Cyber threats and the petroleum industry

Possibilities for learning?

Asbjørn Ueland
Petroleum Safety Authority Norway

PETROLEUMSTILSYNET

Asbjørn Ueland

- Principal engineer – department for process integrity
  - Process control & safety systems
  - Safety systems independence – SIL
  - Alarm management
  - ICT security
  - Regulations and guidelines

- 23 years in the industry:
  - Technical authority – process control & safety systems
  - System responsible – process control & safety systems
  - ICT security responsible – process control & safety systems
  - Maintenance – procedures and follow-up for F&G instruments
  - NOROG 104 guideline

Asbjørn Ueland
Principal engineer
Petroleum Safety Autority
Norway
E-mail:
asbjorn.ueland@ptil.no
Phone: (+47) 51 87 35 08
Mobile: (+47) 918 02 563

Agenda

1. Critical infrastructure on the agenda
2. Rules and regulation – IT versus OT
3. Cyber security audit at the Norwegian petroleum sector
   – findings and learning


Picture to be replaced by video!

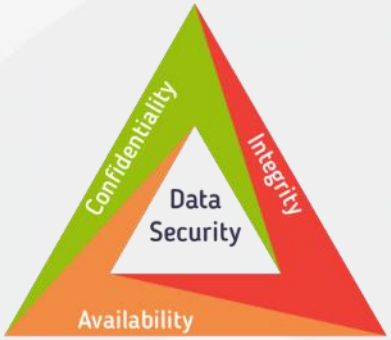
Cyber security history for industrial systems

- 1998
  - Presidential Decision Directive from Bill Clinton
- 2002
  - ISA99 established
- 2004
  - NIST: System Protection Profile – ICS
  - NOROG: 104 work started
- 2006
  - NOROG: 104 published
  - IEC/ISO 62443-1-1
- 2007
  - Aurora generator test
- 2010
  - Stuxnet discovered
  - NERC: Recommendation to industry on the Aurora vulnerability
- 2012
  - Stuxnet understood
- 2013
  - Presidential Order from Barack Obama: Improving Critical Infrastructure Cybersecurity
- 2014
  - NIST CSF published
  - KraftCERT established
- 2016
  - NOROG 104 revised

Based on "An Abbreviated History of Automation & Industrial Controls Systems and Cybersecurity" from SANS

Red text are Norwegian specific events
NOROG – Norwegian Oli and Gas

Rules and regulations for Cyber security



Information about people

GDPR

Automation & industrial control
Critical infrastructure

NIS directive
Industry standards

Digitalisation

Companies to regulate
(Act of Security)

Authorities – regulations for Cyber security

- Ministry – **sector responsibility**
- Company responsibility
- National Security Authority
- PSA

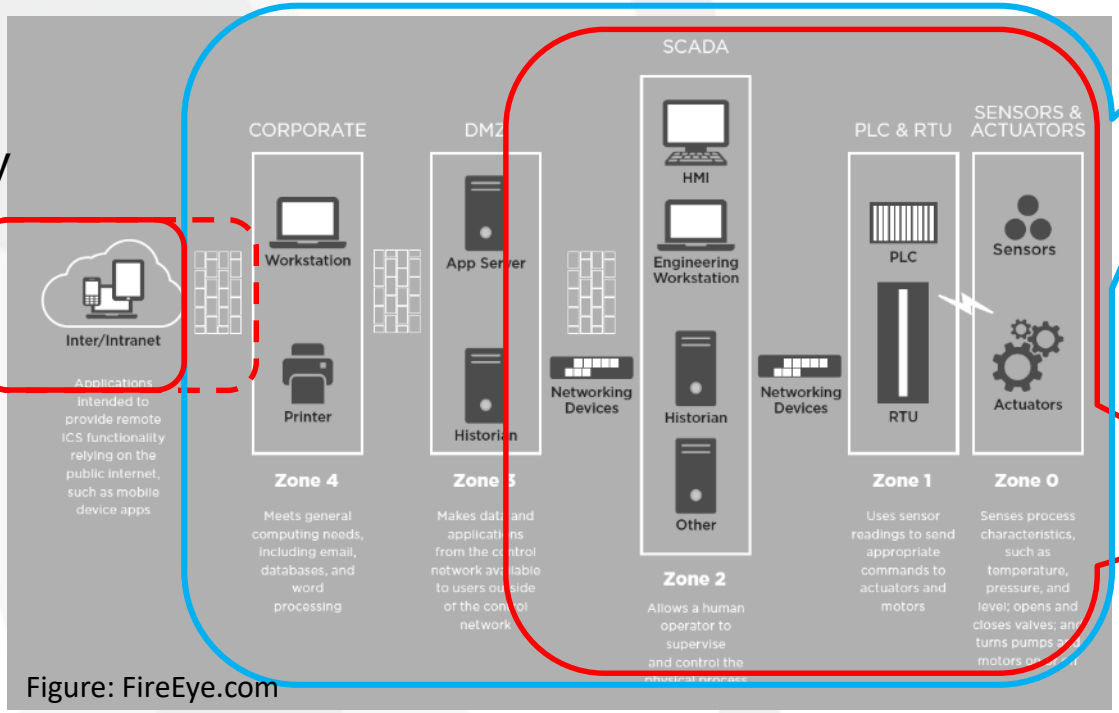


Figure: FireEye.com

Audit – Cyber security

- Risk assessments
- ICT architecture and links to other systems
- Passive safeguards
- Monitoring, analysis and response
- Incident reporting
- Own audits and reviews

