

# What works in securing control systems

Helle Stoltz

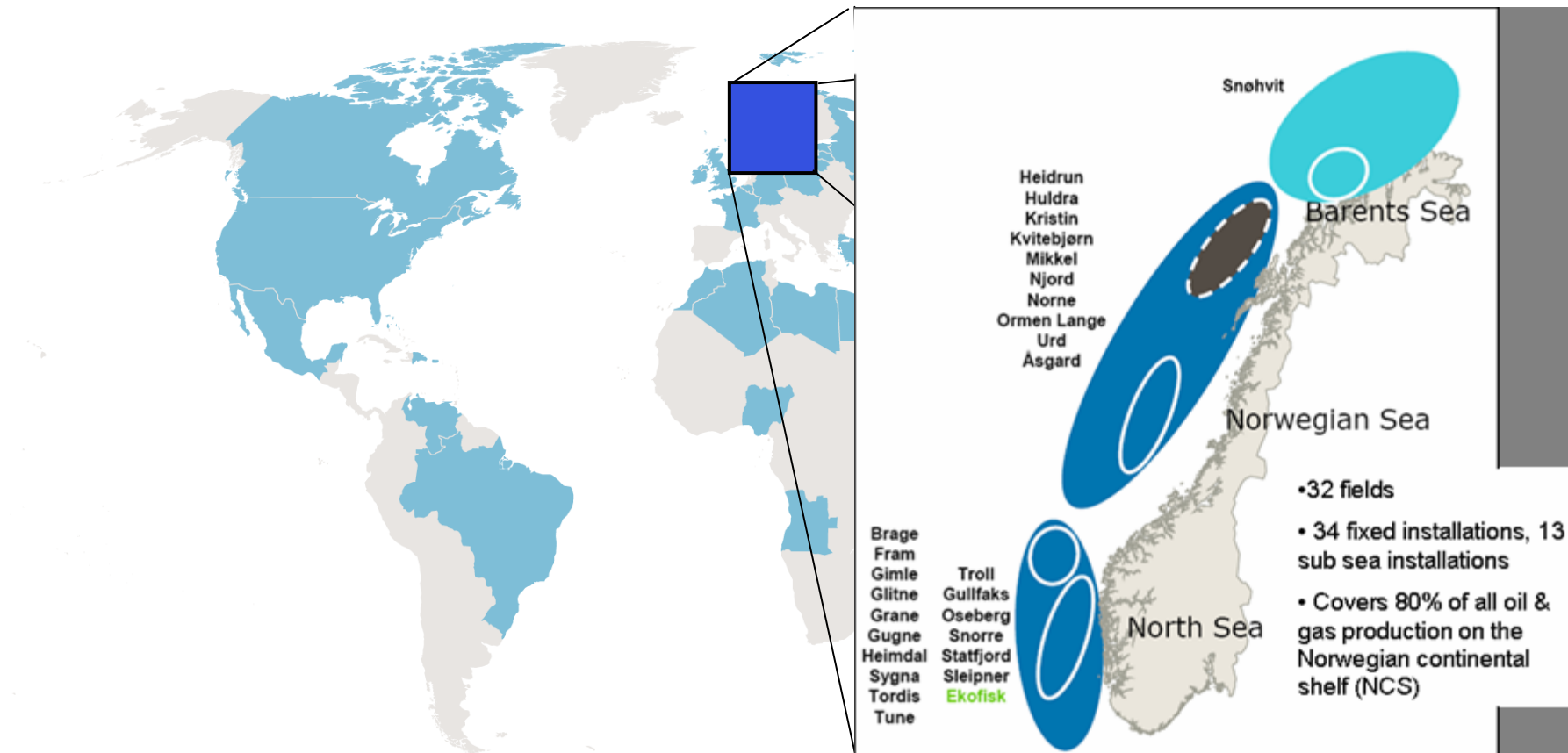
Leading Advisor Automation – Information Systems and Security

StatoilHydro



## This is StatoilHydro

- An international integrated energy company based in Norway
- The world's largest deepwater operator and the world's third largest net seller of crude oil
- Equity production of 1.7 million barrels of oil equivalent per day and more than 6 billion boe in proven reserves
- About 29,500 employees in 40 countries



More than 31.000 employees in 40 countries

# Characteristics of plant technical systems

- Frequent plant system modifications, concurrently
- 2-4 shift personnel responsible for maintenance
- Integrated operations (IO / e-Fields / Smart Fields)
  - Real time information to be made available
  - “Remote maintenance”
  - Remote control?

