HFC - 17.10.2023

The operator's role in cybersecurity

Prevention, detection and response

Espen Nystad
Senior research scientist

Critical infrastructure

Security property	Consequence if breeched
Confidentiality	Unauthorized access to plant information / plant data
Integrity	Inaccurate plant data
Availability	Loss of access to plant systems or data

Cyberattacks towards nuclear organizations

Organization	Year	Attack vector	Consequence
Kudankulam NPP	2019	Personal computer	Espionage
Gudremmingen NPP	2016	USB	Data leak
University of Toyama	2015	Phishing	Data leak
Nuclear Regulatory Commission	2015	Insider threat	No consequence
Monju NPP	2014	Third-party software	Data leak
KHNP	2014	Phishing	Data leak
Iranian Nuclear program	2012	USB	Espionage
Oak Ridge National Laboratory	2011	Phishing	Data leak

Organization	Year	Attack vector	Consequence
Areva	2011	Unknown	Espionage
Iranian Nuclear program	2011	Phishing	Espionage
Natanz uranium plant	2010	USB	Sabotage
Energy Future Holdings	2009	Insider threat	Data leak
Syrian Nuclear Program	2006	Access to digital media	Espionage
Japanese NPP	2005	Personal computer	Data leak
Davis-Besse NPP	2003	Personal computer	Loss of availability
Bradwell NPP	1999	Insider threat	Sabotage
Ignalina NPP	1992	Insider threat	No consequence

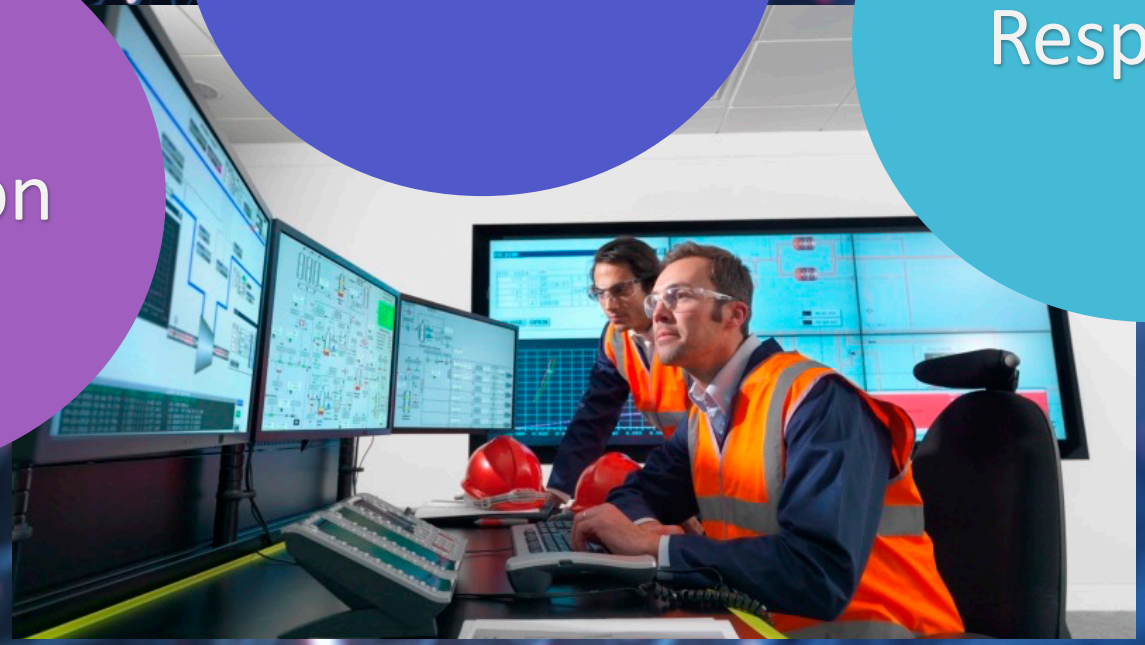
Attack vectors	
Phishing	4
Insider threat	4
USB	3
Personal computer	3
Access to digital media	1
Third-party software	1
Unknown	1

Consequences	
Data leak	7
Espionage	5
Sabotage	2
No consequence	2
Loss of availability	1