2 hour presentation from each

- operator
- ship owner

- Technical, organizational and operational questions

References to standards and guidelines

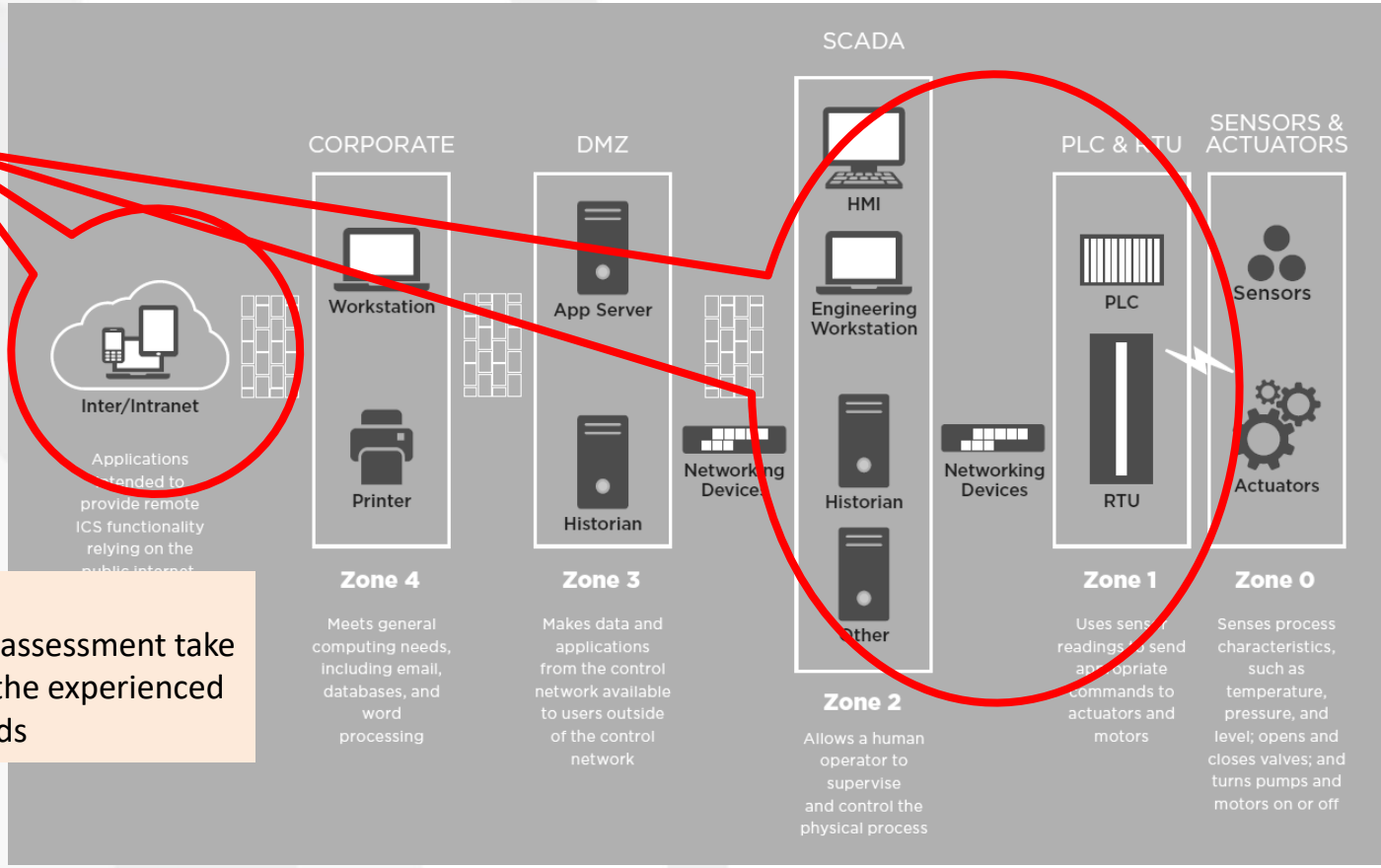
- NOROG 104
  - Published: -06, revised: -16
- IEC/ISO 62443
  - 62443-1-1 published in -06, some parts still in draft mode
- NIST CSF and 800-82
  - CSF: -14, 800-82: -06, rev.2 i -15
- Maritime regulations – DNV-GL, ISPS and IADC
  - DNVGL-RP-0496: -16,
- IEC/ISO 27001
  - Focus at general IT, not industrial control systems

- Internal requirements based on above
  - Equinor TR1658v5: -15

Risk assessment:

Focus on

- actor
- vulnerability
- consequences

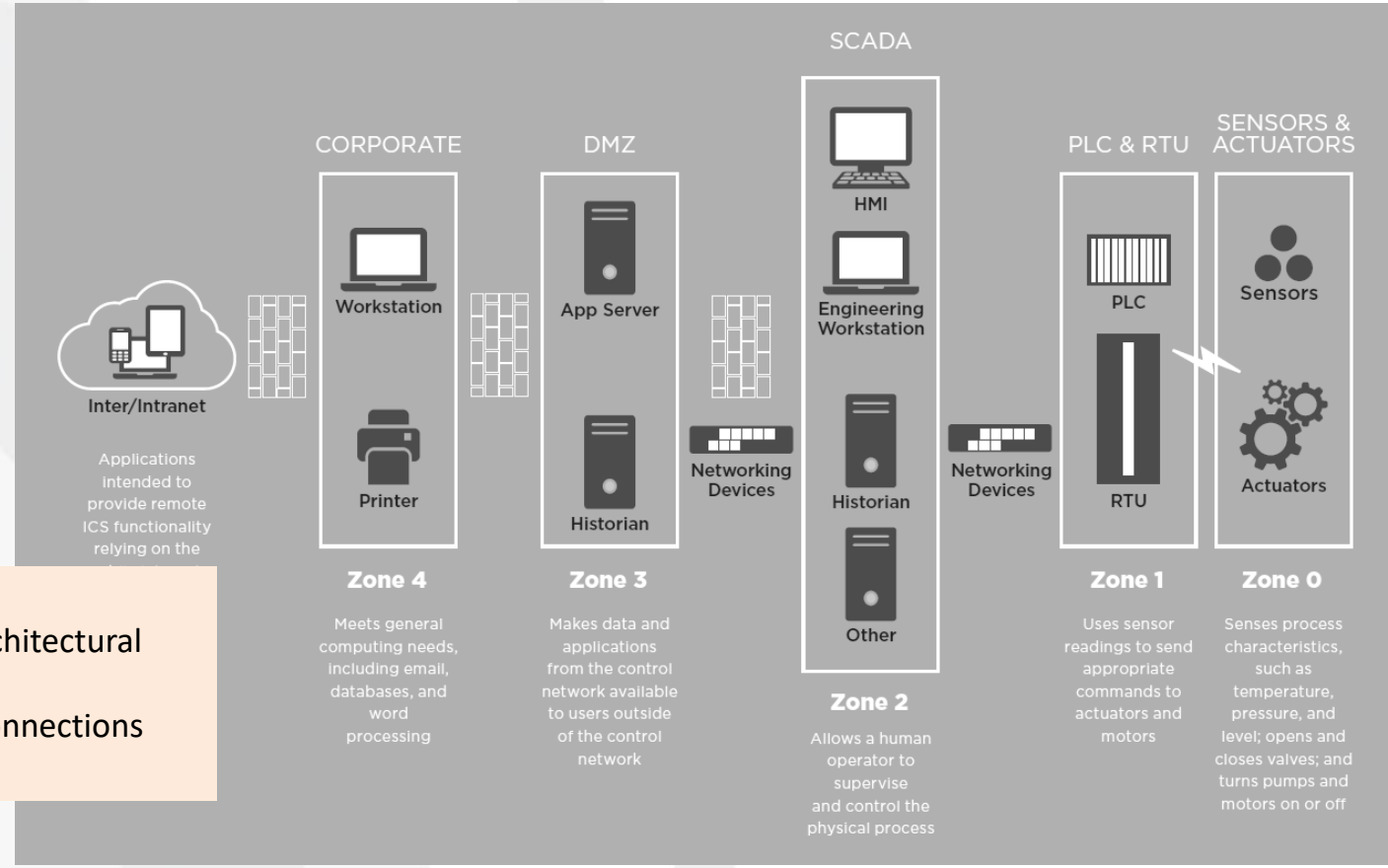


Challenge:

- Does our risk assessment take into account the experienced attack methods

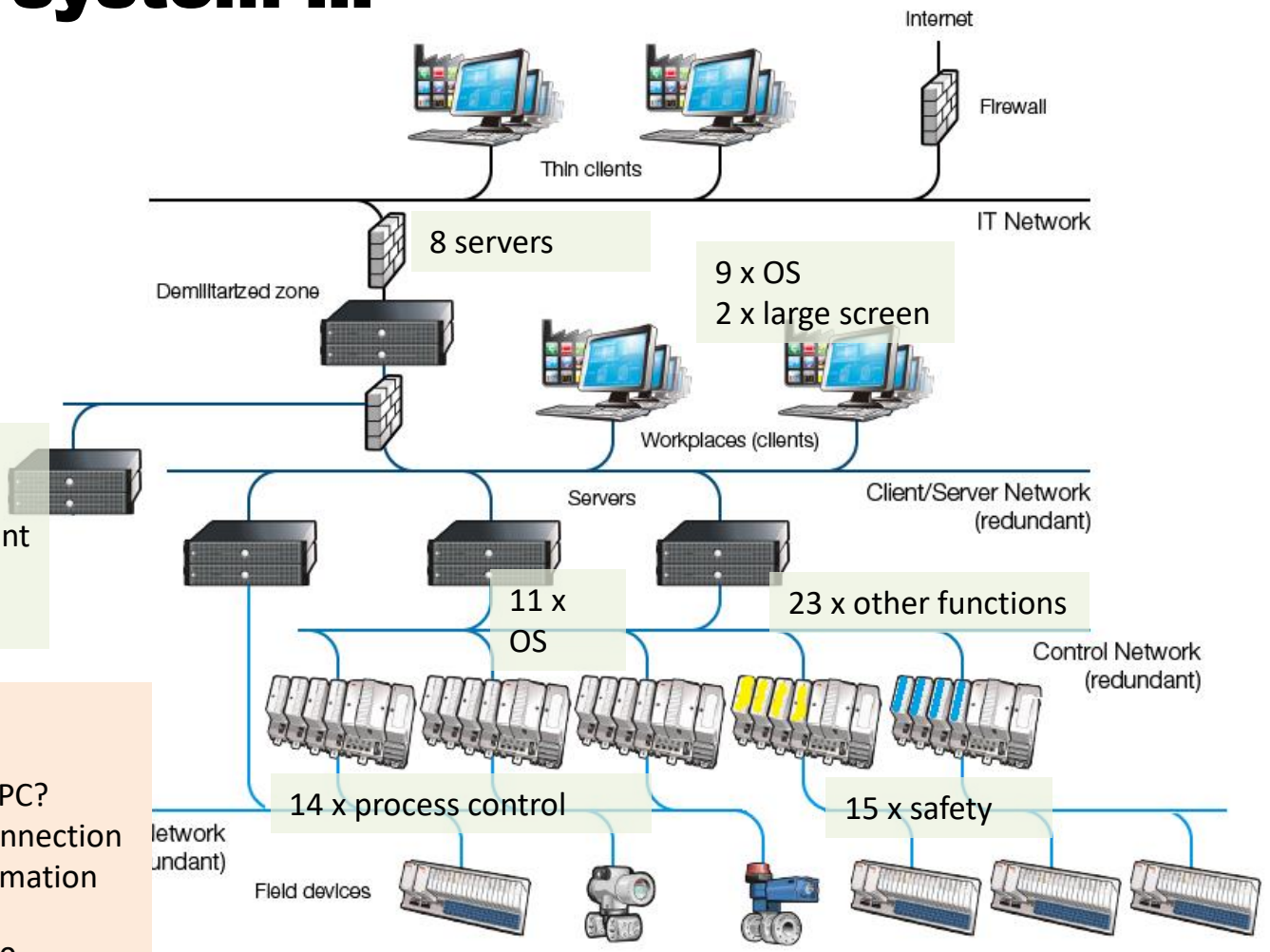
ICT architecture

- Segregation
- Controlled channels
- Industy standard



Challenge:
- Maintain architectural principle
- New data connections required

A platform system …



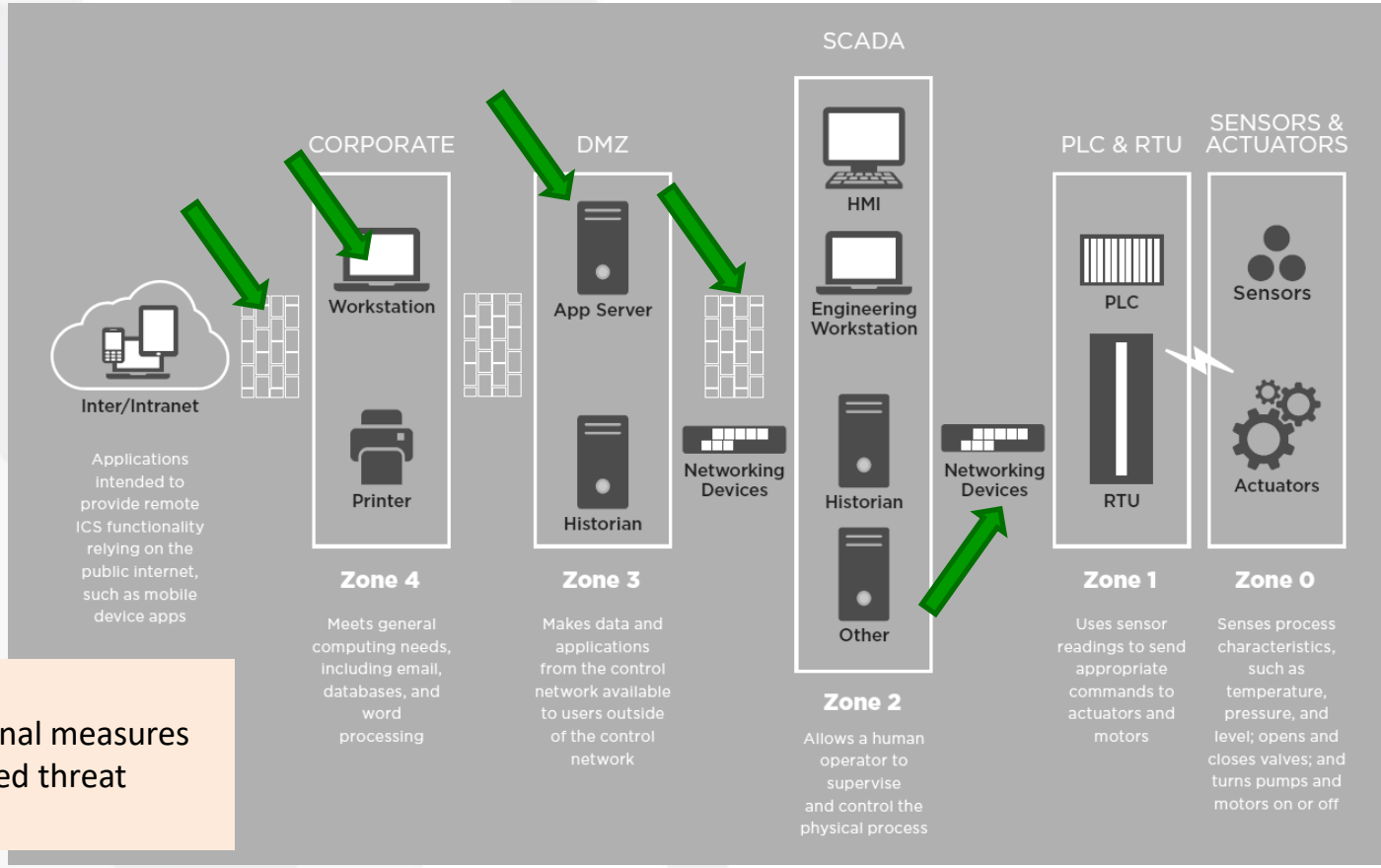
5 other systems
- Metering
- Power management
- Environment data
- …