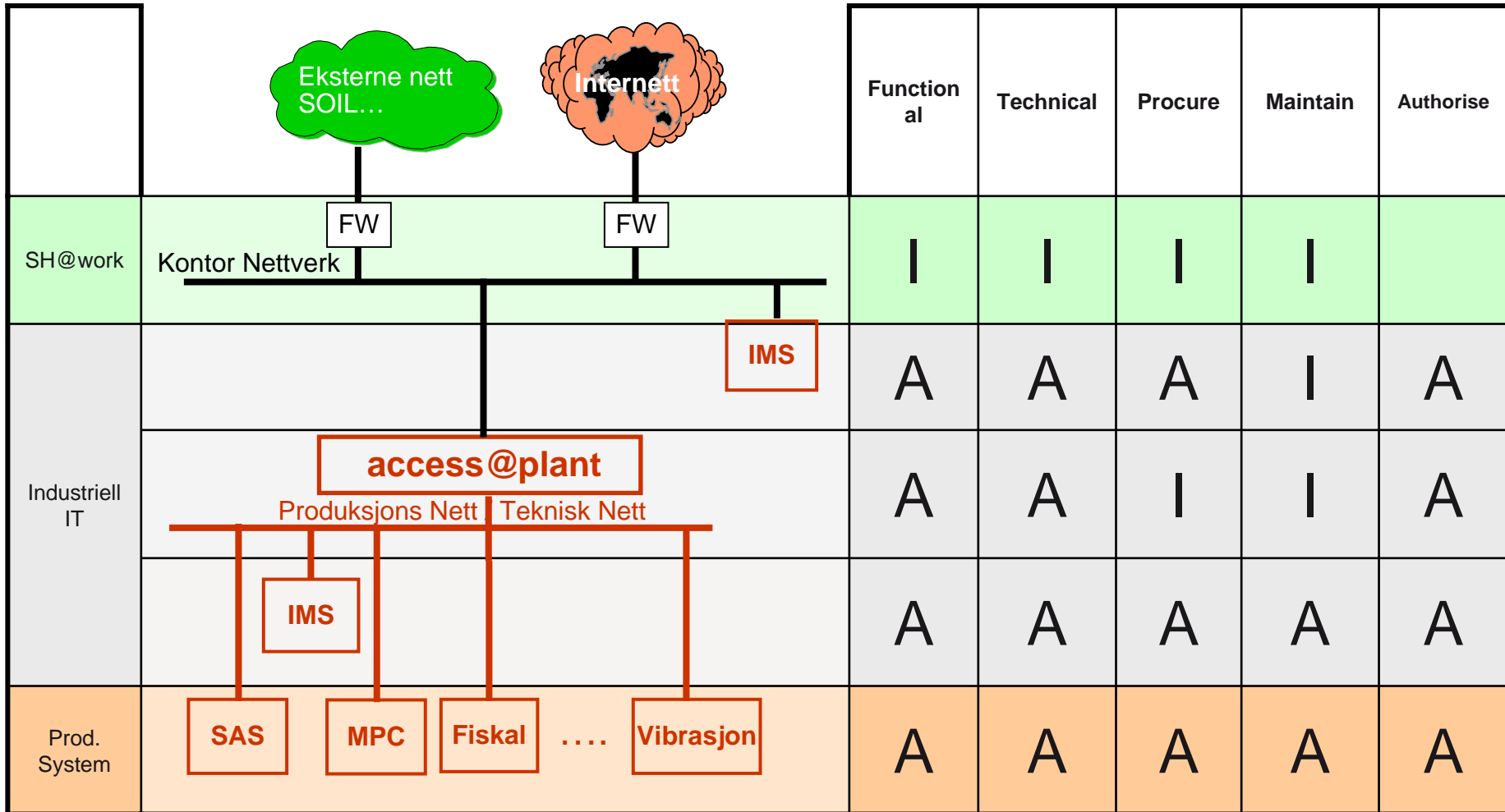


## Characteristics (cont.)

- Converging technology, more use of “standard IT”
  - Several generations IT technology on the same network
  - IT components have longer life time than in office use
- Process control increasingly connected to business network
  - Cyber attack possible
  - Protocols and libraries available online
- Process control and safety systems require high availability and real-time performance.



