NTNU | Kunnskap for en bedre verden

How may cybersecurity impact the design of safety instrumented systems?

SFI NORCICS conference 21.11.2024

Professor Mary Ann Lundteigen| Department of Engineering Cybernetics, NTNU

About me

- Professor at Engineering Cybernetics department
- Master in Engineering Cybernetics, PhD in safety and reliability
- Focus:
  - Instrumentation systems, including industry 4.0
  - Safety-instrumented systems and functional safety
  - Cybersecurity of operational technology (OT) systems
- Mix of industrial and academic experience

https://innsida.ntnu.no/my-profile/

Role in SFI NORCICS:
Part of supervisor team for new 2-years postdoc (researcher) on cybersecurity and safety-instrumented systems (SIS).

Content of presentation

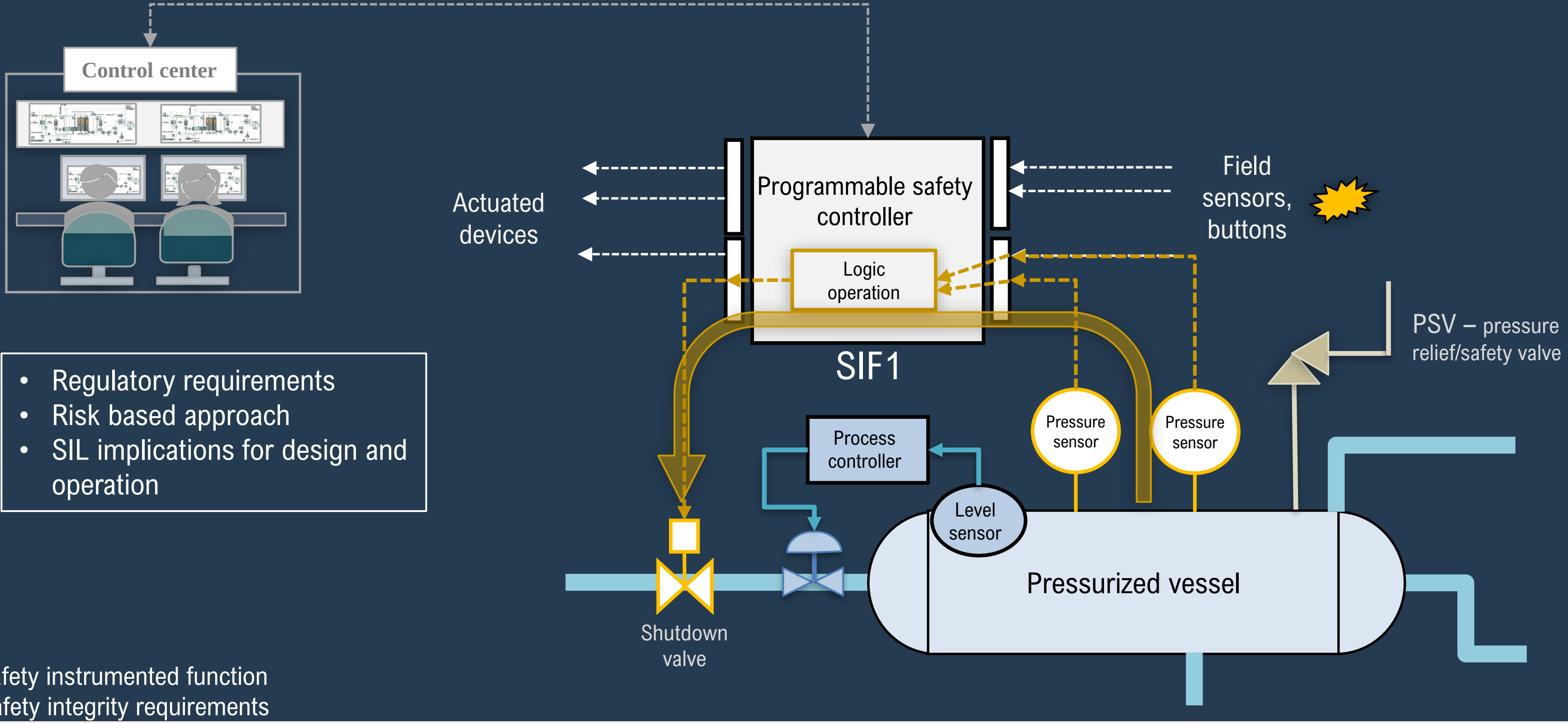
Safety instrumented systems

Cybersecurity vs safety

Impacts of attacks

About managing both

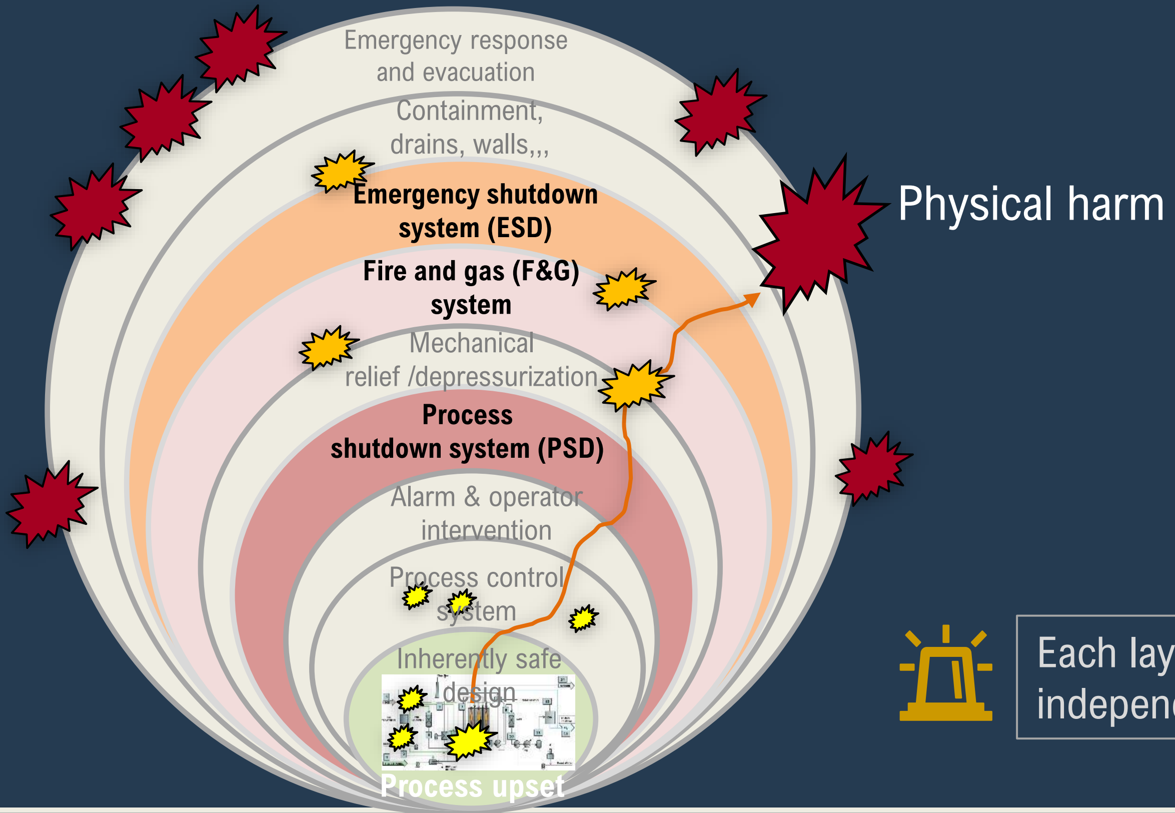
Safety instrumented system (SIS)



- Regulatory requirements
- Risk based approach
- SIL implications for design and operation

