Øvelsesplanlegger

Pakke 1 øving 3

«*Vedlikehold og modifikasjon*»

Utgave 1.0

Innholdsfortegnelse

1 Innledning

1.1 Bakgrunn og formål

Anlegg og installasjoner i petroleumssektoren skal ha beredskapsplaner for håndtering av uønskede hendelser. Næringen har scenarioer som kan knyttes til IKT-hendelser men Havindustritilsynet (Havtil) har i tilsyn sett at det knapt trenes innen IKT-sikkerhet for de industrielle kontroll- og sikkerhetssystemene. Derfor har Havtil fått utarbeidet et sett med trenings- og øvelsesscenarioer. Dette øvelses-opplegget ble utarbeidet av Proactima med Netsecurity som partner. Opplegget er videre bearbeidet av Havtil.

Aktivitetsforskriften § 23 beskriver at «det utføres nødvendig trening og nødvendige øvelser, slik at personellet til enhver tid er i stand til å håndtere operasjonelle forstyrrelser og fare- og ulykkessituasjoner på en effektiv måte». Samme formulering finnes også i teknisk og operasjonell forskrift § 52. Det er altså samme krav til trening og øvelser for anleggene på land som det er til innretningene på sokkelen.

Når vi trener, øker vi personlige ferdigheter og kunnskaper. Øvelser tester samhandling og beredskapsevne, avdekke styrker og svakheter, samt forbereder ledelsen på å håndtere ulike kriser.

1.2 Oppbygging av veilederen

Hver enkelt øvelsesplanlegger inneholder ulike scenarioer, og det er foreslått hvilke funksjoner som er aktuelle å inkludere i øvelsen. Scenarioene kan benyttes som trening, table top eller spilløvelse.

Veilederen har i del 3 ekstra informasjon til forberedelse og gjennomføring så som:

- et mulig hendelsesforløp i forkant av startpunkt
- sekvensskjema for hendelsen
- relevant fagstoff

2 Scenario

Scenariet for denne veilederen er modifikasjonsarbeid som utføres fra leverandørens kontorer.

2.1 Oversikt scenarioer

Tabell 1 indikerer hvilke funksjoner/avdelinger som er aktuelle å trene ved bruk av de ulike scenarioene. Det er opp til øvingsledelse å velge hvilke oppgaver som skal inkluderes i øvelsen.

Tabell 1: Oversikt over hvem som kan trenes/øves i de ulike modulene

Oppgave	Tittel	SAS/IACS - ansvarlig	Lokal driftsledelse	System-ansvarlig drift	IKT-avdeling
2.2	Innledende forhold - Oppdatering av CCTV programvare	x	x		
2.3	Eskalering		x	x	

2.2 Innledende forhold – Oppdateringer av CCTV programvare

Det gjennomføres rutinemessig oppdatering av programvare for CCTV. Siden CCTV ikke er klassifisert som sikkerhetskritisk utstyr har leverandøren permanent tilgang til systemene på alle innretningene til operatøren. Arbeidet gjøres fra leverandørens lokaler for fjernarbeid og skal reguleres av arbeidstillatelser. En kontrollromsoperatør oppdager uregelmessigheter med CCTV-systemet.

2.2.1 Veiledende spørsmål

Lokal driftsledelse

- Hva har skjedd?
- Hvilke konsekvenser kan dette ha for drift av eller sikkerhet på innretningen?
  - Hvordan kan konsekvensene håndteres?
- Hvem kan man kontakte?

SAS/IACS-ansvarlig

- Hvordan finner man ut hva som har skjedd?
- Hvem involveres? Hvorfor?

2.2.2 Oppfølgingspunkter, avhengig av utfall på diskusjon og beslutninger

- Hvordan håndteres situasjonen om mange CCTV kamera ikke lar seg betjene?
- Hva kan skje dersom CCTV bildene fryser uten at det umiddelbart oppdages?
- Hvordan er CCTV kritikalitetsvurdert hos oss?
  - i vedlikeholdssystemet?
  - opplevd kritikalitet i kontrollrom og driftsledelse?

