Regulering og informasjonssikkerhet for industrielle IKT-systemer

Asbjørn Ueland, sjefingeniør

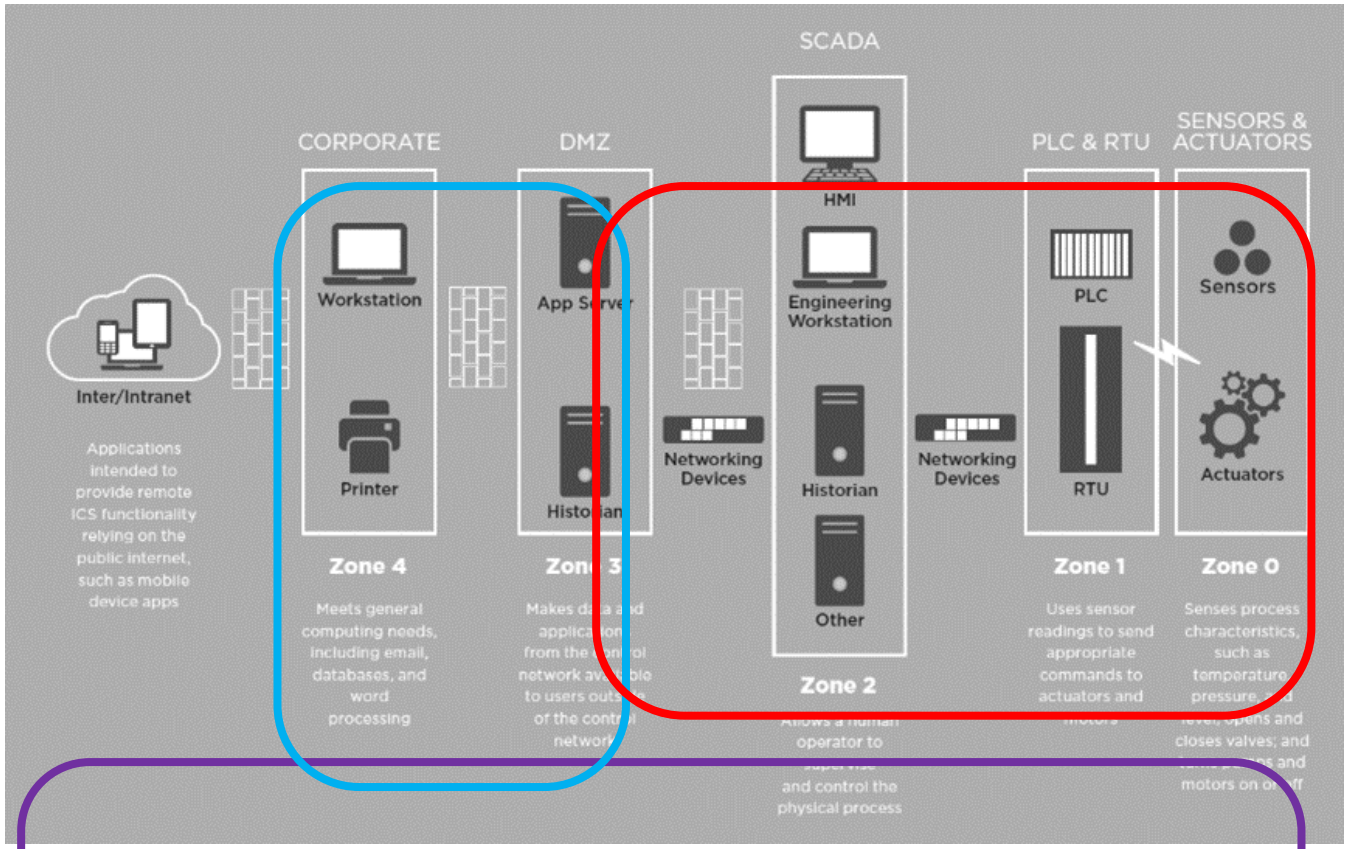
Ansvarsforhold

Petroleumstilsynet har myndighetsansvar for sikkerhet, beredskap og arbeidsmiljø i petroleumsvirksomheten på norsk kontinentalsokkel

- Krav til tekniske systemer ombord, ref IF §§ 32-34a
  - … kan ha grensesnitt mot andre systemer dersom det ikke kan bli negativt påvirket som følge av …
- Krav om funksjoner f.eks. vedlikehold og planlegging, ref AF § 45 og § 48

Digitalisering

- Eksisterende informasjon: design, undergrunn, 3D-modell etc.
- Driftsdata (dataeksport fra kontrollsystemer til database i kontornettet)
- IIoT (data fra nye smarte instrumenter på eget nettverk)



Vår regulering

SF § 4: … tekniske, operasjonelle og organisatoriske løsninger som reduserer sannsynligheten for at det oppstår skade …

SF § 8: … interne krav som konkretiserer krav i regelverket, og som bidrar til å nå målene for helse, miljø og sikkerhet.