Prevention

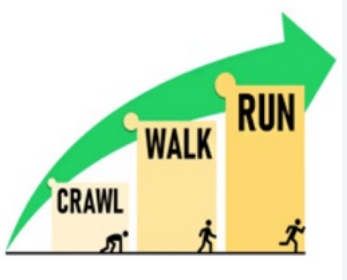
Detection

Response



1 Prevention of cyber-attacks

Cybersecurity training in Norwegian critical infrastructure companies



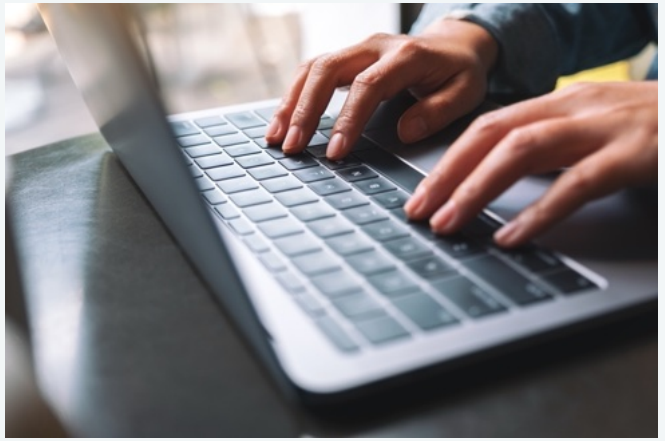
Maturity indicator levels	develop CS workforce	increase CS awareness
MIL3	i) Continuing training opportunities h) Effectiveness regularly evaluated & improvements made g) Training program aligned with Workforce Management objectives f) Recruitment / retention aligned with WM objectives e) CS WM objectives established	e) Effectiveness regularly evaluated & improvements made d) Aligned with states of operation
MIL2	d) Training as prerequisite to access c) Gaps addressed in training b) CS gaps identified	c) CS awareness content based on threat profile b) CS awareness activities established and maintained
MIL1	a) CS training made available	a) CS awareness activities occur

Mostly fulfilled
Partly fulfilled
Not defined

Nabin Cowdhury, Espen Nystad, Kine Reegård (2022). Cybersecurity Training in Norwegian Critical Infrastructure Companies.

Cybersecurity training in Norwegian critical infrastructure companies

- Training focused on basic cybersecurity competence and awareness
- All respondents saw a need for further improvement of cybersecurity competence
- Staff in urgent need of further cybersecurity competence improvement:
  1. General staff and Management
  2. IT personnel
  3. Operative personnel
- Lacking: Keep updated view of threat landscape -> Update content accordingly



Cybersecurity training – insights from NPP operators

- Interviews with 20 operators and operational managers
- 4 crews
- US and Sweden
- Analogue control rooms with some digital systems

General training	• Password protection • Recognizing malicious emails, phishing campaigns • Use of USB sticks and portable devices	All 4 crews
Role-specific training	• **Recognize cyber issues in plant equipment** • **Separation of plant equipment network and business network** • **Keylogging** • **Cyber incidents experienced at other plants**	2 crews
	• **Recognize malware: Unexpected mouse movements or changes on screen**	1 crew

2 Detection of cyber-attacks

Cybersecurity awareness in air traffic control

- Air traffic control systems have known vulnerabilities, e.g. may lack means for authentication or encryption.
- Vulnerabilities have been identified in:
  - Communication systems (VHF, Controller Pilot Data Link Communications systems)
  - Radar / surveillance systems (Secondary Surveillance Radar, Automatic Dependent Surveillance systems)
- Possible to produce false or altered data, a false picture of the airspace
- Probability of hackers gaining access to the operational systems is seen as low
  → Operators are usually not trained on such scenarios