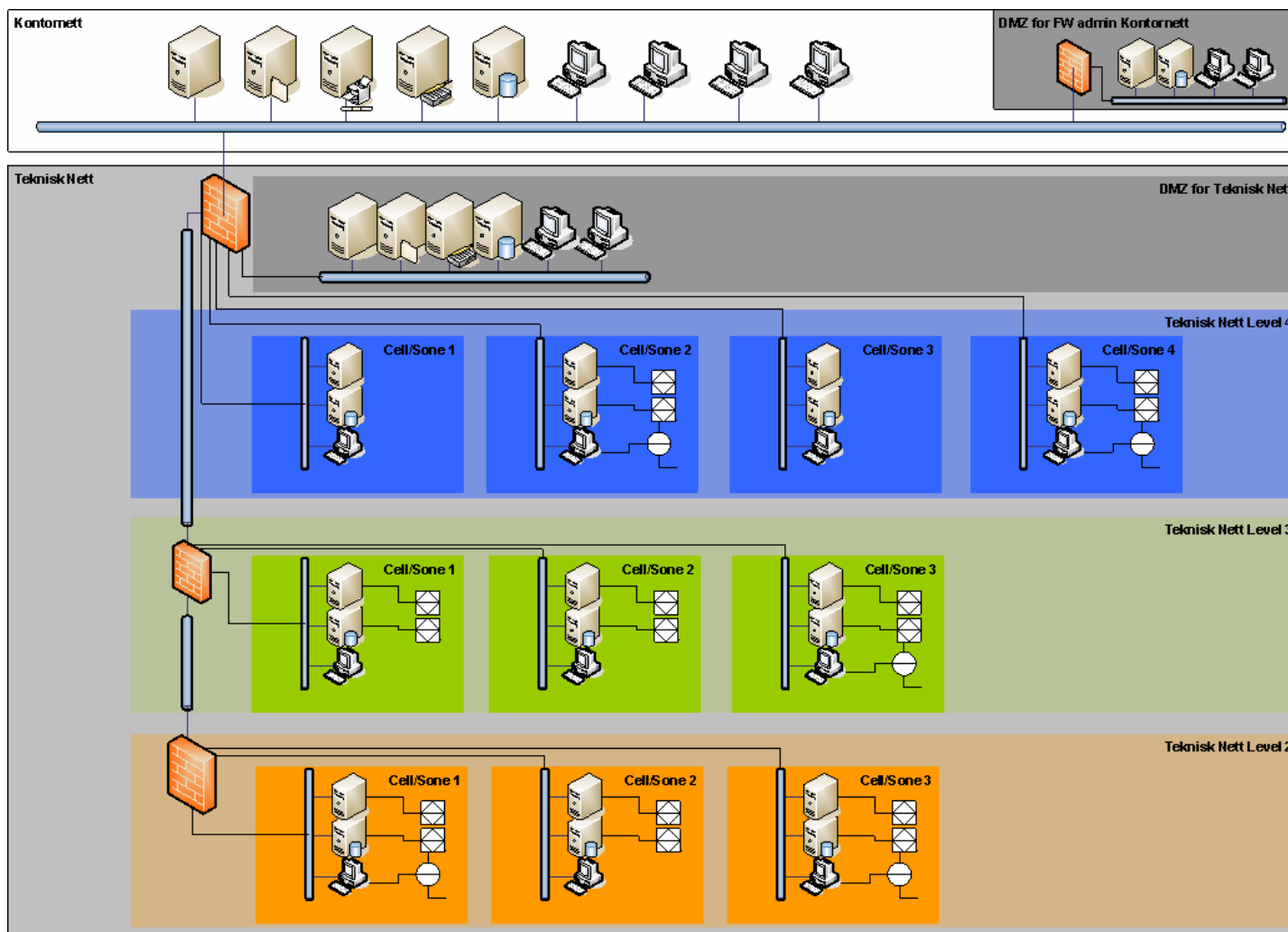
# Automation / IT responsibility sharing



## OLF guideline 104 (The Norwegian Oil Industry Association)

- 1. An Information Security Policy for process control, safety, and support ICT systems environments shall be documented.
- 2. Risk assessments shall be performed for process control, safety, and support ICT systems and networks.
- 3. Process control, safety, and support ICT systems shall have designated system and data owners.
- **4. Infrastructure shall be able to provide segregated networks, and all communication paths shall be controlled.**
- 5. Users of process control, safety, and support ICT systems shall be educated in the information security requirements and acceptable use of the ICT systems.
- 6. Process control, safety, and support ICT systems shall be used for designated purposes only.
- **7. Disaster recovery plans shall be documented and tested for critical process control, safety, and support ICT systems.**
- 8. Information security requirements for ICT components shall be integrated in the engineering, procurement, and commissioning processes.

# Technical Network discussion



Information and  
monitoring  
systems

PCS

SIS



## OLF guideline (cont.)

- 9. Critical process control, safety, and support ICT systems shall have defined and documented service and support levels.
- **10. Change management and work permit procedures shall be followed for all connections to and changes in the process control, safety, and support ICT systems and networks.**
- **11. An updated network topology diagram including all system components and interfaces to other systems shall be available.**
- **12. ICT systems shall be kept updated and patched when connected to process control, safety, and support networks.**
- **13. Process control, safety, and support ICT systems shall have adequate, updated, and active protection against malicious software.**
- 14. All access rights shall be denied unless explicitly granted.
- 15. Required operational and maintenance procedures shall be documented and kept current.
- 16. Procedures for reporting of security events and incidents shall be documented and implemented in the organisation.