2.3 Eskalering – Planlagt CCTV-arbeid på annen innretning

I dialog med System-ansvarlig drift blir det avdekket at det foregår oppdateringer på CCTV på andre innretninger, men at arbeid på gjeldende innretning først er planlagt neste uke. Årsaken til problemene i forrige punkt skyldes at det ikke er samsvar mellom den installerte kamerakonfigurasjonen og den som leverandøren har benyttet ved det gjennomførte arbeidet.

2.3.1 Veiledende spørsmål

Driftsledelse på innretningen

- Hvordan håndteres situasjonen videre?
- Hvilke konsekvenser kan dette ha for drift av eller sikkerheten på innretningen?

Systemansvarlig drift

- Hvordan finner man ut hva som har skjedd?
- Hvordan foregår samhandling med leverandør av CCTV?
- Hva gjøres for å gjenopprette CCTV?
- Er det mulig å tilbakestille systemet til slik det var før vedlikeholdsarbeidet?

2.3.2 Videre avklaringer

Det avdekkes at det ikke er samsvar mellom den installerte kamerakonfigurasjonen og den som leverandøren har benyttet ved det gjennomførte arbeidet.

- Hvordan håndteres «mindre modifikasjoner» som for eksempel installasjon av nye matrisefunksjoner for CCTV kamera?
- Hvordan er rutinene for å sikre at leverandører benytter oppdatert konfigurasjon?

3 Ekstra informasjon til forberedelse og gjennomføring

Det har lenge vært mulig å overvåke og arbeide på industrielle IKT-systemer fra land, både for operatørselskap og systemleverandører, både "lesetilgang" (tilgang til måleverdier, overvåkning og feilsøking) og "skrivetilgang" (gjøre endringer). Noen selskaper har ekspertise offshore, andre har ekspertise i organisasjonen på land, andre igjen har "outsourcet" deler av støttefunksjonene dels til egne globale sentra eller til leverandører.

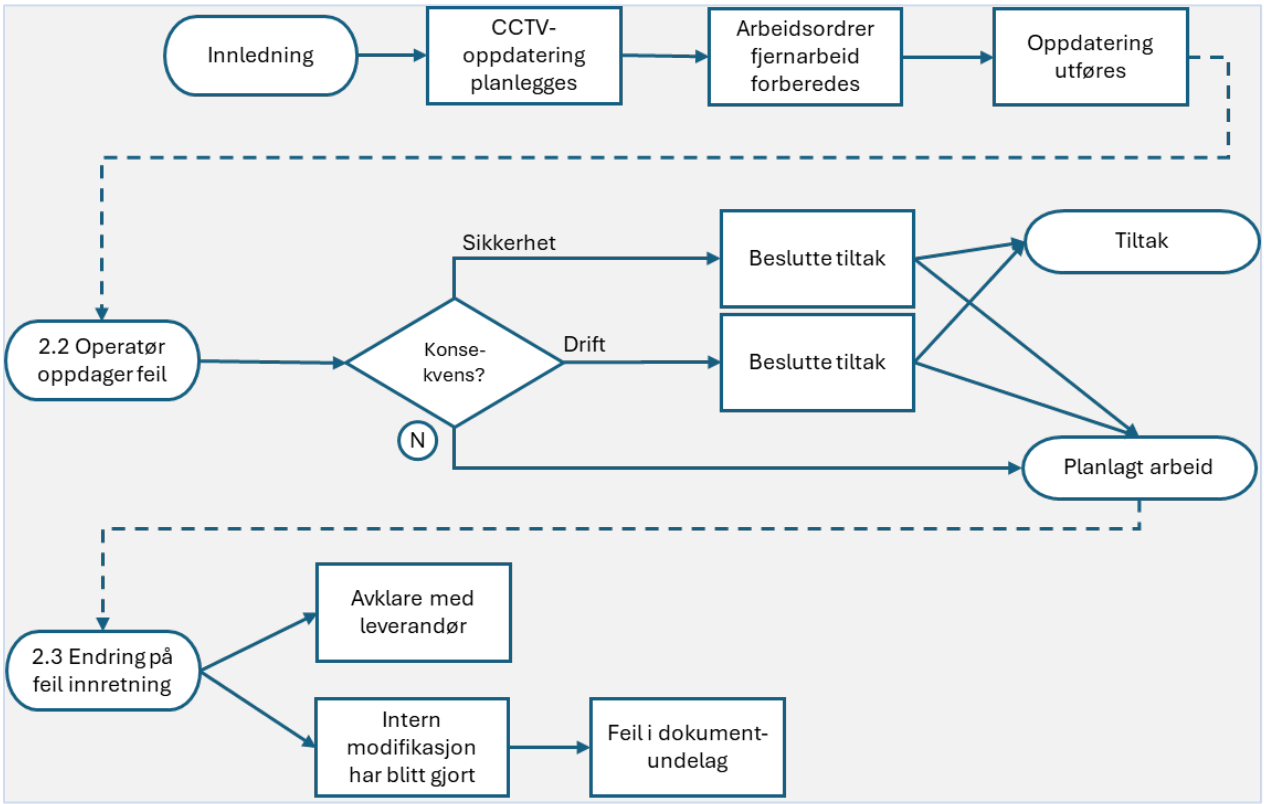
Med jevne mellomrom oppdateres kontrollsystemer og andre datasystemer vi fjerntilgang. Noen planlagte vedlikeholdsoppgaver og modifikasjoner må gjennomføres under revisjonsstans, men mye gjennomføres også under normal drift.