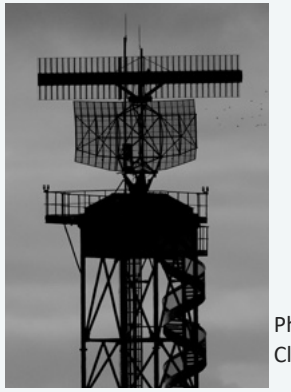
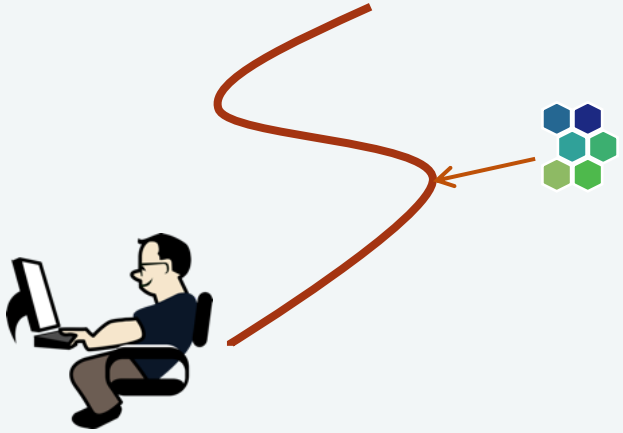


Photo:
Clint Budd



- Study of 'Operative cybersecurity awareness' in ATCOs
  - 5 licensed ATCOs from Avinor
  - Online Table-top exercise of ATM cyber scenarios
- Research questions:
  - Are ATCOs able to detect a cyber intrusion in the operative systems?
  - Are ATCOs' response to a technical incident different from the response to a cyber incident?

Espen Nystad, John Eidar Simensen, Christian Raspotnig (2022). Investigating operative cybersecurity awareness in air traffic control.

Scenario 1 – training/warm up

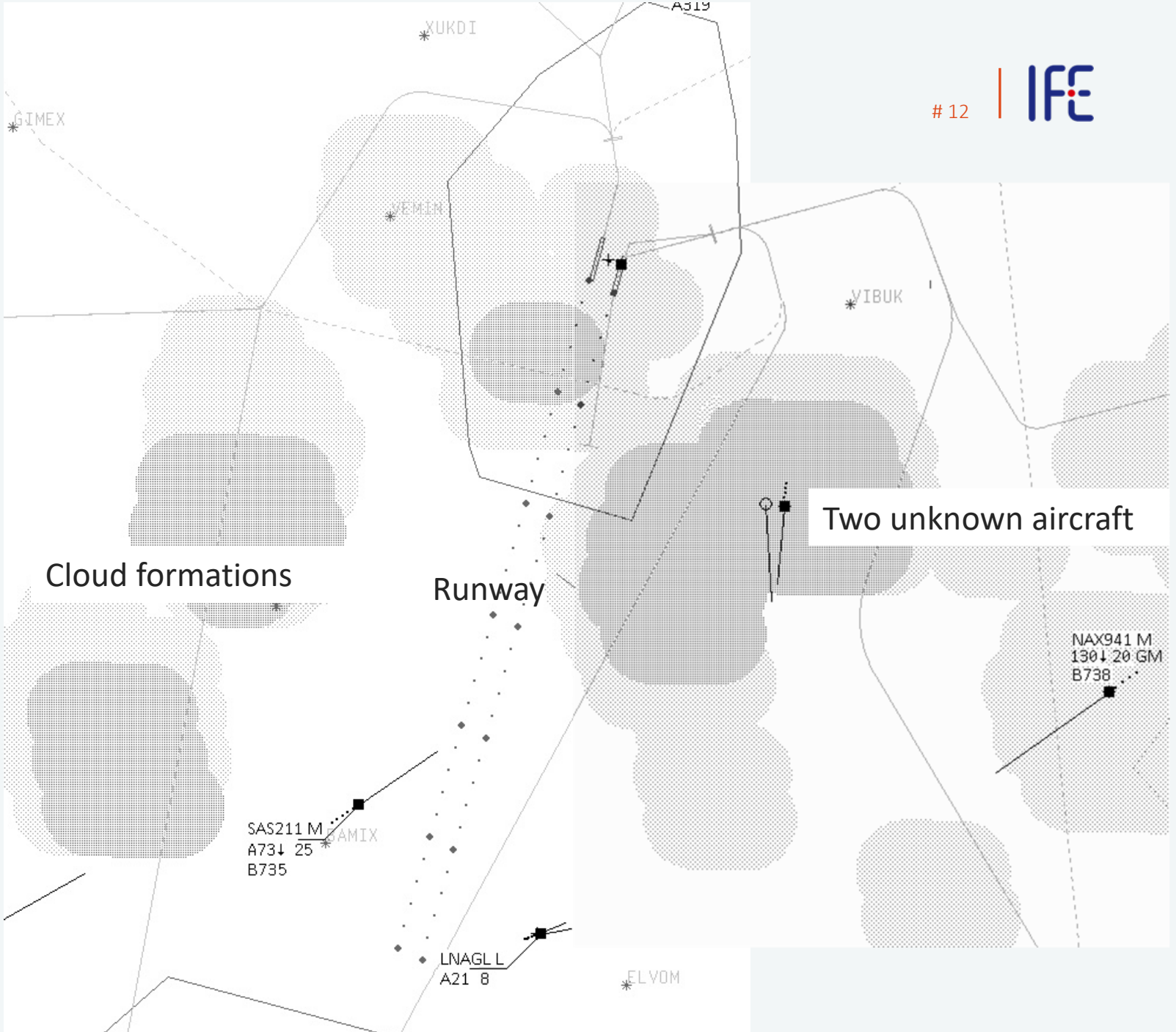
Normal traffic, all systems working correctly

