IKT-sikkerhet

Erfaring og status fra sikringstilsyn og prosjekter innen IKT-sikkerhet

Espen Seljemo
Sjefingeniør
Petroleumstilsynet
espen.seljemo@ptil.no

PETROLEUMSTILSYNET

Trusler og angrep. Stuxnet 2010

- **Stuxnet – Iran**

Det er den første kjente dataormen som spionerer på og omprogrammerer industrielle systemer. Det ble spesielt skrevet for å angripe Supervisory Control and Data Acquisition (SCADA) systemer.

wikipedia

Stuxnet does little or no harm to computers not involved in uranium enrichment. When it infects a computer, it checks to see if that computer is connected to specific models of programmable logic controllers (PLCs) manufactured by Siemens

The U.S. and Israeli governments intended Stuxnet as a tool to derail, or at least delay, the Iranian program to develop nuclear weapons.
CSOonline.com

Trusler og angrep. WannaCry 2017

Trusler og angrep. NotPetya, sommer 2017

- Maersk Chairman Jim Hagemann Snabe said while participating on a cybersecurity panel at the conference that his company **replaced 45,000 PCs, 4,000 servers and install 2,500 applications.** The computer system runs an operation where **a ship carrying 20,000 containers enters a port every 15 minutes** somewhere around the world. Overall, Maersk handles 20 percent of all world trade, he said.
- **“We found we had to reinstall our entire infrastructure.** It was done in a heroic effort in just 10 days,” he said, adding such a job should take about six months to complete.
- The massive IT undertaking along with business lost due to the almost total shutdown of the company's computer network has **cost Maersk between $250 million and $300 million**

Maersk Reinstalled 45,000 PCs and 4,000 Servers to Recover From NotPetya Attack

- Maersk gruppen
- NotPetya

NOTPETYA

Mærsk tapte opptil 2,5 milliarder kroner på dataangrep

Trusler og angrep vår 2018

- *Dataangrepet skal være en del av en spionasjekampanje rettet mot ulike lands myndigheter, bedrifter og kritisk infrastruktur, opplyser etterretningsorganisasjonene i landene, som sier at de har «stor tillit» til rapportene.*

- Sårbarheter i nettverksutstyr:
  Switcher, porter, gateway
  Sårbarhet i software/ firmware i switcher og routere

Flickr.com

Kilde: Dagblad.no 17.04.2018

«En verden av begreper»

IKT: Informasjons og kommunikasjonsteknologi

- Samlebegrep som oftest fokuserer på kontorsystemer: Innsamling, lagring, behandling og overføring.

IT: Informasjonsteknologi

- Typisk kontorsystemer

OT: Operasjonell teknologi

- Industrielle kontrollsystemer, sikkerhetssystemer, industrialisert kontroll teknologi, SAS styring- og kontrollsystemer

IKT sikkerhet

Cyber security

Anti virus

Malware

Ransomware

Industroyers

Stuxnet

notPetaya

WannaCry

IKT-sikkerhet

Hvorfor er det viktig å følge opp IKT-sikkerhet

- Forankring i ledelse og fokusområde
- Trusler, sårbarheter og vurderinger
- IKT systemer og prosesser

  Det «digitale forsvar», hva skal sikres, passiv og aktiv beskyttelse og restrisiko
- IKT sikkerhet er et livsløp

Design, prosjektering, drift- og vedlikehold og avinstallering/ erstatning av nye løsninger.