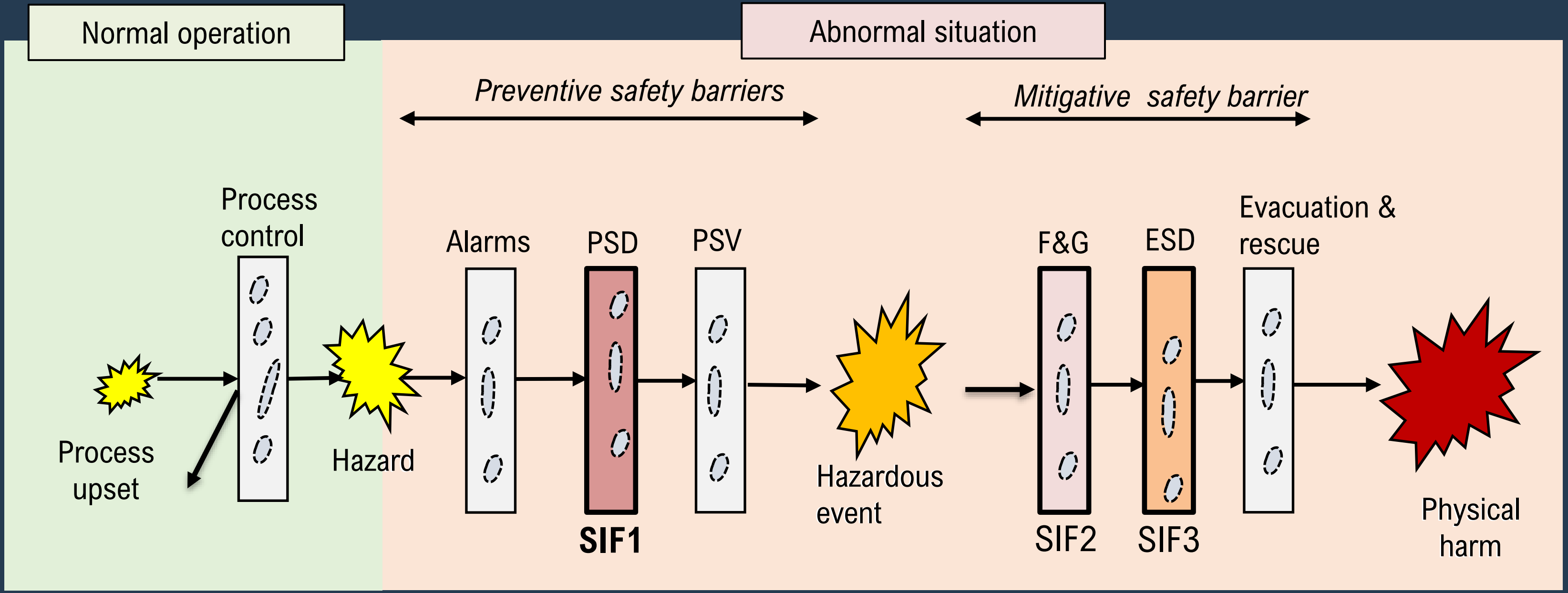
SIF: Safety instrumented function
SIL: Safety integrity requirements

SIS contribution to layers of protection


Emergency response and evacuation
Containment, drains, walls,,,
Emergency shutdown system (ESD)
Fire and gas (F&G) system
Mechanical relief /depressurization
Process shutdown system (PSD)
Alarm & operator intervention
Process control system
Inherently safe design
Process upset
Physical harm

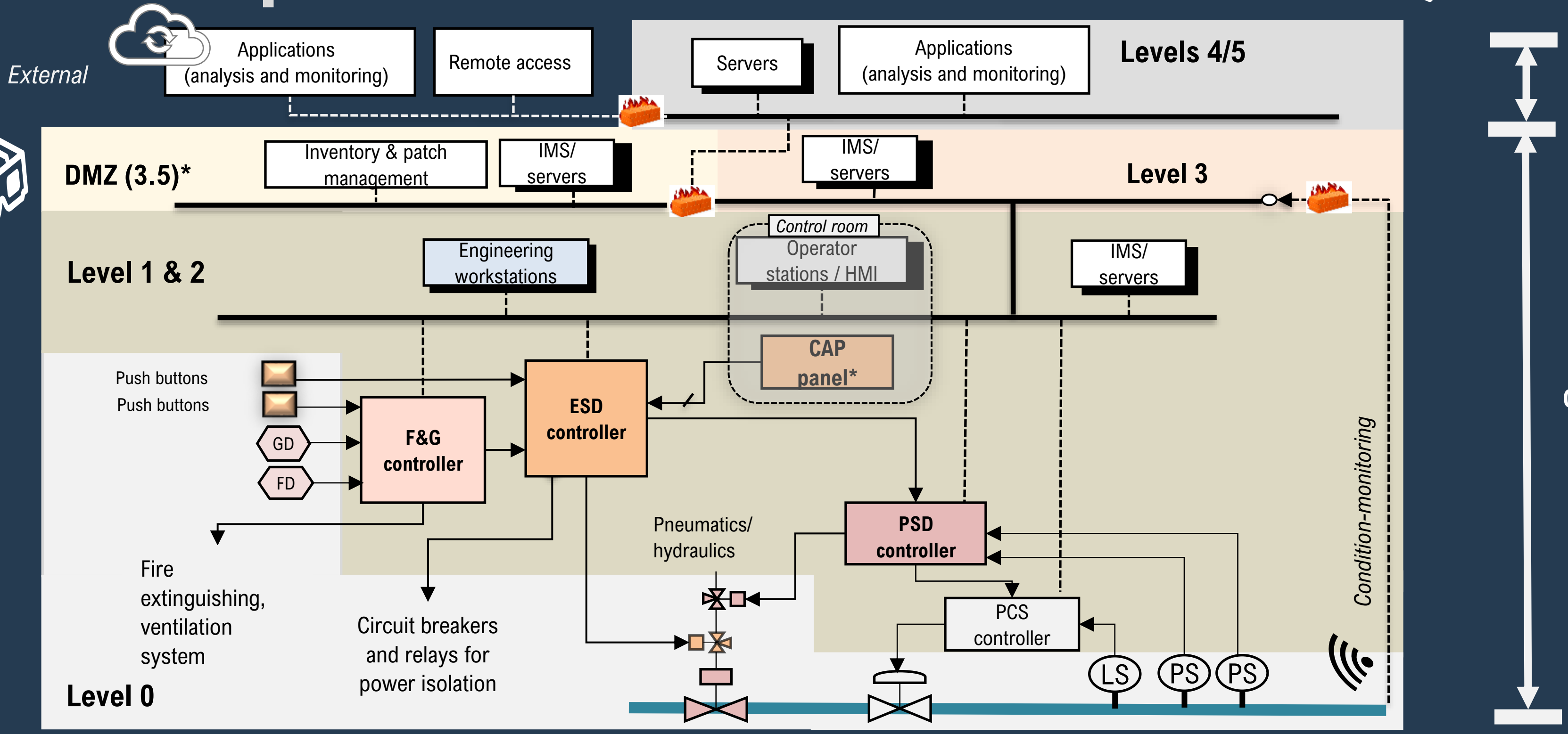
Each layer (or barrier) MUST be independent er to be effective!

