

# Cyber Security

What we think and what we know?

Asbjørn Ueland

Principal Engineer

Petroleum Safety Authority



- **The stories from the press**
- **The incident at Statoil Mongstad**
- **2017 audit at all operators and ship owners**
- **Regulations**





# The stories from the press

**NRK** Nyheter Sport TV Radio Distrikt

Norge Siste nytt Dokumentar Klima NRK Ytring

## Cyberangrep mot No

I fjor avslørte norske myndigheter mer enn 22 000 dataangrep offentlige etater. Urovekkende økning, sier Nasjonal sikkerhetsmyndighet.



**OVERVÅKER:** Risikoen for at kritiske funksjoner i landet blir rammet av alvorlige handlinger er økende. Dette er fra rommet hvor Nasjonal sikkerhetsmyndighet overvåker trafikken i Internett.

FOTO: SIRI VÅLBERG SAUGSTAD/NRK

**digi.no** MENY LOGG INN Ekstra Mobilabonnement bedrift IT-kurs Tips oss



Sven-Erik Egge er leder av DSS CERT, operasjonssentralen som fanger opp og håndterer digitale angrep mot regjeringen og departementene i Norge.

## DSS CERT Her stanser de 500 millioner angrep mot regjeringen og departementene i Norge

Jeg liker å bruke ordet «paranoid». Det er helt i orden å være super-paranoid.

AV: MARIUS JØRGENRUD | PUBLISERT: 17. JAN. 2017 - 15:42


REGJERINGSKVARTALET (digi.no): – Jeg liker å bruke ordet «paranoid». Det er helt i orden å være super-paranoid.

Det sier Sven-Erik Egge, mannen som gjennom flere år har bygget opp det operative IKT-sikkerhetsmiljøet i regjeringens kvartale.

Departementenes sikkerhetsmiljøet er blitt et av de mest sikre i Norge.

**DN Dagens Næringsliv** Oslo Børs: 11.36 Indeks: 691,48 +0,15

**DN Investor. Overvåk markedet med skreddersydd**



Mongstad, 06. april 2016: Statoils raffineri på Mongstad. Kjøleanlegg. Foto: Eivind Senneset

## Energi Statoil Tastefeil i India stanset produksjonen på Mongstad

Sikkerheten ved Statoils anlegg er flere ganger satt i fare etter at driften av datasystemer ble satt ut til et selskap i India, viser flere interne rapporter.

NTB  
Publisert: 28.10.2016 – 09:41 Oppdatert: 28.10.2016 – 09:55

Etter at Statoil i 2012 satte bort IT-arbeidet har det vært en rekke potensielt farlige situasjoner på Statoils anlegg og plattformer. Det viser interne rapporter. NRK har fått tilgang til.



# Statoil Mongstad

## Refinery

- Located at Norwegian west coast, north of Bergen
- Capacity: ~ 12 million tonnes of crude oil per year

## Port

- the second largest oil and product port in Europe after Rotterdam (measured in volume)
- ~ 1700 dockings per year



# Cyber incident at Mongstad?

## Background

- Journalist at NRK requested information about an incident at Mongstad causing shutdown and oil spill
- Statoil confirms an ICT incident , but only minor economic impact, neither shutdown nor oil spill
- Statoil informs PSA about the incident
- The same evening: NRK breaking news - many ICT incident at Statoil





# PSA Audit - ICT security at Statoil



- General:
  - An audit, not an investigation
  - Information from Statoil did not indicate violation of regulation
- Purpose:
  - Verify robustness of barriers within ICT security
- Findings:
  - No oil spill, no plant shutdown,
  - A server restart controlling quality of export oil
- Public audit report (4 lines of text and the document list were removed)

# Underlying cause





# Audit 2017

All operators and ship owners in the Norwegian oil industry to present:

- Risk assessment of threats for the OT domain
- OT architecture and interface to other systems
- Passive protection
- Monitoring, analysis and response related to cyber irregularities
- Procedures for reporting cyber issues
- Audits and findings