- Trening og øvelse (scenario/ casebasert)

Vårt ansvarsområde

CA **80** Faste innretninger/plattformer

59 Rigger/innretninger med SUT

CA **300** Havbunnsinnretninger

8 Landanlegg

25 000 Mennesker

15 400 Km undervanns-rørledninger

Sørlige del av Nordsjøen	Midtre del av Nordsjøen	Nordlige del av Nordsjøen	Norskehavet	Barentshavet	Landanlegg
Brynhild	Atla	Brage	Alve	Snøhvit	1 Kårstø
Blane	Alvheim	Fram	Draugen		2 Kollsnes
Ekofisk	Balder	Fram H-Nord	Heidrun		3 Sture
Eldfisk	Bøyla	Gimle	Hyme		4 Mongstad
Embla	Edvard Grieg	Gjøa	Kristin		5 Nyhamna
Gaupe	Enoch	Gullfaks	Marulk		6 Tjeldbergodden
Gyda	Grane	Gullfaks Sør	Mikkel		7 Melkøya
Hod	Gudrun	Knarr	Morvin		8 Slagentangen
Oselvar	Gungne	Kvitebjørn	Njord		
Tambar	Heimdal	Oseberg	Norne		
Tambar Øst	Islay	Oseberg Sør	Ormen Lange		
Trym	Jette	Oseberg Øst	Skarv		
Ula	Jotun	Snorre	Skuld		
Valhall	Rev	Statfjord	Tyrihans		
	Ringhorne Øst	Statfjord Nord	Urd		
	Sigyn	Statfjord Øst	Åsgard		
	Skirne	Sygna			
	Sleipner Vest	Tordis			
	Sleipner Øst	Troll			
	Svalin	Tune			
	Vale	Valemon			
	Varg	Vega			
	Vilje	Veslefrikk			
	Volund	Vigdis			
	Volve	Visund			
		Visund Sør			

82 Felt i produksjon per 1.1. 2016

Varsel om tilsyn – IKT-sikkerhet

1. Risikovurdering
2. IKT-arkitektur
3. Passive beskyttelses-tiltak
4. Monitorering, analyse og respons.
5. Rapportering
6. Egne tilsyn og revisjoner

2-timer møte med hver enkelt

- operatør eller
- reder

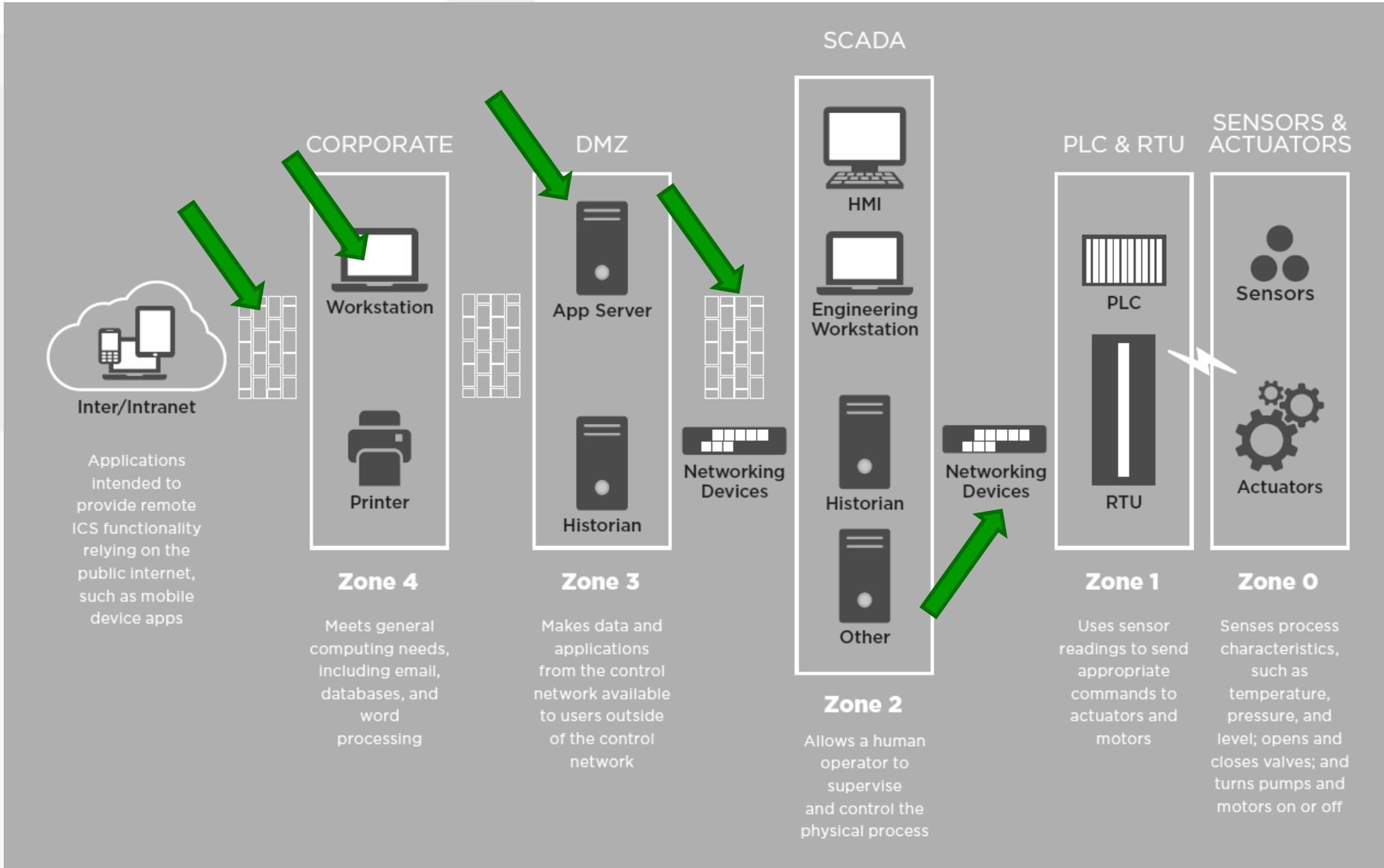
Presentere selskapets svar på de 6 punktene