Safety barriers: Specific roles of protection layers



SIS: Safety instrumented system. ESD: Emergency shutdown, PSD: Process shutdown, PCS: Process control system. F&G: Fire and gas system. PSV: Pressure safety (relief) valve

SIS as part of network architecture

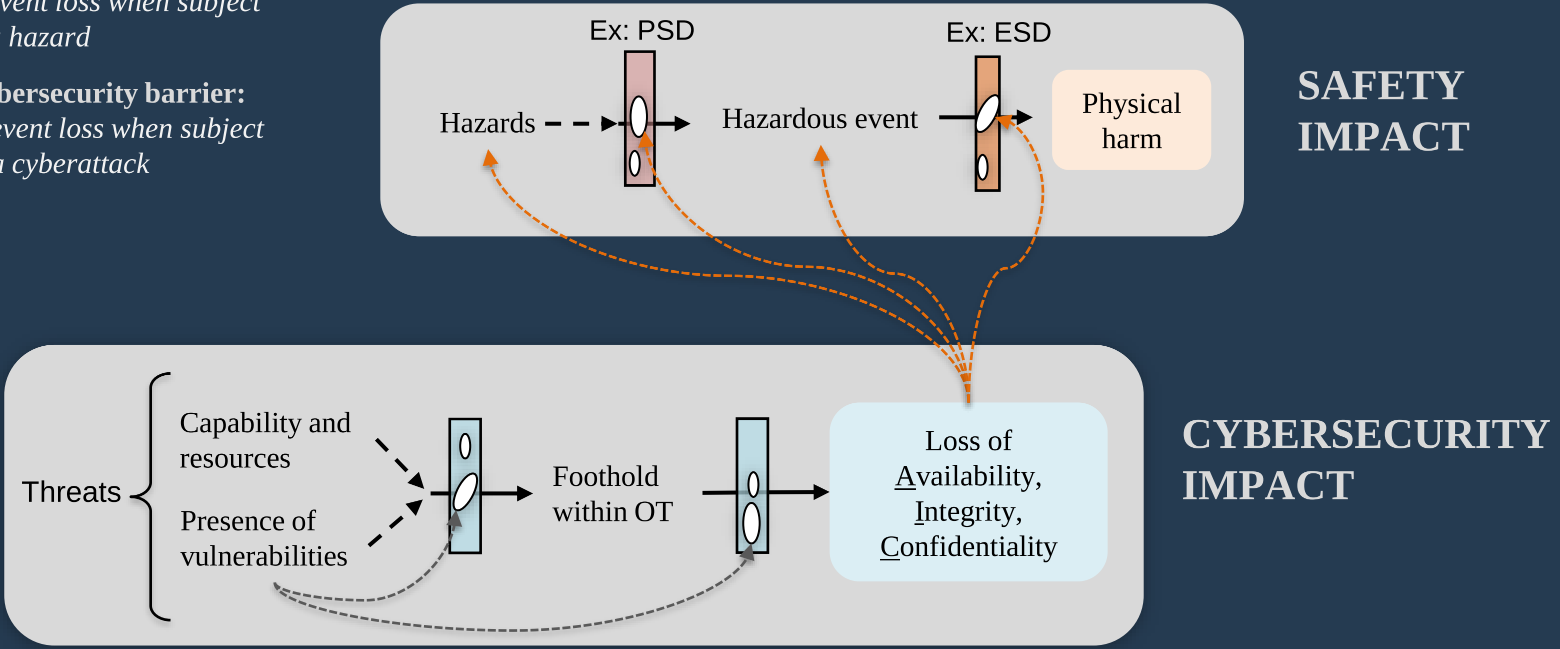


OT: Operational technology. ESD: Emergency shutdown, PSD: Process shutdown, PCS: Process control system. CAP: Critical action panel (*Offshore facilities only)
LS: Level sensor. PS: Pressure sensor. GD: Gas detector. FD: Fire detector. IMS: Information management system.