SF § 29: … skriftlig melding om hendelser …
Veiledning: situasjoner der normal drift … blir forstyrret av arbeid som ikke er planlagt (IKT-hendelse)

AF § 45: … holdes ved like, slik at de er i stand til å utføre sine krevde funksjoner i alle faser av levetiden.

AF § 48: … plan for utføring av vedlikeholdsprogram og korrigerende vedlikeholds-aktiviteter

IF § 32, § 33 og § 34: Systemet skal kunne utføre tiltenkte funksjoner uavhengig av andre systemer.
Veiledning: … kan ha grensesnitt mot andre systemer dersom det ikke kan bli negativt påvirket …

IF § 34a, veiledning: … kan ha grensesnitt mot andre systemer, men bør sikres slik at dette ikke svekker systemet. I tillegg bør Norsk olje og gass retningslinje nr. 104 legges til grunn for beskyttelse mot IKT-relaterte farer.

AF § 21: … personellet skal ha nødvendig kompetanse til å utføre aktivitetene … og håndtere fare- og ulykkessituasjoner

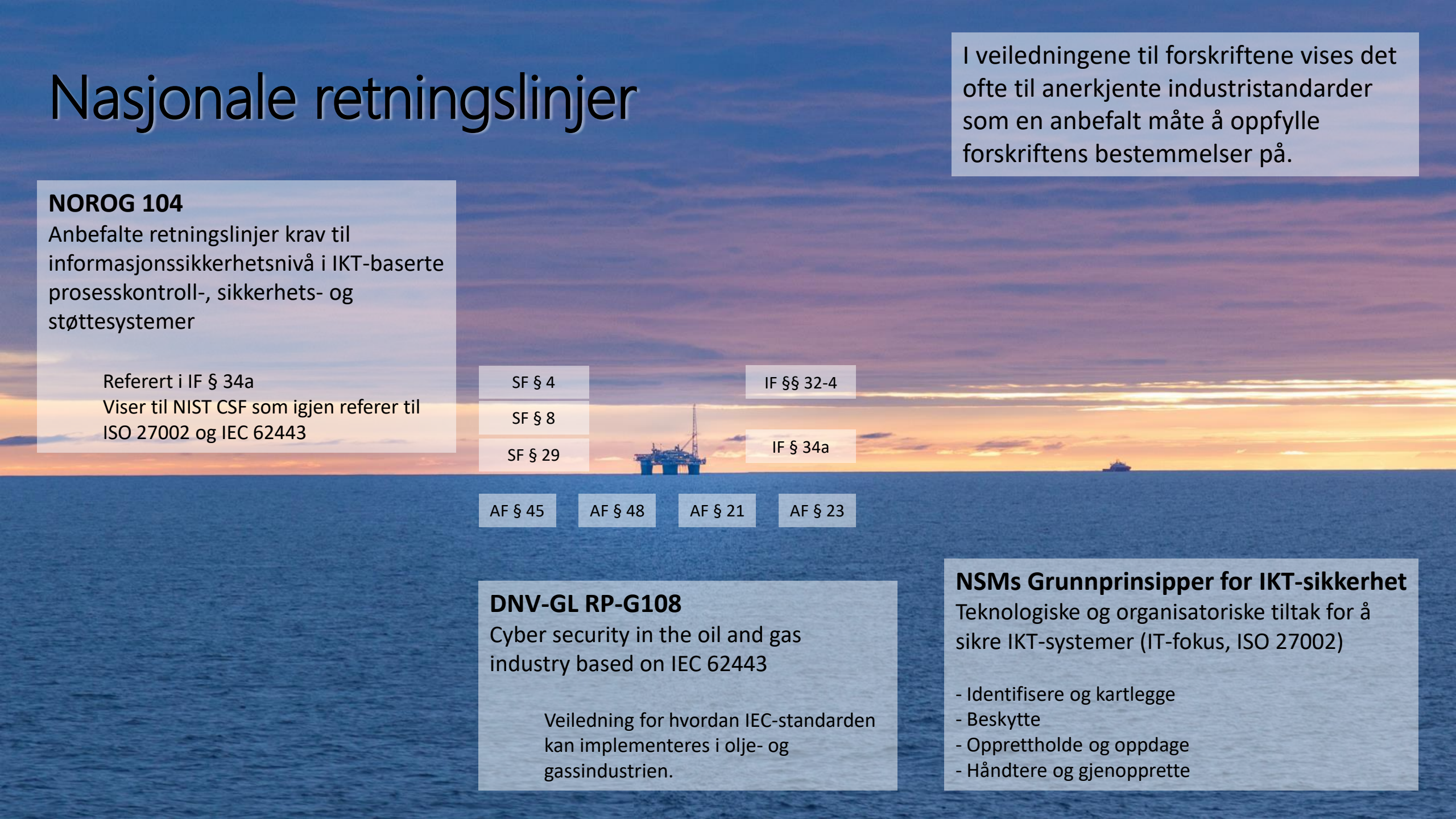
AF § 23: … nødvendig trening og nødvendige øvelser, slik at personellet til enhver tid er i stand til å håndtere operasjonelle forstyrrelser og fare- og ulykkessituasjoner

Nasjonale retningslinjer

I veiledningene til forskriftene vises det ofte til anerkjente industristandarder som en anbefalt måte å oppfylle forskriftens bestemmelser på.