Scenario 2 – seemingly technical issues

- Faulty radar in unrelated sector
- One aircraft indicates inaccurate data

Traffic issue:

- Unknown aircrafts safe distances diminishing

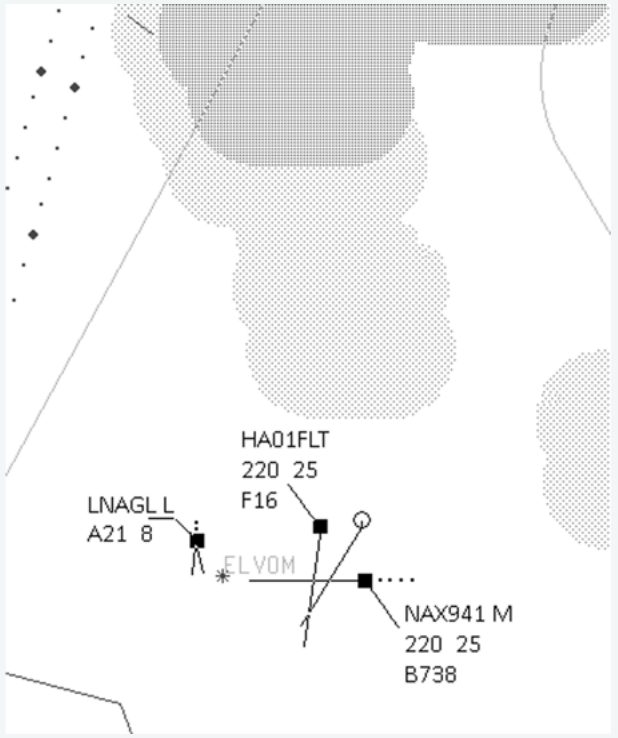


Scenario 3 – Ambiguous technical / cyber issues

Label information (altitude) is clearly wrong for three aircraft

Previously unknown aircraft now identified.

Two targets seem to be on collision course.



Scenario 4 – Clearly abnormal / cyber

Scenario 4a:

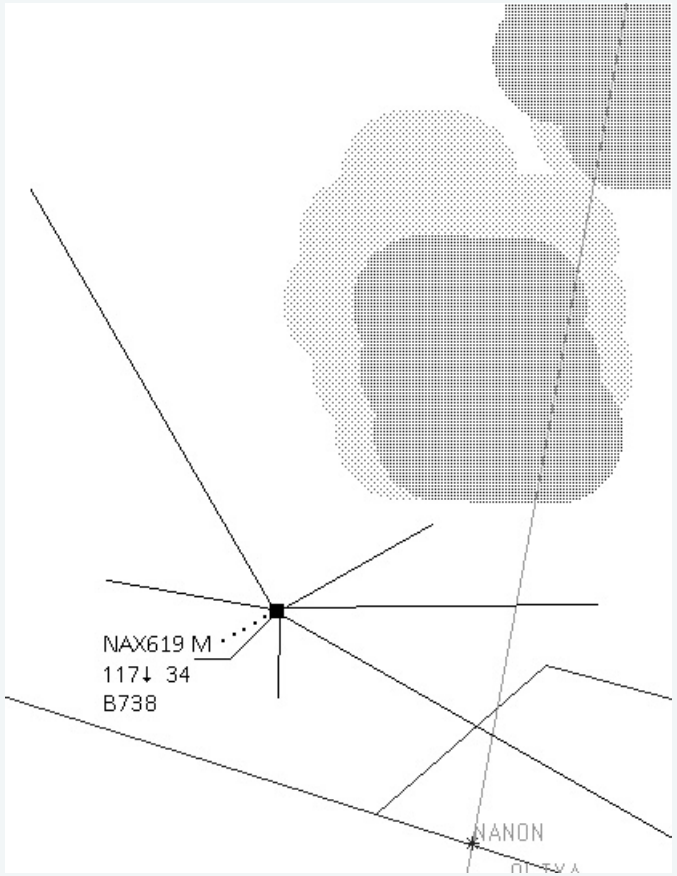
- Two aircraft jumped to previous location
- One duplicate aircraft