Cybersecurity impact on safety

🟫 **Safety barrier:** *Prevent loss when subject to a hazard*

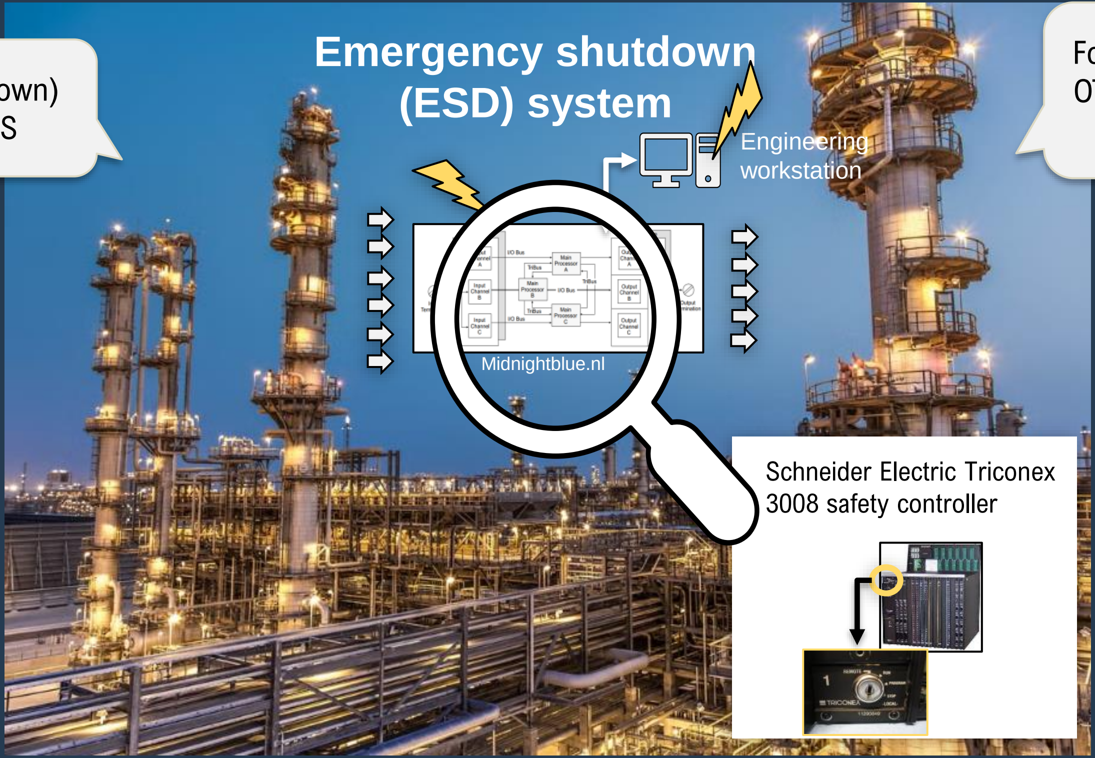
🟦 **Cybersecurity barrier:** *Prevent loss when subject to a cyberattack*



ESD: Emergency shutdown, PSD: Process shutdown

Example: Attack on SIS in Saudi-Arabia (2017)