NOROG 104
Anbefalte retningslinjer krav til informasjonssikkerhetsnivå i IKT-baserte prosesskontroll-, sikkerhets- og støttesystemer

Referert i IF § 34a
Viser til NIST CSF som igjen referer til ISO 27002 og IEC 62443



DNV-GL RP-G108
Cyber security in the oil and gas industry based on IEC 62443

Veiledning for hvordan IEC-standarden kan implementeres i olje- og gassindustrien.

NSMs Grunnprinsipper for IKT-sikkerhet
Teknologiske og organisatoriske tiltak for å sikre IKT-systemer (IT-fokus, ISO 27002)

- Identifisere og kartlegge
- Beskytte
- Opprettholde og oppdage
- Håndtere og gjenopprette

NSMs Grunnprinsipper for IKT-sikkerhet

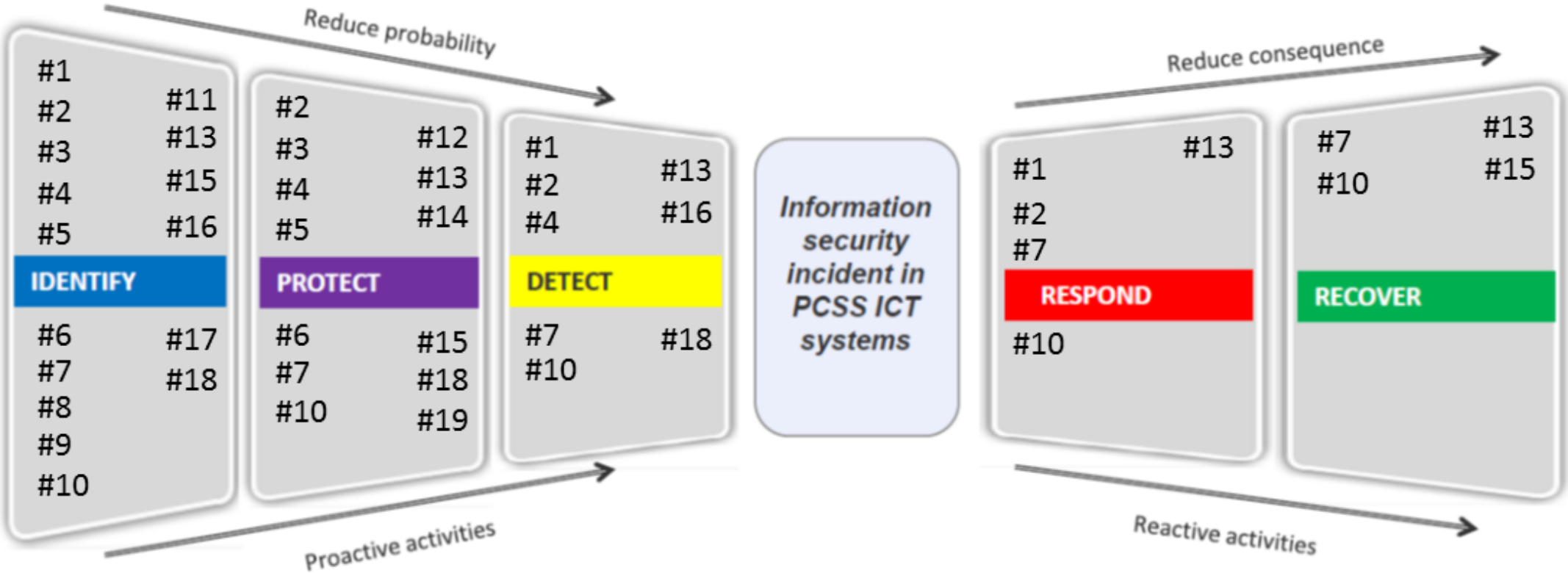
- Identifisere og kartlegge
- Beskytte
- Opprettholde og oppdage
- Håndtere og gjenopprette

Retningslinje 104 (NOROG)

NIST CSF

Cyber Security Framework

- Identify
- Protect
- Detect
- Respond
- Recover



ARCHITECTURE

The planning, establishing, and upkeep of systems with security in mind

PASSIVE DEFENSE

Systems added to the Architecture to provide reliable defense or insight against threats without consistent human interaction

ACTIVE DEFENSE

The process of analysts monitoring for, responding to, and learning from adversaries internal to the network

INTELLIGENCE

Collecting data, exploiting it into information, and producing Intelligence

OFFENSE

Legal countermeasures and self-defense actions against an adversary

SANS ICS Industrial Control Systems