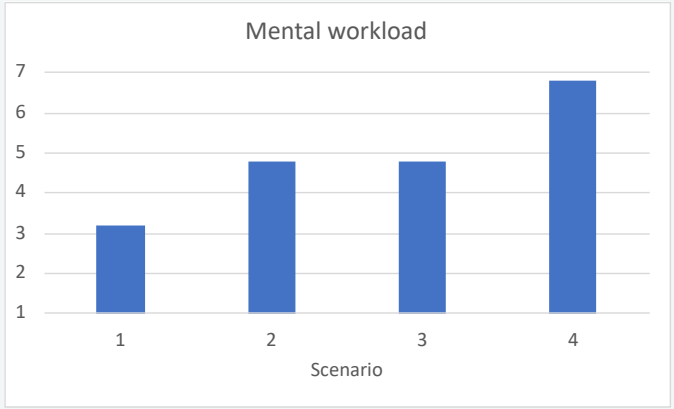
Scenario 4b:

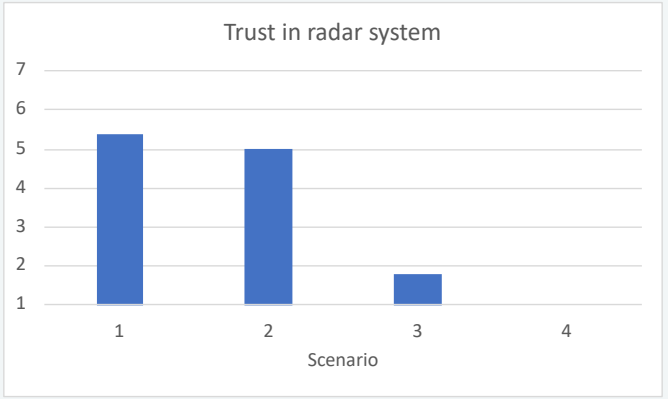
- Extra Predicted Track Lines (PTL) added to five aircraft

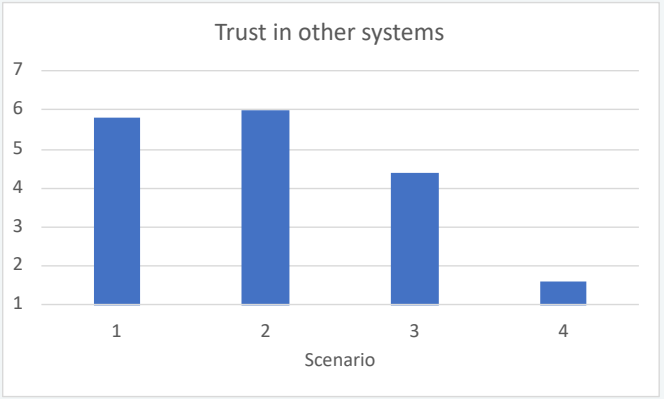
Scenario 4c:

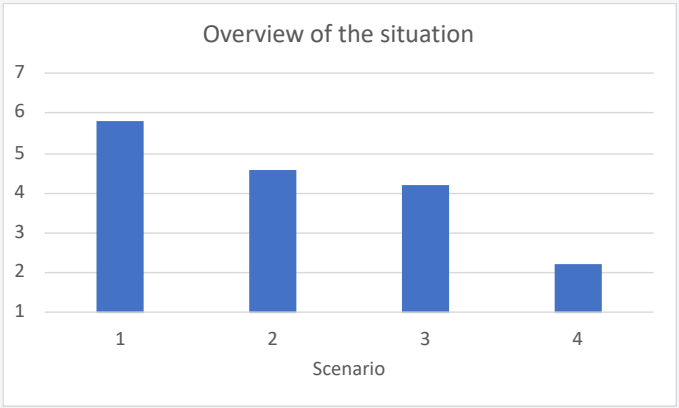
- Message and image from intruders shown in the surveillance picture

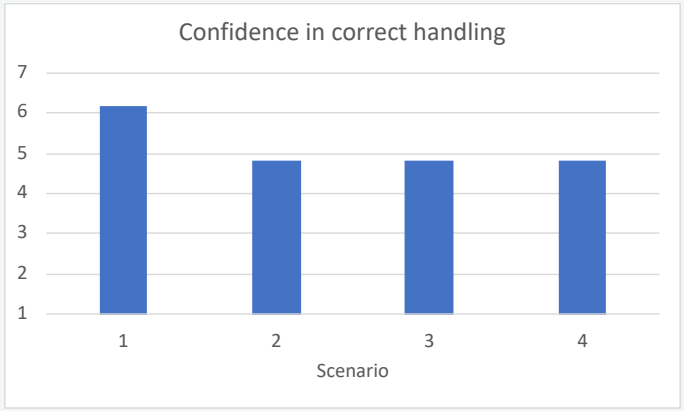












Results

- The cyber event negatively affected the ATCOs' workload, situation overview and trust in the technical systems.
- ATCOs did not suspect a cyber event until the very last scenario.
  - Did not have any experience of cyber events that could be used to help in understanding the situation
- When ATCOs suspected a cyber-attack:
  - Perception of the situation changed. ATCOs understood they were dealing with an actor with a malicious intent. Acted to enable planes to land on their own.

Simulator study on NPP operator's cybersecurity awareness

- Individual participation, 8 operators
- HPWR simulator
- 4 scenarios with ambiguous cyber / technical failures
- Warning of potential cyber incident before last 2 scenario runs

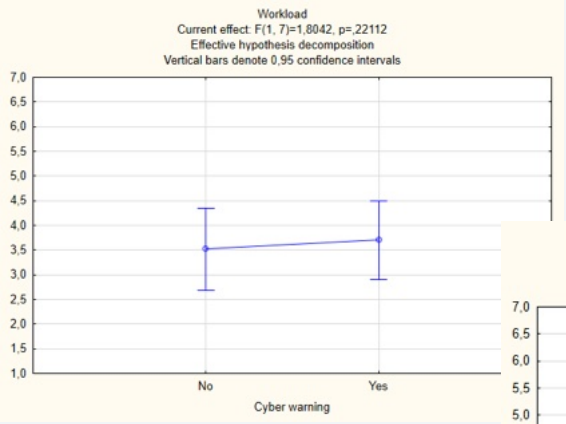
Run 1	No warning
Run 2	No warning
Run 3	Warning
Run 4	Warning

Balanced scenario sequence

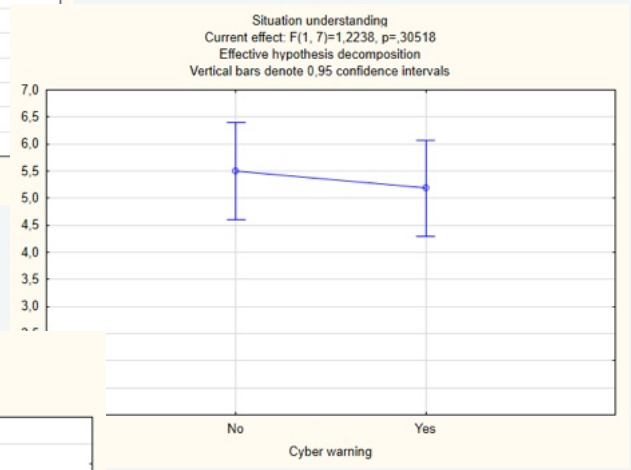
- Rated own workload, situation understanding and confidence in scenario handling
- Interview