First (publicly known) attack on a SIS


Emergency shutdown (ESD) system

Engineering workstation

Midnightblue.nl

Schneider Electric Triconex 3008 safety controller

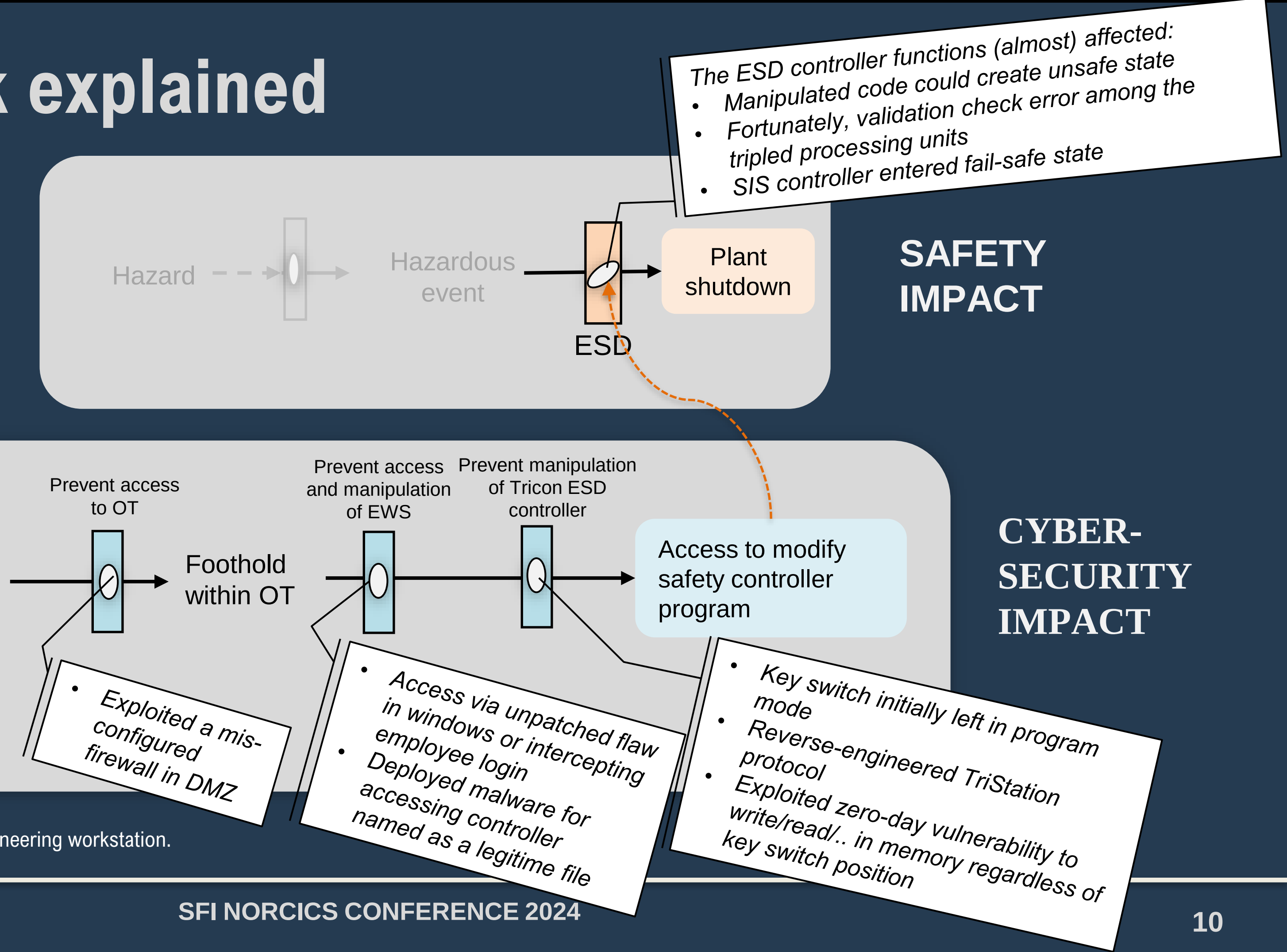
Foothold inside OT for a longer period

TRISIS
TRITON
HATMAN

SIS: Safety instrumented system. ESD: Emergency shutdown

The attack explained

- Capabilities and motivation of TsNIIKhM
- Triton* malware: remote access Trojan
- Zero-day in Triconex safety controller firmware


Hazard
Hazardous event
ESD
Plant shutdown
SAFETY IMPACT
Prevent access to OT
Foothold within OT
Prevent access and manipulation of EWS
Prevent manipulation of Tricon ESD controller
Access to modify safety controller program
CYBER-SECURITY IMPACT

The ESD controller functions (almost) affected:

- *Manipulated code could create unsafe state*
- *Fortunately, validation check error among the tripled processing units*
- *SIS controller entered fail-safe state*

- Exploited a mis-configured firewall in DMZ

- Access via unpatched flaw in windows or intercepting employee login
- Deployed malware for accessing controller named as a legitime file

- Key switch initially left in program mode
- Reverse-engineered TriStation protocol
- Exploited zero-day vulnerability to write/read/.. in memory regardless of key switch position

ESD: Emergency shutdown system. EWS: Engineering workstation.
DMZ: Demilitarized zone (layer 3.5)

Standards framing SIS and cybersecurity

Functional safety

- **IEC 61508** – generic (2010)
- **IEC 61511** – process industry (2016)
- **IEC 62061/ ISO 13849** – Machinery
- ….
- Offshore Norge GL 070 – petroleum (2024)

Framing SIS design and operation

Functional safety & cyber security

- IEC **TS** 63069 – generic (2019)
- ISA **TR** 84.00.09 – process industry (2017)
- IEC **TR** 63074 – machinery (2023)

Related:

- Cyber-informed engineering

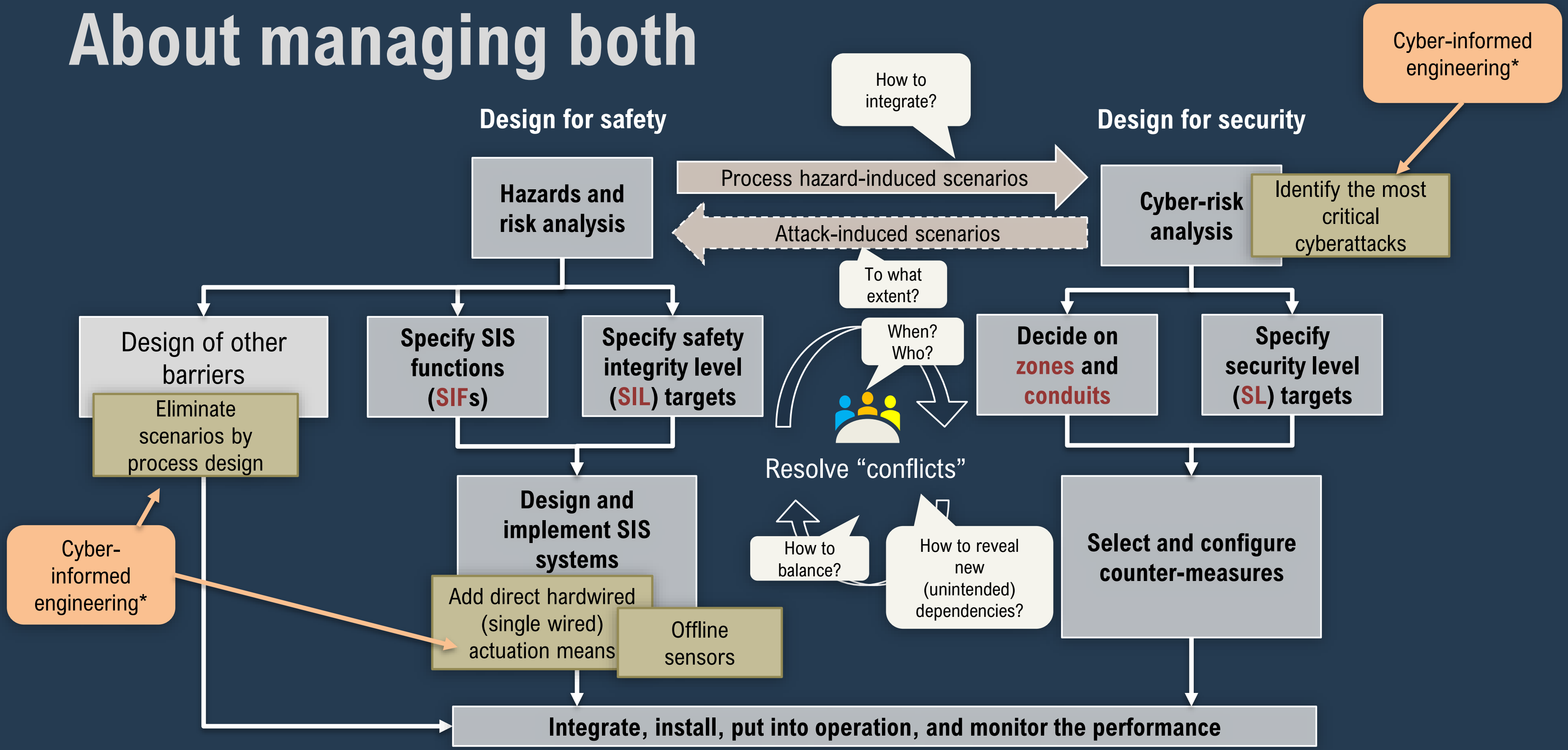
Initiatives to manage both

Cybersecurity

- **IEC 62443** OT cybersecurity (201x/202x)
- DNV GL G108 – use of IEC 62443 (2020)
- NIST Cybersecurity framework (2024)
- NIST SP 800-82 OT cybersecurity guideline (2023)
- Offshore Norge GL 114 (2014)