- Varsel i feb -17
- Møter i mai/juni 17

- Vi etterspør **tekniske**, **organisatoriske** og **operasjonelle forhold**

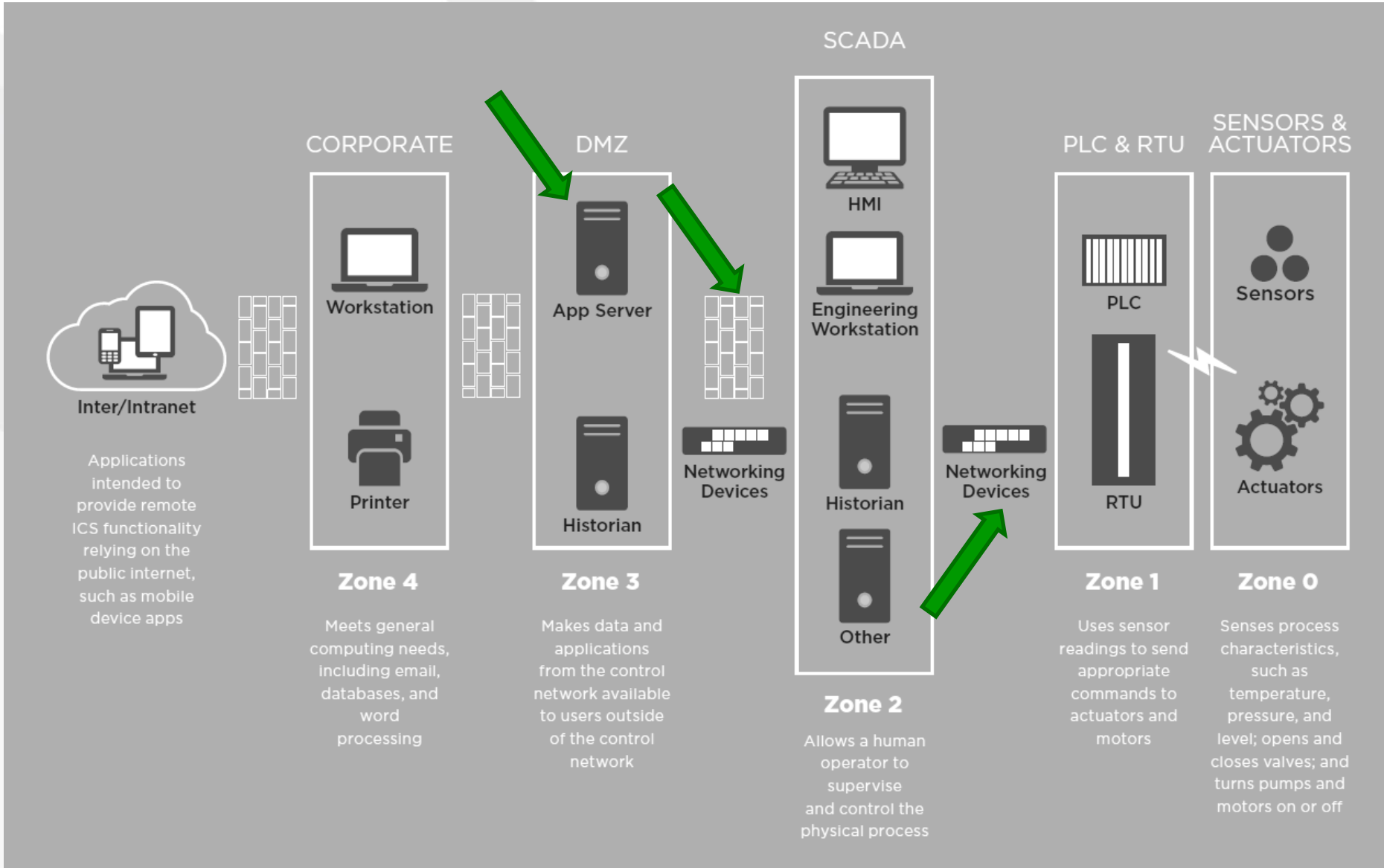
Passive beskyttelses-tiltak

1. Risikovurdering
2. IKT-arkitektur
3. Passive beskyttelses-tiltak
4. Monitorering, analyse og respons.
5. Rapportering
6. Egne tilsyn og revisjoner