Challenge:
- System support
  - Vendor w/PC?
  - Remote connection
- Additional information
  - IIoT
  - Industry 4.0

Figure based new.abb.com: 800xA Network Topologies - 800xA DCS (System 800xA)

Passive functions for protection

- Passwords
- Port blocking
- Management of network adresses
- Fire wall rules



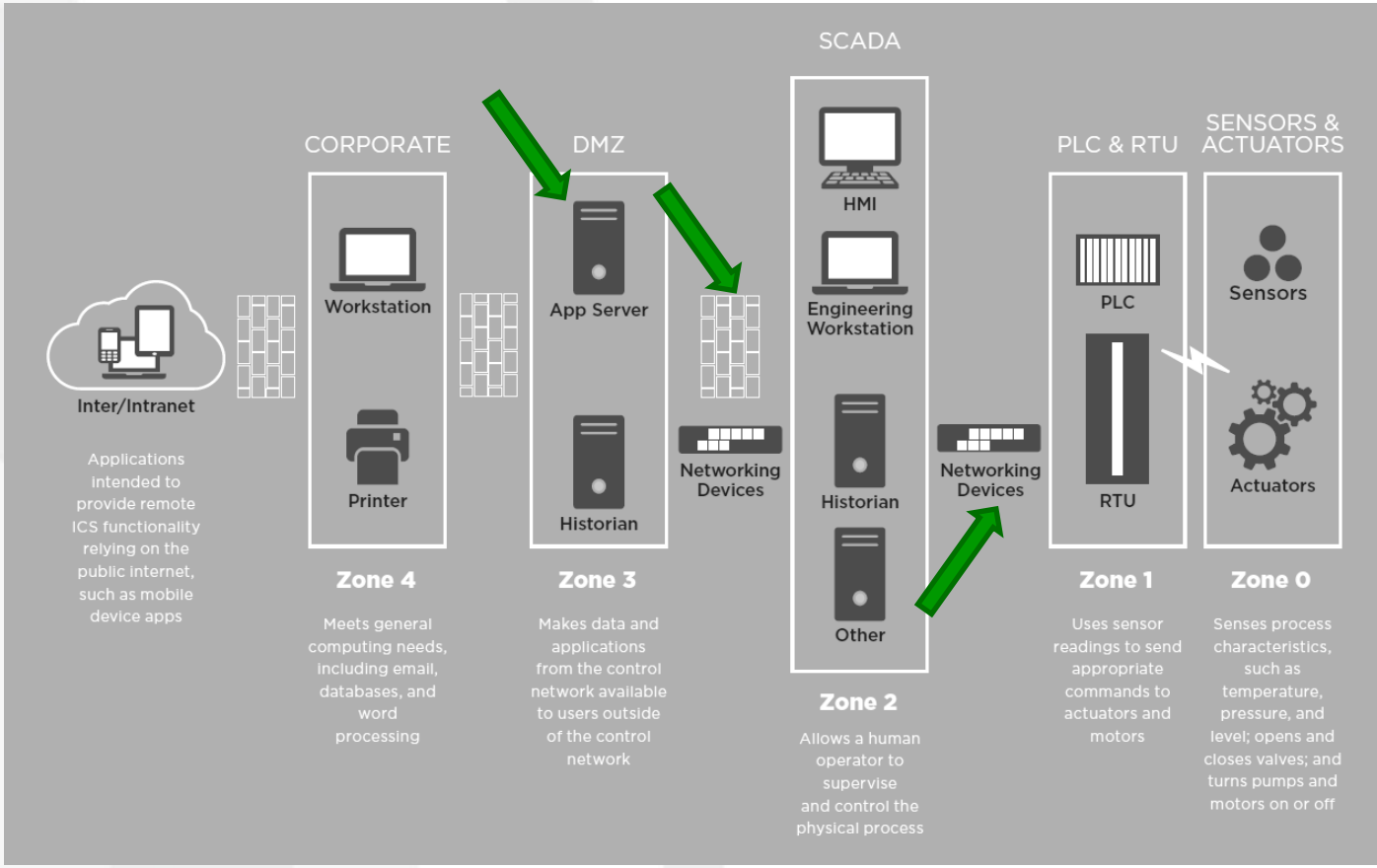
Challenge:

- Additional measures for raised threat level?

Monitoring, analysis & response

Challenges:

- How to detect anomalies without monitoring?
- Who will be able support you during an incident?
- People trained?



