23 November 2020

Cybersecurity Webinar

Humans in incident response: Lessons learned from the nuclear domain

Espen Nystad, IFE

Contents

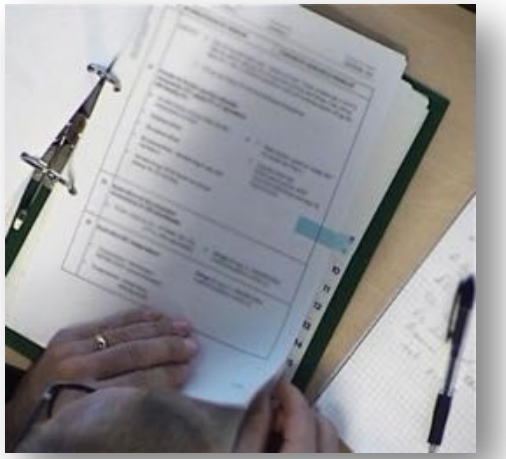
- Incident response in nuclear safety incidents
- A pilot study of cyber attack in a nuclear control room
- Relevance for aviation

Incident response in nuclear safety incidents

IFE's Halden Man-Machine Laboratory (HAMMLAB)

Incident response in nuclear safety incidents

- Nuclear industry is highly **proceduralised**
  - Procedures assist in diagnosis and response
  - Different procedures for different situations
    - What parameters to check
    - Point out course of action to bring plant to safe state



  - Danger: Operators go passively through procedure
    - Must be active in monitoring, interpretation of situation, make hypotheses, in addition to technical work

Incident response in nuclear safety incidents

Teamwork is important in handling incidents

- Communicate detections and interpretations to the crew
- Team orientation: take info from others into account

- Short status meetings to:
  - Gather input from all team members
  - Discuss situation
  - Agree on immediate goals and prioritise actions
  - Help reduce uncertainty, workload and stress

Incident response training

	Training of standard events	Training of unforeseen events
Training focus	Predefined set of emergency events	Unique, unpredictable events
Training approach	Use of procedures to handle the predefined event	Training to handle unforeseen events. - Transition form EOPs to guidelines - Coaching approach
Transfer of training to real situation	similarity across situations	ability to handle novel and unique situations

Adaptive-Expertise Theory

(Hatano and Inagaki, 1986)