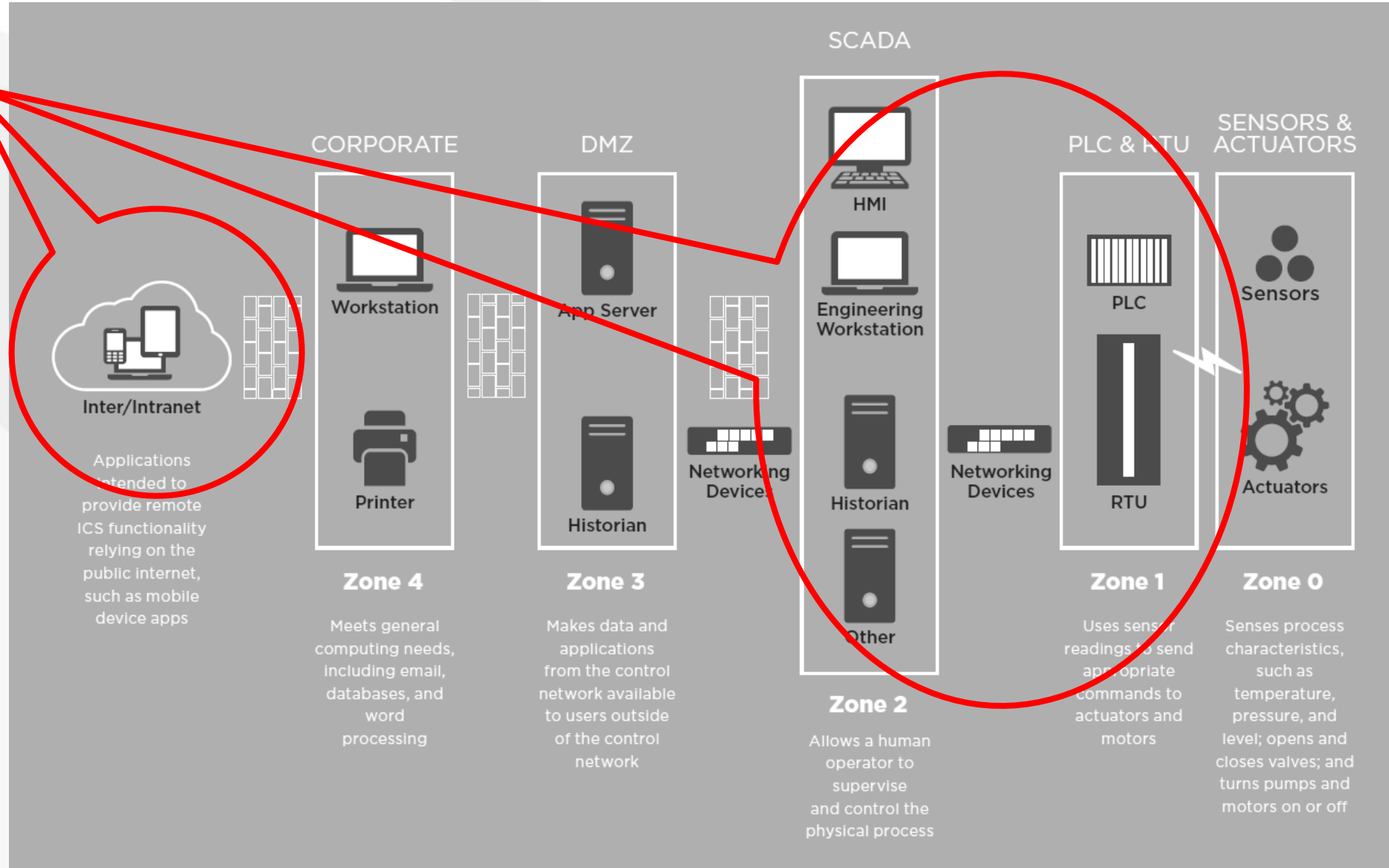
Monitorering, analyse og respons

1. Risikovurdering
2. IKT-arkitektur
3. Passive beskyttelses-tiltak
4. Monitorering, analyse og respons.
5. Rapportering
6. Egne tilsyn og revisjoner

