PETROLEUMSTILSYNET

Revisjonsrapport

Rapport	
Rapporttittel **Rapport etter tilsyn med aktørenes håndtering av IKT-sikkerhet**	Aktivitetsnummer **992487**

Gradering		
☑ Offentlig	☐ Begrenset	☐ Strengt fortrolig
Enkeltdeler er unntatt offentlighet	☐ Fortrolig	
☐ Unntatt offentlighet		

Involverte	
Hovedgruppe T-	Oppgaveleder Asbjørn Ueland
Deltakere i revisjonslaget Tommy Bugge Hansen, Bjørnar Heide, Anthoni Larsen, Else Riis Rasmussen, Espen Seljemo, Kristi Wiger og Asbjørn Ueland	Dato 28.9.2017

1 Innledning

Petroleumstilsynet (Ptil) gjennomførte i tidsrommet 2. mai – 16. juni 2017 tilsyn med operatører med felt og anlegg i drift samt redere med innretninger som har SUT[1]. Tilsynet var rettet mot aktørenes håndtering av IKT-sikkerhet og ble gjennomført som møter med hver enkelt operatør og reder der det ble gjort rede for utvalgte tema.

Engelsk oversettelse følger på side 4.

2 Bakgrunn

Petroleumstilsynet skal legge premisser for, og følge opp at aktørene i petroleums-virksomheten holder et høyt nivå med hensyn til helse, miljø og sikkerhet og at risikoen reduseres så langt som mulig.

De industrielle sikkerhets- og kontrollsystemene på innretninger og flyttbare innretninger er essensielle for sikker drift, og IKT-sikkerheten for disse er vesentlig for å ivareta dette. Trusselbildet er i stadig endring og det er stor oppmerksomhet på denne problemstillingen. Hendelser de siste årene har vist at problemstillingen er relevant også for vår næring.

3 Mål

Målsetningen med tilsynet var å undersøke hvilken tilnærming operatører og redere har til risikovurdering, beskyttelse, oppfølging og tilsyn med IKT-sikkerhet for de industrielle sikkerhets- og kontrollsystemene.

Tilsynet baserte seg blant annet på følgende lover og forskrifter:

[1] Samsvarsuttalelse

- Styringsforskriften § 4 om risikoreduksjon; den ansvarlige skal velge tekniske, operasjonelle og organisatoriske løsninger som reduserer sannsynligheten for at det oppstår skade, feil og fare- og ulykkessituasjoner.
- Styringsforskriften § 5 om barrierer; etablere barrierer som reduserer sannsynligheten for at feil og fare- og ulykkessituasjoner utvikler seg og begrenser mulige skader og ulemper.
- Petroleumsloven § 9-3 om beredskap mot bevisste anslag; rettighetshaver skal iverksette og opprettholde sikringstiltak for å bidra til å hindre bevisste anslag mot innretninger og anlegg, samt til enhver tid ha beredskapsplaner for slike anslag.

4 Resultat

Tilsynet ble gjennomført som møter med den enkelte operatør og reder der de gjorde rede for punktene fra varselbrevet; forhold knyttet til risikovurdering, IKT-arkitektur, passive beskyttelsestiltak, monitorering, analyse og respons, rapportering av hendelser, egne tilsyn og revisjoner.

Tilsynet viser at næringen er bevisst behovet for sikring av de industrielle sikkerhets- og kontrollsystemene. Dette kommer til syne i revisjonsarbeidet av retningslinje 104 fra Norsk olje og gass og i industrisamarbeidet i regi av DNV GL som har ført til retningslinjer både innen maritim sektor generelt (RP-0496) og innen vår næring (RP-G128).

De enkelte selskapene har i stor grad et rammeverk som baserer seg på internasjonale standarder og som har selskapsspesifikke tilpasninger. Standarder som ISO/IEC[2] 27001, NIST 800-82, NIST CSF[3] og ISO/IEC 62443 blir ofte referert. Blant rederne benyttes også dokumenter basert på ISPS[4]-koden og veiledninger fra IADC[5].

Operatørene og rederne synes å ha en noe forskjellig tilnærming i forhold til sikringen av de industrielle systemene. Blant operatørene er det ofte fokus på at informasjon fra drift og om tilstand på utstyr blir gjort tilgjengelig i organisasjonene. Rederne legger ofte til rette for fjerntilgang slik at leverandørene kan gis mulighet for tilgang til systemene ved feilsituasjoner. Disse forskjellene fører gjerne til at valg av sikringsløsninger prioriteres ulikt.

Sladdet

I punktene nedenfor gis en overordnet oppsummering av status for næringen. Resultatene for det enkelte selskap er gitt i separate vedlegg til hvert enkelt selskap.