Activity against Critical Infrastructure

Alert (TA18-074A)

Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors

Since at least March 2016, Russian government cyber actors—hereafter referred to as "threat actors"—targeted government entities and multiple U.S. critical infrastructure sectors, including the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors.

https://www.us-cert.gov/ncas/alerts/TA18-074A

Technical Details

The threat actors in this campaign employed a variety of TTPs, including

- spear-phishing emails (from compromised legitimate account),
- watering-hole domains,
- credential gathering,
- open-source and network reconnaissance,
- host-based exploitation, and
- targeting industrial control system (ICS) infrastructure.

Incident reporting

PSA:

… situations where normal operation of control or security systems is disturbed by unplanned work (ICT event)

NIS Directive:

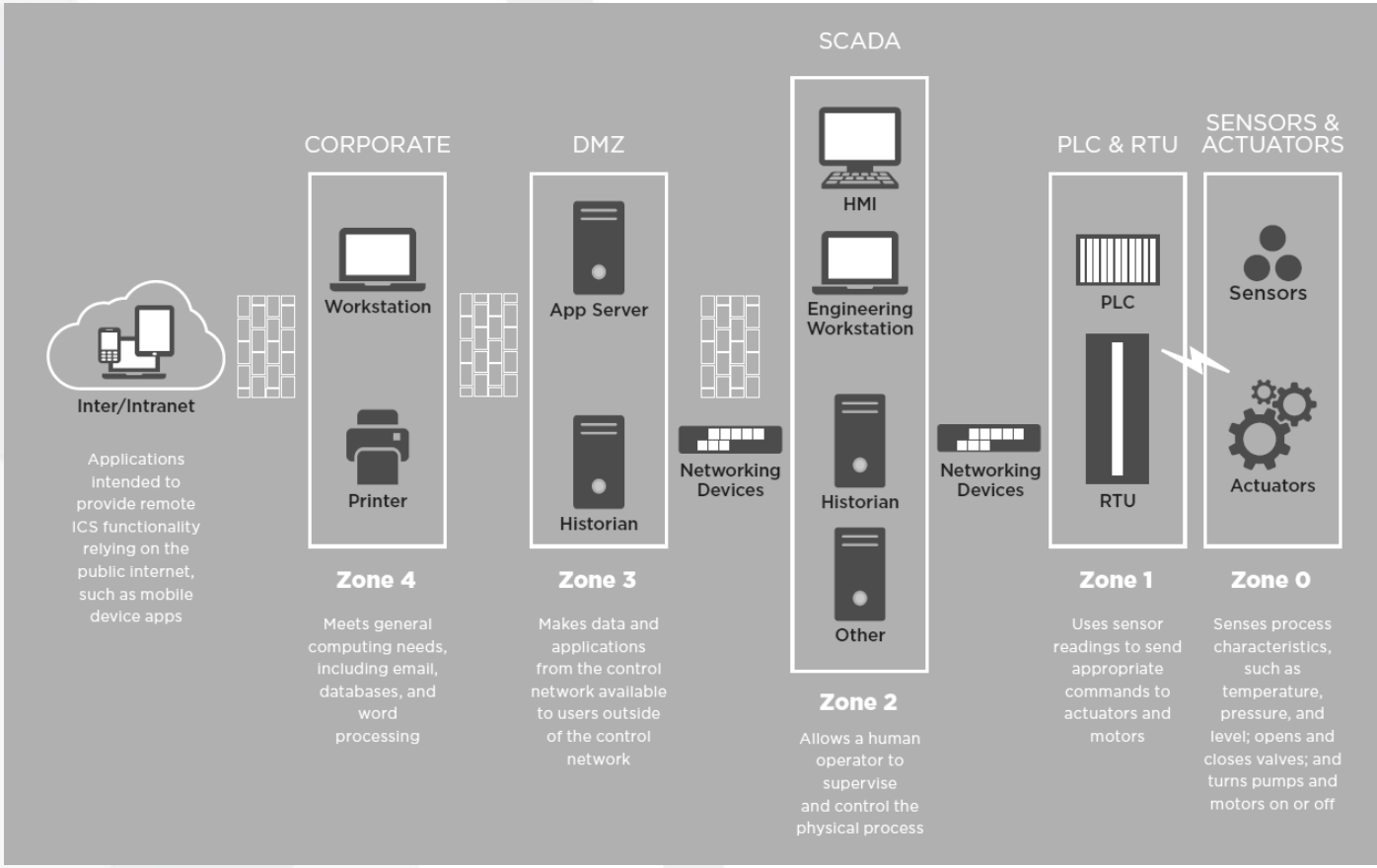
… incidents having a significant impact on the continuity of the essential services they provide

Norwegian Financial Supervision:

... as the enterprise itself categorizes to severity degree very seriously or critically