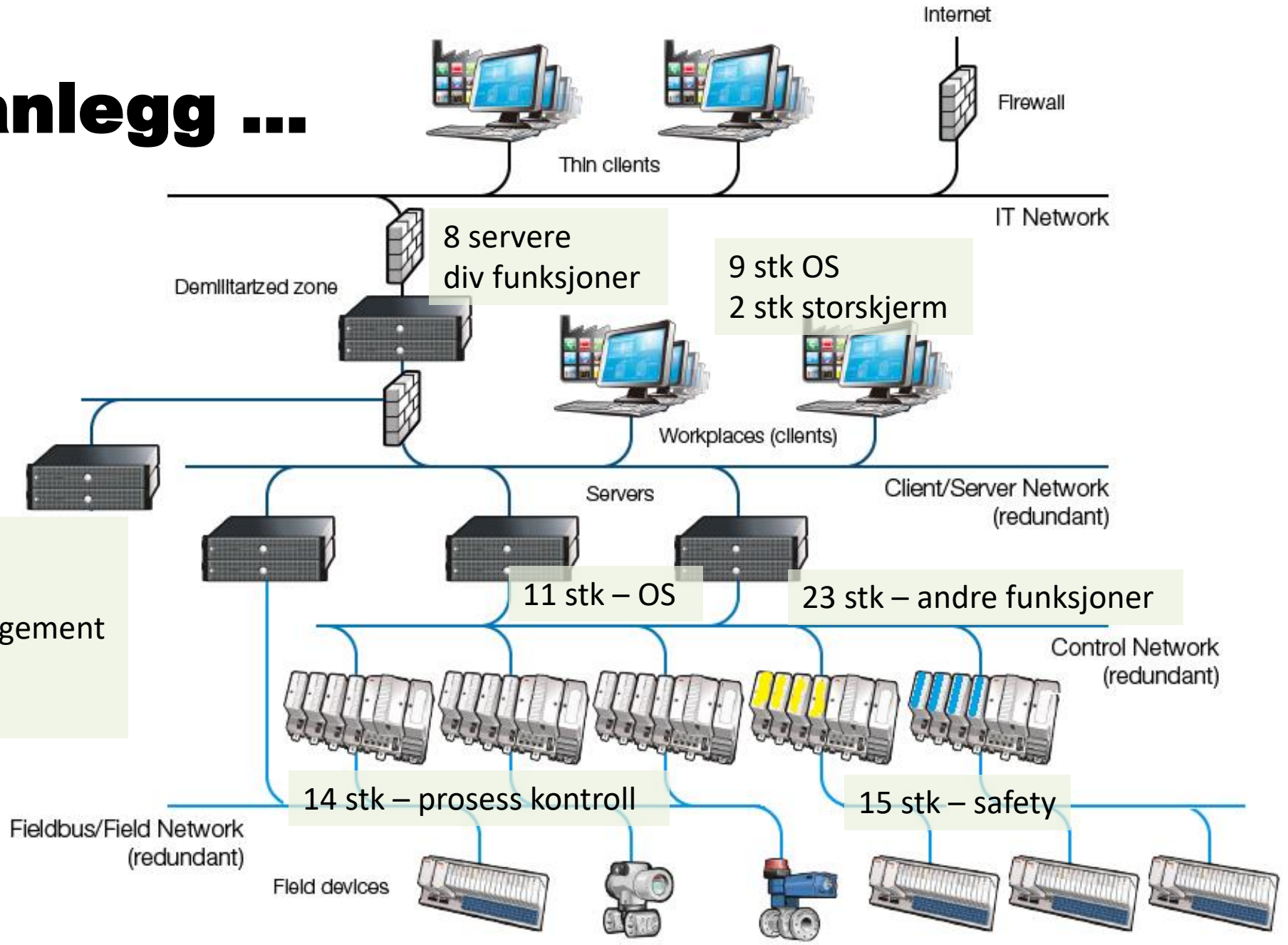


Ulik fokus på risiko:
aktør – sårbarhet – konsekvens

1. Risikovurdering
2. IKT-arkitektur
3. Passive beskyttelses-tiltak
4. Monitorering, analyse og respons.
5. Rapportering
6. Egne tilsyn og revisjoner