Results

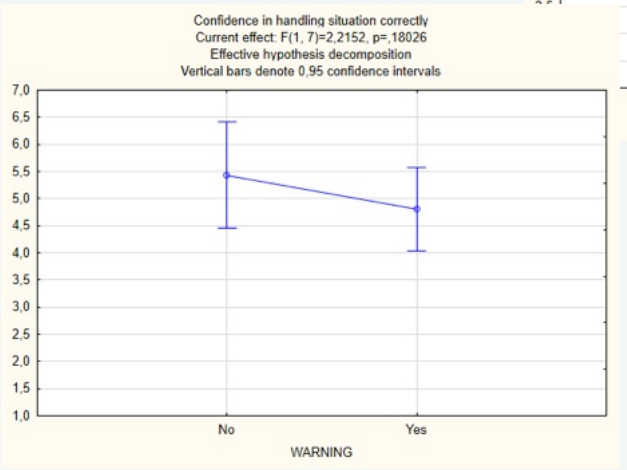
Workload



Situation understanding



Confidence



No significant differences between 'cyber warning' group and 'no cyber warning' group

Cyber security concerns from operators

Operator	Scenario	Run	Fault
A	1	3	Si-340 not closing
A	2	4	cond. booster pump not starting
B	3	4	SG level deviation
C	2	4	starts pump with discharge valve closed

Look at this, make sure it's not a cyber security threat

Detection of a cyber incident – insights from NPP operators

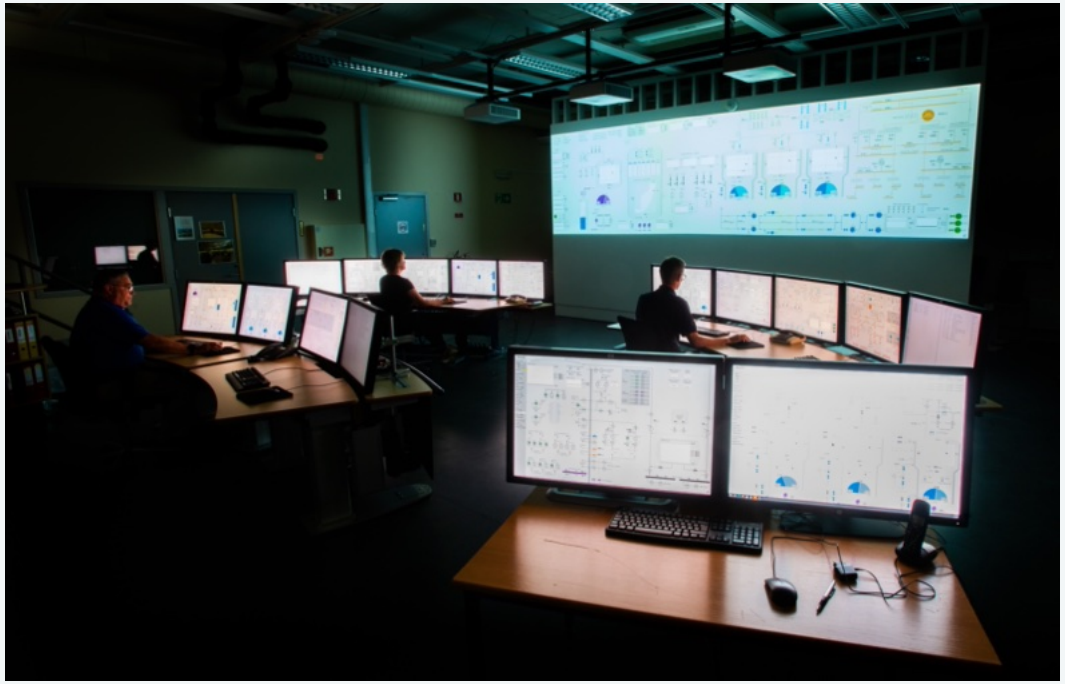
- Would question and investigate any abnormal indications — All crews
- Would first assume technical failure — 3 crews
- Signs of something other than mechanical failure
  - Multiple failures in unrelated systems — 2 crews
  - Mouse was moving on its own or things changing in the HMI on its own — 1 crew