Conceptual understanding of the domain

- e.g. thermodynamics, plant systems

Domain-specific skills

Awareness and control of own cognition

- e.g. guide own thinking about plant response

Metacognitive skills

Transfer and apply the knowledge to novel situations

- correctly adapt procedures, develop new strategies

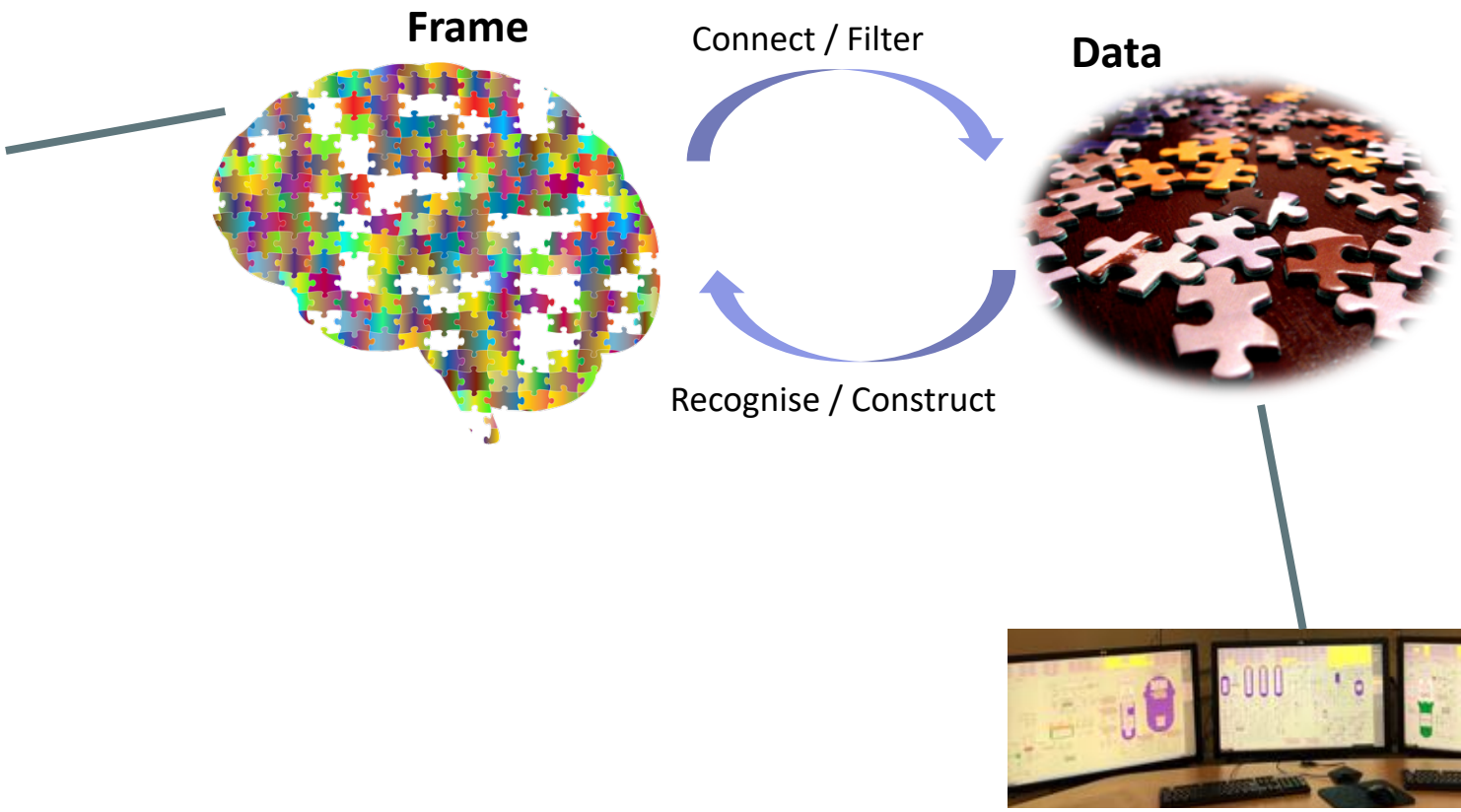
Innovative skills

How are signs of abnormality detected by operators?

Klein's Data-Frame theory of sensemaking

For nuclear setting:

Mental model of the factors assumed to be influencing the nuclear plant state at a given point in time



Simulation of cyber incidents for incident response

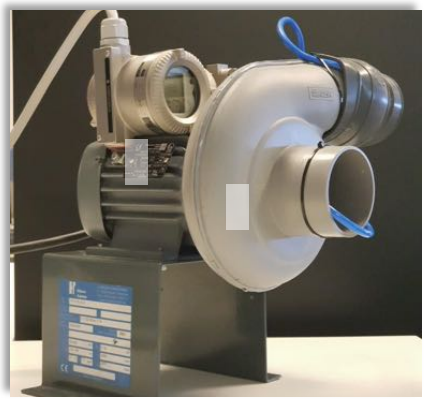
- Getting knowledge and experience from actual incident response can be difficult
  - Difficult to run exercises in real environment
  - Confidentiality prevents sharing of lessons learned
- Operators and IT/security team play important roles in cybersecurity defence
- Knowing how to respond to incidents is crucial

Pilot study: Cyber-attack in a nuclear control room

Purpose:

- To better understand cybersecurity incidents in a control room setting:
  - how operators react
  - challenges for incident response