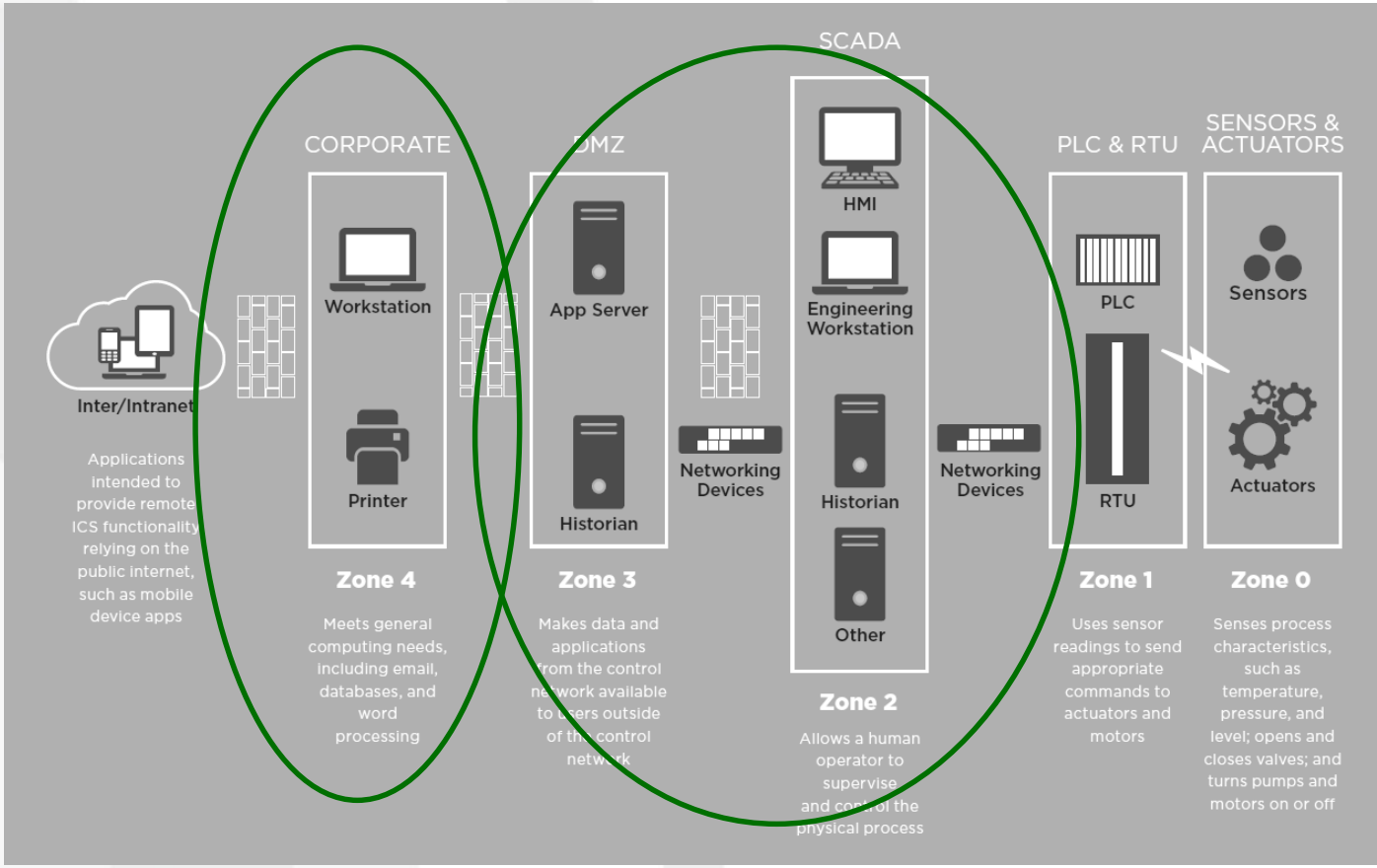
National Security Authority:

… are important for critical infrastructure or critical social functions



Internal audits and revisions

- IT audits versus OT audits
- Whom are responsible for IT equipment in the OT domain?



Audit – Cyber security

- Risk assessments
- ICT architecture and links to other systems
- Passive safeguards
- Monitoring, analysis and response
- Incident reporting
- Own audits and reviews

2 hour presentation from each

- operator
- ship owner

- Technical, organizational and operational questions


Follow us at: **www.psa.no**
PETROLEUM SAFETY AUTHORITY NORWAY

BACKUP SLIDES

PSA, ICT security and digitalisation

PSA have a wide range of activities to gain expertice about ICT security and HSE challenges within digitalisation