Framing OT cybersecurity

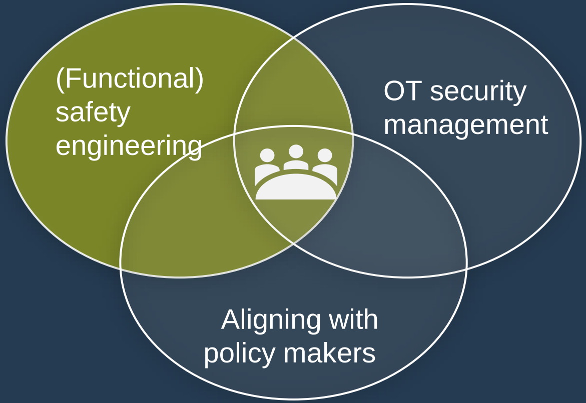
About managing both


Cyber-informed engineering*
Design for safety
How to integrate?
Design for security
Hazards and risk analysis
Process hazard-induced scenarios
Attack-induced scenarios
Cyber-risk analysis
Identify the most critical cyberattacks
To what extent?
Design of other barriers
Eliminate scenarios by process design
Specify SIS functions (SIFs)
Specify safety integrity level (SIL) targets
When? Who?
Decide on zones and conduits
Specify security level (SL) targets
Resolve "conflicts"
Cyber-informed engineering*
Design and implement SIS systems
Add direct hardwired (single wired) actuation means
Offline sensors
How to balance?
How to reveal new (unintended) dependencies?
Select and configure counter-measures
Integrate, install, put into operation, and monitor the performance

*Example: Consequence-driven cyber-informed Engineering (CCE^{TM}).

SFI NORCICS is recruiting now!

2-year full-time Postdoc position on **Cybersecurity of safety-instrumented systems (SIS)**



Supervision team NTNU: Sokratis Katsikas, Vasileios Gkioulos, Mary Ann Lundteigen

Research topics:

- **SIS attack scenarios:** Identification of new and learning from the past
- **Understand SIS vulnerabilities:** Existing commercial systems and new smart instrumentation and IIoT
- **Compare practices and identify gaps:** With basis in current standards and guidelines
- **Provide new contributions:** To existing frameworks and as new guideline

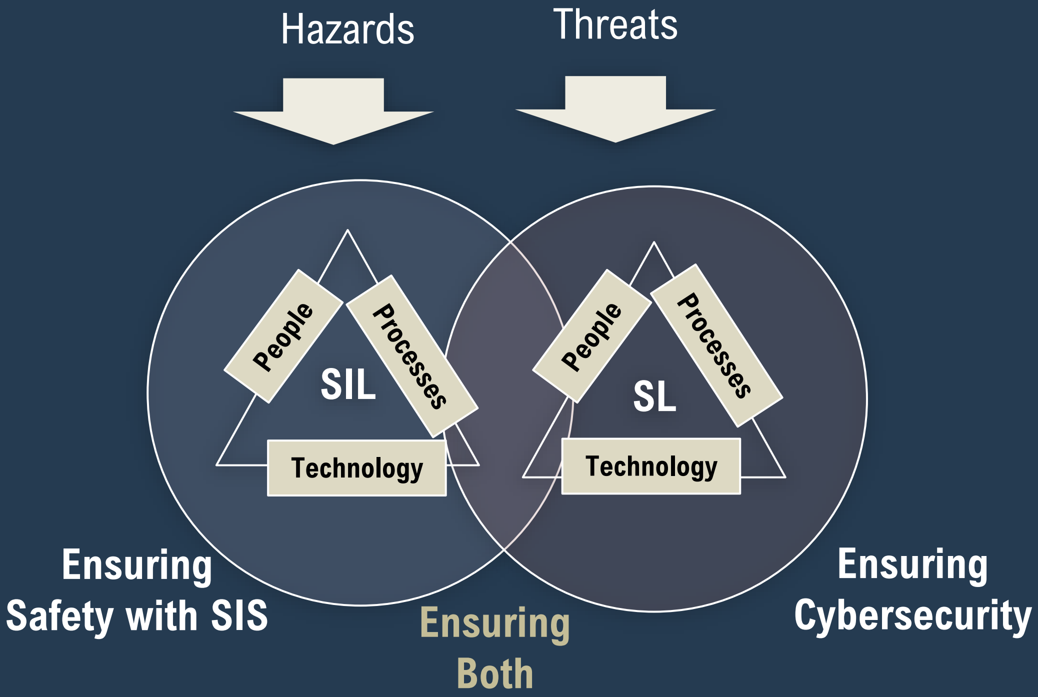
Partners involved in the project: **Yara, Hydro, Equinor**

Thank you for the attention! Any questions?

Selected references (beyond standards):

- Makrakis, G. M. et al (2021). Industrial and Critical Infrastructure Security: Technical Analysis of Real-Life Security Incidents. IEEE Access.
- Guzman, N., Kozine, I., Lundteigen, M.A. (2021) An integrated safety and security analysis for cyber-physical harm scenarios. Safety Science.
- Cyber-informed engineering: https://inl.gov/national-security/cie/
- Publications through the CDS forum, including cyberbarrier management project, see https://cds-forum.com/

https://innsida.ntnu.no/my-profile/



SIL: Safety integrity level. SL: Security level