3.1 Innledning til hendelse

Det gjennomføres rutinemessig oppdatering av programvare for CCTV. Siden CCTV ikke er klassifisert som sikkerhetskritisk utstyr har leverandøren permanent tilgang til systemene på alle innretningene til operatøren. Arbeidet gjøres fra leverandørens lokaler for fjernarbeid og skal reguleres av arbeidstillatelser.

3.2 Hendelse

I utarbeidelsen av øvingen er det tatt utgangspunkt følgende forløp:



3.3 Læring

Gjennomgang av rutiner, avklaring av ansvarsforhold og forbedring av systemer.

- Hvordan involveres deltakerne i sluttrapporten fra øvelsen?

Systemansvarlig drift

- Er ansvar og roller tilstrekkelig beskrevet?
- Hvordan støtter definerte rutiner håndteringen av hendelsen?
- Ble rutinene fulgt? Hvilke endringer bør gjøres?

SAS/IACS-ansvarlig

- Er ansvar og roller tilstrekkelig beskrevet?
- Hvordan støtter definerte rutiner håndteringen av hendelsen?
- Ble rutinene fulgt? Hvilke endringer bør gjøres?
- Hvordan sikrer en læring til alle skift?

Lokal driftsledelse

- Hvordan støtter definerte rutiner håndteringen av hendelsen?
- Hvordan sikrer en læring til alle skift?

3.4 Aktuell litteratur

Havtil har gjennomført et større arbeid knyttet til IKT-sikkerhet for industrielle IKT-systemer. Rapporten «IKT-sikkerhet – Fjernarbeid og HMS»[1] fra Sintef er en del av dette arbeidet. Rapporten er basert på 14 gruppeintervju høst 2018/vinter 2019 med representanter fra operatørselskaper, boreselskaper og systemleverandører, samt gjennomgang av relevant litteratur, dokumenter fra operatør- og boreselskaper og SINTEFs generelle kompetanse og erfaring innenfor HMS og IKT-sikkerhet.

[1] «IKT-sikkerhet – Fjernarbeid og HMS», 05.04.2019, https://www.ptil.no/globalassets/fagstoff/prosjektrapporter/ikt-sikkerhet/sluttrapport-ptil-ikt-sikkerhet---fjernarbeid-og-hms-med-underskrift-og-vedlegg.pdf