Collect information about ICT security and strategies for digitalisation

Identify competence within ICT security, HSE and risk

Monitor activities regarding ICT security and digitalisation

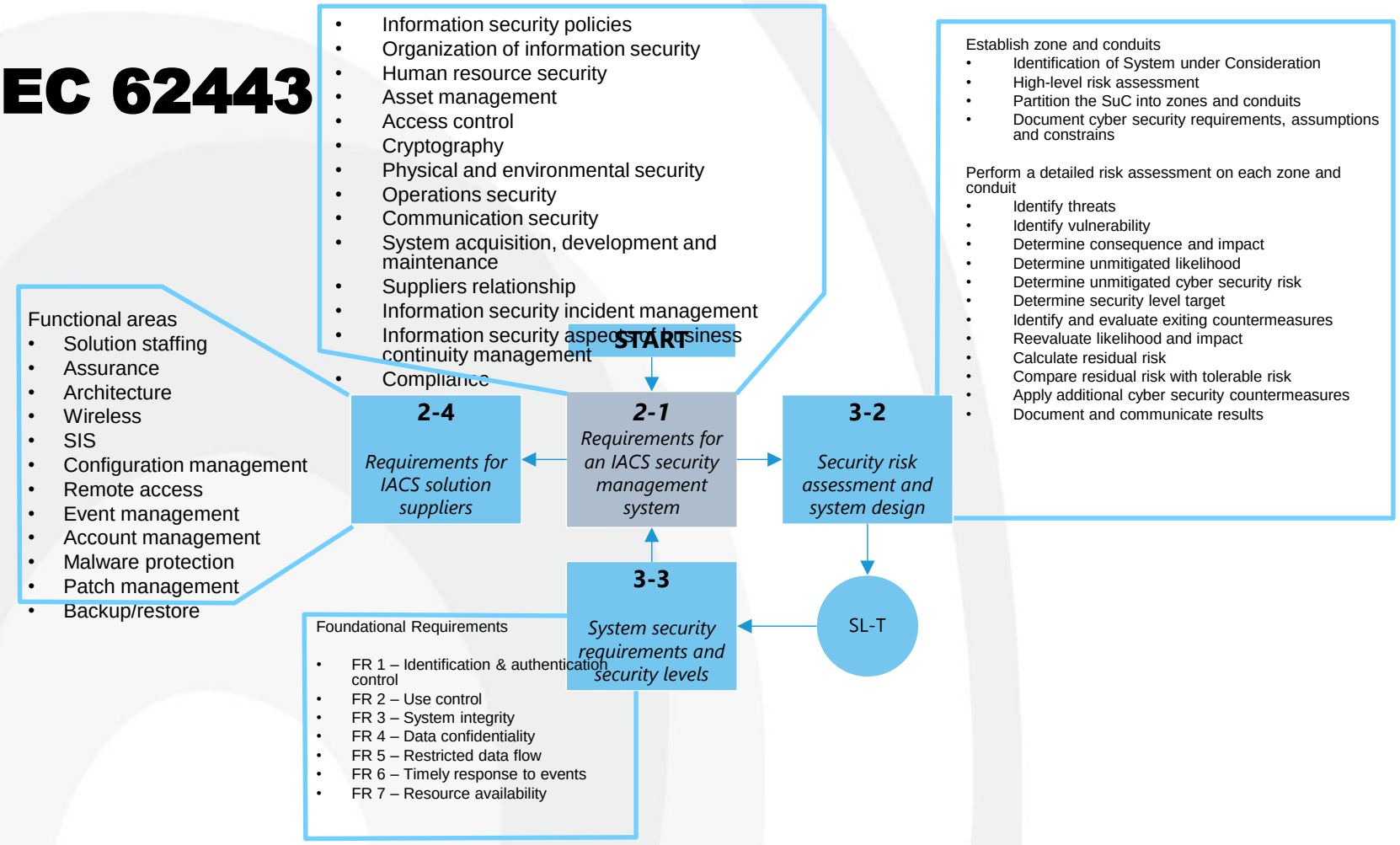
Participate in communities for ICT security and digitalisation

Establish overview of competency about HSE consequences of digitalisation in the petroleum industry

Support the three part cooperation regarding digitalisation

Further development of regulations and methods for audit

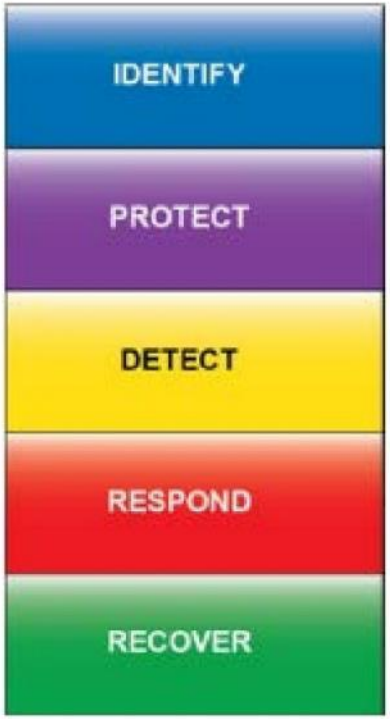
IEC 62443


Information security policies
Organization of information security
Human resource security
Asset management
Access control
Cryptography
Physical and environmental security
Operations security
Communication security
System acquisition, development and maintenance
Suppliers relationship
Information security incident management
Information security aspects of business continuity management
Compliance
Functional areas
Solution staffing
Assurance
Architecture
Wireless
SIS
Configuration management
Remote access
Event management
Account management
Malware protection
Patch management
Backup/restore
START
2-4
Requirements for IACS solution suppliers
2-1
Requirements for an IACS security management system
3-2
Security risk assessment and system design
3-3
System security requirements and security levels
SL-T
Foundational Requirements
FR 1 – Identification & authentication control
FR 2 – Use control
FR 3 – System integrity
FR 4 – Data confidentiality
FR 5 – Restricted data flow
FR 6 – Timely response to events
FR 7 – Resource availability
Establish zone and conduits
Identification of System under Consideration
High-level risk assessment
Partition the SuC into zones and conduits
Document cyber security requirements, assumptions and constrains
Perform a detailed risk assessment on each zone and conduit
Identify threats
Identify vulnerability
Determine consequence and impact
Determine unmitigated likelihood
Determine unmitigated cyber security risk
Determine security level target
Identify and evaluate exiting countermeasures
Reevaluate likelihood and impact
Calculate residual risk
Compare residual risk with tolerable risk
Apply additional cyber security countermeasures
Document and communicate results

NIST

CSF – 5 Functions

- **Identify**
  - Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities
- **Protect**
  - Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- **Detect**
  - Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond**
  - Develop and implement the appropriate activities to take action regarding a detected cyber security event.
- **Recover**
  - Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event



IPDR2

5-22-98