3 Response to cyber-attacks

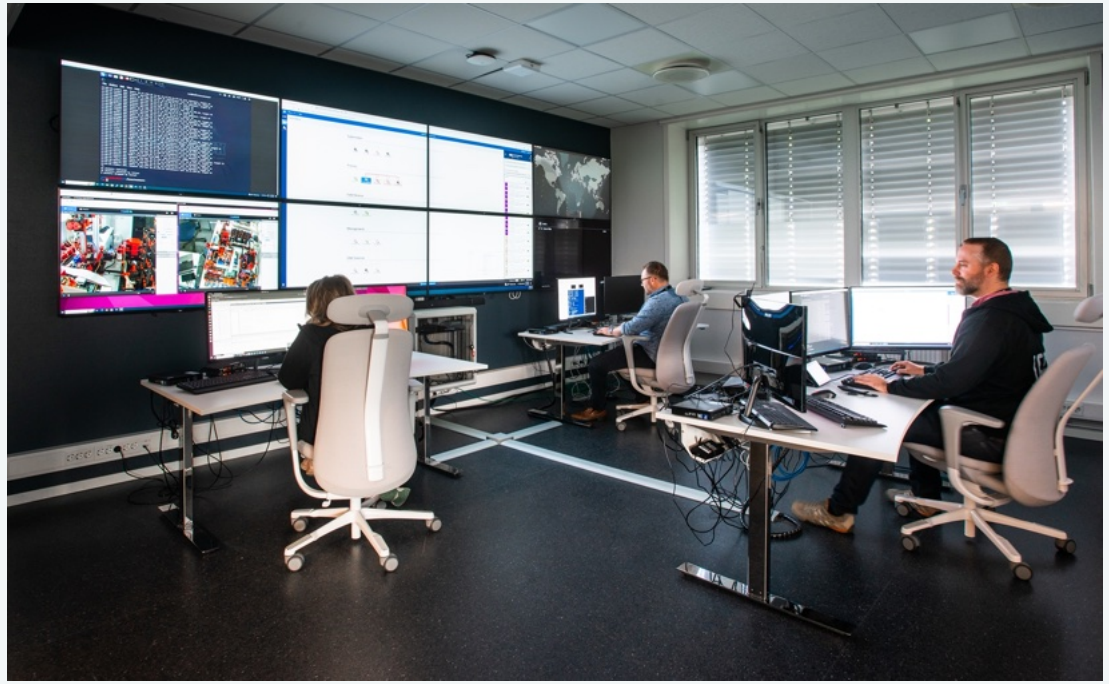
Response to a cyber incident – insights from NPP operators

- Report and monitor — All crews
  - Try to verify status of indications
  - Report to supervisor
  - Supervisor reports to IT / cybersecurity responsible / security / cyber issue response team
- Follow procedures — All crews
  - Use existing operating procedures
  - No cyber procedures exist (on operator level)
  - Take plant to safe condition
  - Diagnosis would come later (difficult to distinguish cyber from technical faliure)
  - Follow advise from cyber security responsible — 2 crews
  - If suspected cyber incident: Would be on lookout for more failures, increase monitoring — 1 crews

Collaboration between control room and Security Operation Center



IFE's Halden Man-Machine Laboratory (HAMMLAB)



IFE's Cybersecurity Center

Challenges:

- Safety focus (CR) vs security focus (SOC)
- Physical process domain (CR) vs abstract digital domain (SOC)
- Communication of risk

Espen Nystad, , Vikash Katta, John Eidar Simensen (2020). What happens in a control room during a cybersecurity attack? Preliminary observations from a pilot study

4 Conclusion

Implications for Prevention of Cyber-attacks

- Consider need for role-specific cyber awareness training
- Evaluate and improve training
- Update training based on current threat picture

Implications for Detection of Cyber-attacks

- Operators may be first line of detection
  - Limited training for detecting cyber-attacks in the control room
- Improvement of Operative cybersecurity awareness:
  - Cyber-attacks can impact plant systems
  - Signs of cyber-attack
  - Experience of cyber incidents from similar facilitites
  - Cyber scenarios in simulator training

Implications for Response to Cyber-attacks

- Procedures / guidelines for handling cyber-attacks
  - Consider cyber as possible cause
  - Escalation procedures
- Ensure business continuity
- Bridge gap between control room operators and cybersecurity operators

Questions?

Espen Nystad
Senior research scientist
ife.no
espen.nystad@ife.no