sikkerhet for sikkerhetssystemer.	5.1
2	Det er BOP installasjoner der det er åpnet for fjernvedlikehold og installasjoner der tilstanden på systemene kommuniseres til eksterne systemer.	**Separasjon av BOB systemer:** BOP systemer bør være adskilt fra andre systemer med luft-gap eller diodeløsninger.	5.1
3	Nødavstengningssystemer og sentrale deler av brann og gass-systemer er for det meste designet på samme nett som kontrollsystemene	**Dedikerte nett for ESD og brann og gass:** Det er å anbefale at SIS systemer bruker dedikerte nettverk for å skape segregering fra kontrollsystemene.	5.1
4	Leverandørene av sikkerhetssystemer har i liten grad tatt i bruk regimer for sikker programvareutvikling.	**Sikker programvareutvikling:** Det er å anbefale at det tydeliggjøres krav fra operatørene at dokumentert sikker programvareutvikling vil være avgjørende faktor for valg av og videre bruk av sikkerhetsløsninger. Leverandører bør være sertifisert etter 62443-4-1 eller tilsvarende.	5.2
5	Det er bekymring knyttet til om programvare i sikkerhetssystemer kan endres av ondsinnede aktører etter at den er utviklet av produsent og frem til produktet settes i drift	**Integritetskontroll på programvare**: Det anbefales å styrke fokuset på å sikre integriteten på programvare for sikkerhetssystemer i perioden fra utviklet løsning til produktet settes i drift.	5.3
6	Under sikkerhetsverifikasjon og test av sikkerhetsløsninger er det avdekket at flere av sårbarhetene skyldes manglende rutiner under	**Verifikasjon av IKT-sikkerhet etter igangsetting:** Det anbefales derfor ytterligere styrking av og fokus på IKT sikring av alle industrielle systemer under	5.4

	igangsetting («Commissioning»).	igangsetting, og spesielt for SIS systemer. Leverandører bør være sertifisert etter 62443-2-4 eller tilsvarende.	
7	Majoriteten av sikkerhetshendelser er ofte grunnet i svakheter i programvare hvor det allerede finnes rettelser og korreksjoner utarbeidet og distribuert av leverandørene	**Oppdatering av sikkerhetsrettelser:** Det anbefales å styrke fokuset på å følge oppdatering av sikkerhetsrettelser for industrielle systemet inkludert sikkerhetssystemer så hypping som mulig.	5.6.1
8	Det er lite bruk av antivirusbeskyttelse på sikkerhetssystemer	**Antivirusbeskyttelse:** Det er sterkt å anbefale at denne beskyttelsen også benyttes på SIS systemene dere det er mulig og der leverandøren godkjenner bruk av dette.	5.6.2
9	Det er ikke identifisert planlagte eller gjennomførte tester for tilbakelegging av sikkerhetskopier på SIS systemer blant intervjukandidatene i markedet	**Sikkerhetskopiering og tilbakelegging:** Det er sterkt å anbefale å teste og prøve sikkerhetskopiering og tilbakelegging periodisk.	5.6.3
10	Trender og utvikling av olje og gas sektoren samt ny tilgjengelige sikkerhets teknologi reiser nye sikkerhetsutfordringer og muligheter	**Sikre industrielle nett:** Det anbefales å ytterligere vurdere muligheten for utvidet bruk av sikre industrielle nett og protokoller samt data-diode løsninger for beskyttelse av SIS systemer, og andre industrielle systemet.	6.0
		«All electric subsea»: Det anbefale å gjøre IKT-sikkerhets vurdering av «all electric subsea» løsninger og teknologi for å kartlegge mulige risiko.	
		Operasjonsrom på land: Det anbefales å vurdere ytterligere utredninger av IKT sikkerhets utfordringer ved landbaserte operasjons sentra, både for SIS systemer og andre industrielle systemer.	
11	Det er store bekymringer for at ondsinnede handlinger skal koble ut	**IKT-sikkerhet og elkraft:** Det anbefale å gjøre IKT-sikkerhets	7

	sikkerhetssystemer eller modifisere slik at systemene kan utgjøre en tennkilde i områder med hydrokarboner.	vurdering av mulige ondsinnede angrep mot sikkerhetssystemer for elektriske anlegg.	
12	Det er også oppdaget at styresystemer for elkraft i større grad er utdatert enn for annen prosesskontroll. Det er ikke uvanlig med systemer som ikke er oppdatert de siste 10 årene.	**Sikkerhetsrettelser elkraft:** Det anbefales å styrke fokuset på å følge oppdatering av sikkerhetsrettelser for industrielle systemet inkludert sikkerhetssystemer så hypping som mulig.	7.4
13	For å sikre stabil strømforsyning til olje- og gass-sektoren kreves samspill mellom drift av sentralnett (Statnett), drift av lokale kraftselskaper (f.eks. BKK og Hammerfest Energi), landbaserte omformerstasjoner og installasjoner på innretninger. Uklare ansvarsforhold og manglende rutiner i dette samarbeidet kan medføre unødvendig nedetid. Det er også identifisert installasjoner der en aktør kan styre komponenter hos en annen aktør. Dette krever sammenkoblinger som kan være sårbare for IKT-sikkerhetshendelser.	**Samspill aktører elkraft:** Det anbefale å gjøre risikovurdering av samspillet mellom aktører innen kraftforsyning.	7.4

Om DNV GL

DNV GL er et internasjonalt selskap innen kvalitetssikring og risikohåndtering. Siden 1864 har vårt formål vært å sikre liv, verdier og miljøet. Vi bistår våre kunder med å forbedre deres virksomhet på en sikker og bærekraftig måte.

Vi leverer klassifisering, sertifisering, teknisk risiko- og pålitelighetsanalyse sammen med programvare, datahåndtering og uavhengig ekspertrådgivning til maritim sektor, til olje- og gass-sektoren, og til energibedrifter. Med 80,000 bedriftskunder på tvers av alle industrisektorer er vi også verdensledende innen sertifisering av ledelsessystemer.

Med høyt utdannede ansatte i 100 land, jobber vi sammen med våre kunder om å gjøre verden sikrere, smartere og grønnere.