Et typisk anlegg …

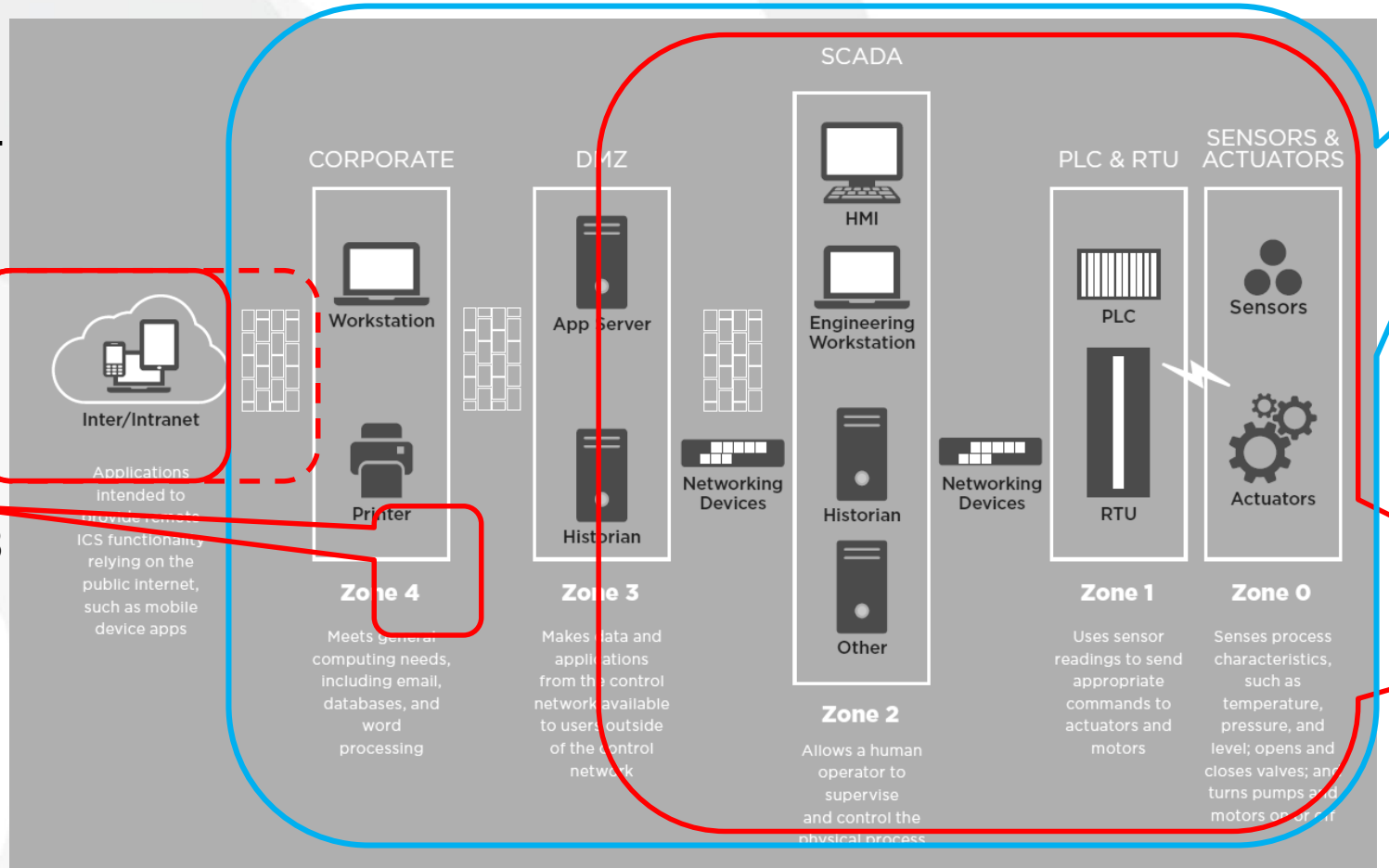


5 andre system
- Metering
- Power management
- Miljødata
- …

Figur basert på illustrasjon fra new.abb.com: 800xA Network Topologies - 800xA DCS (System 800xA)

IKT-sikkerhet – samspill og ansvarsområder

- Fagdepartement – **overordnet sektoransvar**
- Virksomhetens ansvar
- NSM/NorCERT
- Datatilsynet
  (persondata)
  GDPR 1. mai 2018
- Ptil



Forankring i standarder

- NOROG Retningslinje 104
  - Utarbeidet i -06, revidert i -16
- IEC/ISO 62443
  - 62443-1-1 ferdig i -06, noen av totalt 13 deler er fortsatt i draft
- NIST CSF og 800-82
  - CSF: -14, 800-82: -06, rev.2 i -15
- Maritimt regelverk – DNV-GL, ISPS og IADC
  - DNVGL-RP-0496: -16
- IEC/ISO 27001
  - Fokus på generell IT, ikke industrielle styringssystemer
- Interne retningslinjer forankret i ovenfor nevnte standarder
  - Statoil TR1658v5: -15

DNV-GL RP-G108, Cyber security in the oil and gas industry based on IEC 62443 (2017) (utgitt september 2017)

Satsing IKT-sikkerhet
Mål og bakgrunn

Bakgrunn
Forankret hos departementet og i tildelingsbrev
Rapporter fra ulike utvalg og Stortingsmelding

Mål
- Næringen holder et forsvarlig nivå for IKT-sikkerhet innen operasjonell teknologi og industriell IKT

- Hovedmål med prosjektene er å beskrive de endringene/ driverne som påvirker risikobilde innen industrialisert kontroll teknologi (IKT) på innretninger som har petroleumsvirksomhet på norsk sokkel.