---

[2] International Electrotechnical Commission

[3] National Institute of Standards and Technology, Cybersecurity Framework

[4] International Ship and Port Facility Security Code

[5] International Association of Drilling Contractors

4.1 Risikovurderinger

Vi ser en økende årvåkenhet rundt risiko, men og en stor variasjon i tilnærmingen til å vurdere risiko. Vi er opptatt av en helhetlig tilnærming til risikostyring og at det legges til rette for erfaringsoverføring og læring mellom relevante fagmiljøer, både internt i det enkelte selskap og mellom selskapene.

De risikovurderingene som ble presentert synes å være konsentrert om ett eller flere av følgende punkter:

- Hvem er trusselaktøren?
- Hvordan kan aktøren få tilgang til systemene (sårbarhet)?
- Hvilken skade kan gjøres (konsekvens)?

4.2 IKT-arkitektur for de industrielle sikkerhets- og kontrollsystemene samt koblinger mot andre systemer

Det er et tydelig skille i implementeringen av IKT-arkitektur mellom innretninger og flyttbare innretninger.

På innretninger finner vi implementeringer som i hovedsak reflekterer systemarkitektur slik den vises i retningslinje 104 fra Norsk Olje og Gass. Det innebærer separate nettverk for sikkerhets- og kontrollsystemene, og sikrede løsninger som gir fjerntilgang til systemene og informasjonsflyt til kontormiljøet.

På flyttbare innretninger finner vi gjerne løsninger der det er tilnærmet ingen kommunikasjon mellom de ulike systemene. Det er da etablert en IKT-arkitektur der det er lagt til rette for fjerntilgang fra leverandører og der denne tilgangen er styrt av personell på innretningen.

4.3 Passive beskyttelsestiltak for nettverkene til de industrielle sikkerhets- og kontrollsystemene

Alle aktørene har installert et sett av passive beskyttelsestiltak. Dette omfatter forhold knyttet til:

- brukertilgang og autentisering,
- adgangskontroll og arbeidstillatelser,
- logiske og fysiske løsninger for blokkering av tilkomst,
- opplæring.

Bruken av passive beskyttelsestiltak synes i hovedsak å være tilpasset de enkelte anlegg og operatørene sin vurdering av risiko og trusler.

4.4 Monitorering, analyse og respons

Monitorering og analyse av datatrafikk er en funksjon som oftest utføres av sentrale avdelinger i selskapene eller av tjenesteleverandører når det er disse som ivaretar driften av kommunikasjonsnettverkene. Denne overvåkningen er i hovedsak knyttet til datatrafikk inn til selskapenes kontornettverk, men en del overvåker også nettverksutstyr for de industrielle systemene for å avdekke unormaliteter. Behovet for overvåkning varierer siden selskapene har ulike tilnærminger til og løsninger for leverandørsupport og eksport av data.

4.5 Rapportering av hendelser

Selskapene benytter til dels de ordinære systemene som Synergi eller lignende, eller de benytter løsningene de har for vanlig IT for registrering av IKT-relaterte hendelser. Vi ba også om en gjennomgang av de alvorligste IKT-relaterte hendelser etter 1.1.2014. Gjennomgangen viser at det er lav terskel for å rapportere uregelmessigheter innad i selskapene.
Varsling og melding til tilsynsmyndighetene er regulert i styringsforskriftens § 29. Det arbeides med en presisering i veiledningen for å gjøre det tydeligere hvilke IKT-relaterte hendelser som omfattes av denne paragrafen.

Sladdet

4.6 Egne tilsyn og revisjoner

Selskapene har, i all hovedsak, gjennomført tilsyn og revisjoner med sikringen av de industrielle sikkerhets- og kontrollsystemene. Metodikkene som benyttes omfatter utsjekk mot interne retningslinjer, bruk av anerkjente normer og standarder, samt eksterne selskaper som også benytter etisk hacking. Funn fra revisjonene synes å bli fulgt opp på en tilfredsstillende måte.

1 Introduction

From 2 May to 16 June 2017, the Petroleum Safety Authority Norway (PSA) carried out an audit of operators with fields and facilities in operation and mobile offshore unit owners with facilities that possess AoC[6]. The audit was focused on the participants' handling of ICT security and was conducted in the form of meetings with each individual operator and owner in which selected topics were reviewed.

2 Background

The Petroleum Safety Authority Norway is responsible for setting the agenda and monitoring to ensure that participants in the petroleum industry maintain a high level in respect of health, safety and the environment and that risk is reduced as much as possible.

The industrial safety and control systems on facilities and mobile offshore units are essential for safe operations, and their ICT security is crucial for protecting this. The threat picture is constantly changing and a lot of attention is focused on this issue. Incidents in recent years have shown that this problem is also relevant for our industry.

[6] Acknowledgement of compliance

3 Objective

The objective of the audit was to investigate the approach of operators and owners to risk assessment, protection, follow-up and surveillance of ICT security for the industrial safety and control systems.