-INTERNET  
-LIVE CHAT  
-MEDIA  
-PHOTOS  
-VIDEOS  
-MUSIC



# Risk assessment in the OT domain

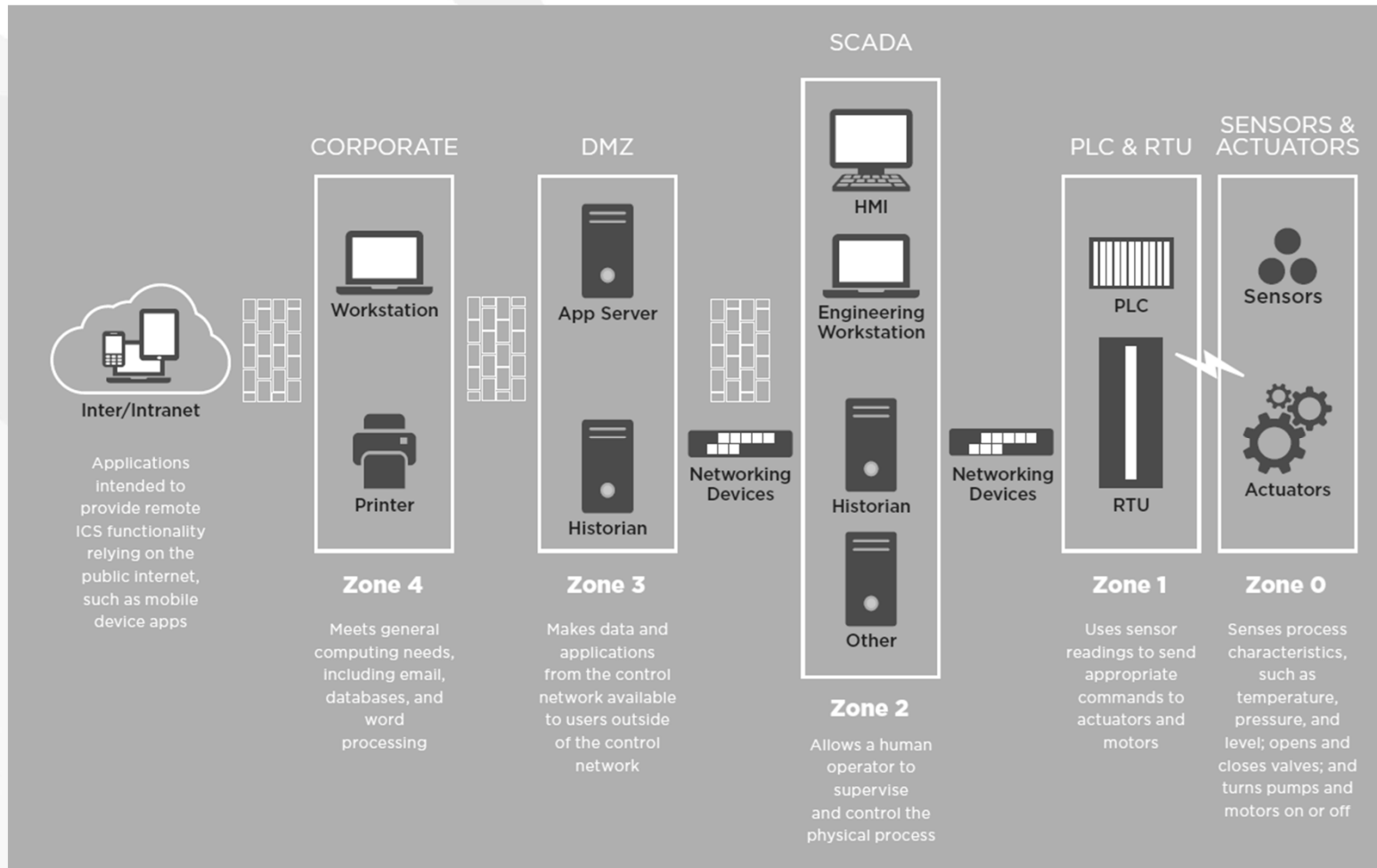
- Some understand that the threat issue and works integrated with their HSE departments
- Others don't have a risk assessment approach at all, just implementing basic security and measures related to vulnerabilities





# OT architecture and interface to other systems

- OT isolated from IT
  - Firewall and DMZ
- Controlled vendor access
  - Request from inside
  - Access to specified computer and use of terminal servers
- Historian with read only
  - Condition based maintenance
  - Big data & digitalisation





# Audits and findings

- IT domain and employees are under pressure
- No one has experienced any critical issues
  - Virus detection as part of vendor support when using their own PC
- No one has experienced insiders
- No one has seen external attacks towards OT environment





# General questions

- How are we doing?
- What can we learn from the others?
- How to maintain ICT security when system no longer are supported?
  
- We plan to host a workshop for all participants to
  - Present findings and discuss solutions
  - Enable for networking



# Current regulation points to industry guideline

## Norwegian Oil and Gas Industry guideline (NOROG 104)

Recommended guideline on information security baseline requirements for process control, safety and support ICT system

- A guideline based on ISO 27002 and adjusted for OT environment
  - 16 requirements with implementation guide
  - References to relevant chapters in 27001 and 27002
  - Published 09.06.2006
- Guideline revised and expanded in 2016
  - 3 new requirements
  - implementation guide in line with NIST CSF





**Thank you for attention**



**System Protected**