- Prosjektene er spisset innen IKT, operasjonell teknologi (OT) som er tilsynsområdet for Petroleumstilsynet (Ptil).

Hvorfor satsing på IKT sikkerhet?
- Øke forståelse og bevissthet ytterligere innen området
- Ny teknologi og flere integrerte systemer
- Mer deling av data mellom systemer og lokasjoner.
- Hvordan endres risikobilde og hvordan ivaretas HMS

IKT-sikkerhet satsinger 2018

Prosjekt
1. Kunnskapsprosjekt IKT (CERT) Computer emergency response team (CERT) funksjon i næringen. Prosjektet skal belyse CERT kapasitet i næringen Vurdere lignende CERT løsninger i andre segmenter nasjonalt og internasjonalt. SektorCERT. KraftCERT
2. IKT sikkerhet- Fjernarbeid og HMS Definere og innhente kunnskap om fjernarbeid på sokkelen. Dette er spisset innen bruk av remote oppkobling fra land mot innretninger, landanlegg og rigger. Se spesielt på hyppighet, hvilke typer endringer som utføres via remote og fjernarbeid med fokus på HMS og arbeidsprosesser
3. IKT sikkerhet- Infrastruktur og segregering Se på utviklingen av industrialiserte IKT systemer med fokus på at tidligere proprietær løsninger er blitt mer IT og nettverksbaserte. Dette kan øke risikoen for IKT hendelser på slike systemer siden mer utstyr er koblet sammen i nettverk og det er forbindelser mellom de ulike nettverkslagene mellom IT og OT. Viktig å se på integriteten av slike løsninger mtp HMS risikoen de potensielt kan introdusere ved at sensorer er blitt nettverksbaserte og smarte.
4. IKT sikkerhet- Kunnskapsøkning og læring Knytte kontaktnett på tvers i næringen og utenfor næringen. DSB, UK, NSM, KraftCERT Norge, NVE, NIST (USA) med flere. Delta i ulike fora og seminarer med relevans innen IKT sikkerhet for industriell IKT.
5. IKT sikkerhet- Trening og øvelser Øke fokus og kunnskap hos selskapene innen trening og øvelser på IKT hendelser i OT domenet (industrielle kontrollsystemer). Dialog med næring, NOROG, KraftCERT, NSM/NorCERT Kryssjekk standardene NIST CFM, NOG retningslinje 104, IEC62443 med fokus på trening og øvelser. GAP analyse
6. Digital teknologi og IKT sikkerhet Digitalisering og HMS effekter av dette i næringen. Petroleumsindustrien gjennomgår for tiden flere parallelle omstillingsprosesser knyttet til krav om økt kostnadseffektivitet, nedbemanninger, organisasjonsendringer og langsiktig lønnsomhet ved å ta i bruk nye arbeidsformer og omstilling til flere digitale løsninger.

IKT- sikkerhet
Fremtidsutsikter

- **Hva skjer i fremtiden:**
  - Mer bruk av teknologi og smarte enheter, "alt kobles sammen"
  - Digitalisering, Big Data, data i skyen, appstyrte verktøy, robotisert software og beslutningsstøtte/verktøy

- **«Digital konvergens»**
  - Overgang fra analoge manuelle systemer til digitale løsninger og prosesser
  - Sammensmelting av nettverk (IT OT og CDE TDE ODE) og integrering av flere systemer/utstyr, sendes risikoer ut på vandring?
  - Er vi i ferd med å lage nye angrepsflater med ytterligere sårbarheter for industriell IKT system (OT) som tidligere har vært proprietært og "innesluttet"?

- **Kan vi sikre oss godt nok?**
  - Hvilken rest risiko er vi villige til å akseptere innen IKT sikkerhet og det «*digitale forsvar*».