The audit was based on the following acts and regulations:

- The Management Regulations Section 4 concerning risk reduction; the responsible party shall select technical, operational and organizational solutions that reduce the likelihood that harm, errors and hazard and accident situations occur.
- The Management Regulations Section 5 concerning barriers; establish barriers that reduce the possibility of failures, hazard and accident situations developing, and limit possible harm and inconveniences.
- The Petroleum Act Section 9-3 concerning emergency preparedness against deliberate attacks; the licensee shall initiate and maintain security measures to contribute to avoiding deliberate attacks against facilities and installations, and shall at all times have contingency plans to deal with such attacks.

4 Result

The audit was conducted in the form of meetings with the individual operators and owners in which the items from the letter of notification were reviewed: matters relating to risk assessment, ICT architecture, passive safeguards, monitoring, analysis and response, incident reporting, own audits and reviews.

The audit shows that the industry is conscious of the need to safeguard its industrial safety and control systems. This is apparent in the revision work on Norwegian Oil and Gas recommended guidelines 104 and in the industrial cooperation under DNV GL which has resulted in guidelines both in the maritime sector in general (RP-0496) and in our industry (RP-G128).

The individual companies largely have a framework based on international standards, with company-specific adaptations. Standards such as ISO/IEC 27001, NIST 800-82, NIST CSF and ISO/IEC 62443 are often referred to. Among the mobile offshore unit owners, documents based on the ISPS Code and guidelines from IADC are also used.

The operators and owners appear to differ somewhat in their approach to securing the industrial systems. Among the operators, there is often a focus on information from operations and on the condition of equipment being made available within the organizations. The mobile offshore unit owners often facilitate remote access so that the suppliers can be given the option of accessing the systems in the event of failures. These differences tend to result in different priorities in the choice of security solutions.

Sladdet

The sections below provide a general summary of the status in the industry. The results for the individual companies are provided in separate annexes for each individual company.

4.1 Risk assessments

We see an increasing alertness concerning risk, but also large variation in the approach to assessing risk. We are committed to a holistic approach to risk management and the facilitation of experience transfer and learning between the relevant professional domains, both within the individual company and between the companies.

The risk assessments presented appear to be concentrated around one or more of the following points:

- Who is the threat actor?
- How can the actor gain access to the systems (vulnerability)?
- What harm can be done (consequences)?

4.2 ICT architecture for the industrial safety and control systems and links to other systems

There is a clear distinction between facilities and mobile offshore units in the implementation of ICT architecture.

On facilities, we find implementations that primarily reflect system architectures as shown in Norwegian Oil and Gas recommended guidelines 104. This entails separate networks for the safety and control systems, and secured solutions that provide remote access to the systems and information flow to the office environment.

On mobile offshore units, we find solutions where there is approximate no communication between the different systems. An ICT architecture is then established which facilitates remote access from suppliers and where this access is controlled by the personnel on board the facility.

4.3 Passive safeguards for the industrial safety and control system networks

All the participants have installed a set of passive safeguards. These relate to:

- user access and authentication,
- access control and work permits,
- logical and physical solutions for blocking access,
- training.

The use of passive safeguards appears in the main to be adapted to the individual facility and the operators' assessments of risk and threats.

4.4 Monitoring, analysis and response

Monitoring and analysis of data traffic is a function that is usually performed centrally in the companies, or by service providers when it is they who assure operation of the communication networks. This monitoring is primarily linked to data traffic in the companies' office networks, but some also monitor network equipment for the industrial systems in order to detect anomalies. The need for monitoring varies since the companies have different approaches to and solutions for supplier support and data exporting.

4.5 Incident reporting

The companies use either the ordinary systems such as Synergi or similar, or the usual IT solutions they have for registering ICT-related incidents. We also requested a review of the most serious ICT-related incidents since 1 January 2014. The review shows that there is a low threshold for reporting irregularities within the companies.
Notifying and reporting to the supervisory authorities is regulated by Section 29 of the Management Regulations. The guidelines are being amplified to clarify which ICT-related incidents are comprised by this section.

Sladdet

4.6 Own audits and reviews

The companies have in the main performed audits and reviews of the security of their industrial safety and control systems. The methodologies employed include checks against internal guidelines, the use of recognised norms and standards, and external companies who also employ ethical hacking. Findings from the audits appear to have been followed up satisfactorily.

5 Deltakere

Følgende personer fra Petroleumstilsynet har deltatt:

Tommy Bugge Hansen	fagområde beredskap, logistikk og sikring
Bjørnar Heide	fagområde prosessintegritet
Anthoni Larsen	fagområde beredskap, logistikk og sikring
Else Riis Rasmussen	fagområde prosessintegritet
Espen Seljemo	fagområde prosessintegritet
Kristi Wiger	fagområde prosessintegritet
Asbjørn Ueland	fagområde prosessintegritet (leder for tilsynsaktiviteten)

6 Dokumentasjon

Selskapets presentasjon på møtet

7 Vedlegg

Selskapsspesifikke resultater og oversikt over deltakende personell.