Pilot study



Access and escalate privilege
- enterprise network
- PLC engineering workstation

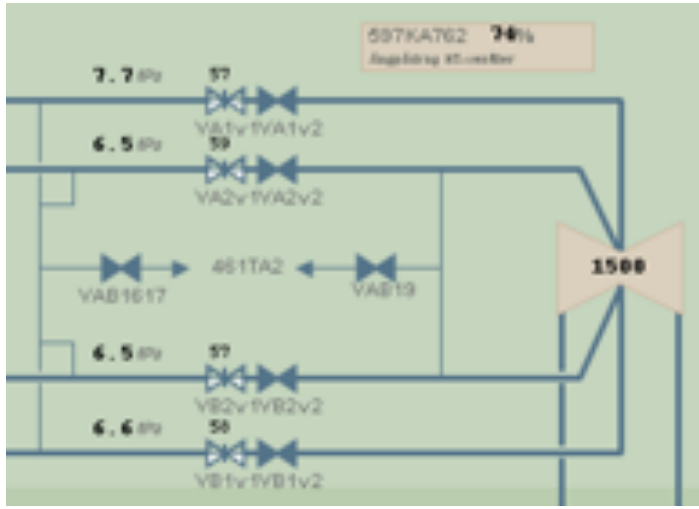
Observe and manipulate
- plant process and flow
- pressure values from PLC

Affect system (pump)
- increase steam pressure

Impact plant process and control
- safety pressure valves
- shutdown plant

Man-In-The-Middle attack on turbine pressure control system

- Generally not classified as a safety-critical system
- Leads to increase in reactor pressure, safety valves open, shut down
- Attack script freezes pressure measurements to mask the attack



PLC: Programmable Logic Controller

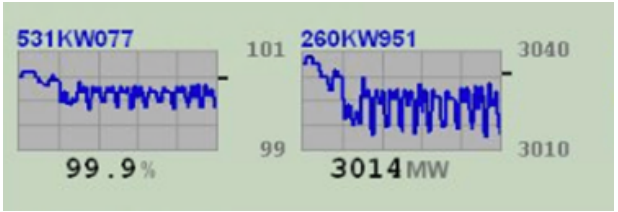
Findings - Lack of cybersecurity awareness and preparedness

Operators were able to use existing safety procedures to bring plant to a safe state, *but*:

- Lack of Monitoring and detection tools and capabilities
  - Little information on status of IT or OT systems to the control room
- Risk communication between security op centre and control room
  - Differences in focus – safety vs security
  - Lack of understanding of each other's domains and tasks
  - Lack of common language

Findings – A cyber-attack from the eye of the operator

- Operator detected the attack due to knowledge of normal reactor behavior
  - Understood something was not right, but did not suspect cyberattack



- When informed of possible cyberattack, it changed the operator's perception of the available plant information
  - Started to doubt some of the other information

Relevance for aviation

- When an abnormal incident occurs:

	Nuclear	Aviation
Goal	Bring plant to safe state	Ensure correct safety margins, shut down traffic
Potential consequences of failure	High	High
Domain complexity	High	High
Procedure complexity	High	Medium

Summary: Cyber security preparedness – ability to handle unforeseen events

- Establish situation awareness
  - Employ existing expertise in the team
  - Monitor, interpret and discuss the situation

- Adaptation of knowledge
  - Interpret signals based on past knowledge
  - Adapt knowledge to new situations

Some questions for cyber events in aviation

- What should be the role of aviation operations personnel in cyber incident detection?
- How can they build expertise to help detect cyber events at an early stage?
  - Would operators consider cyber attacks as a possible cause?
  - Do they need more technical (IT) competence?
- How can operational staff and SOC/IT staff cooperate to understand what is happening?
  - Do they have a common language?
- Do operations personnel have sufficient cyber security awareness?

Thank you for the attention!

Espen Nystad
Senior research scientist,
Human-Centred Digitalization

Espen.Nystad@ife.no