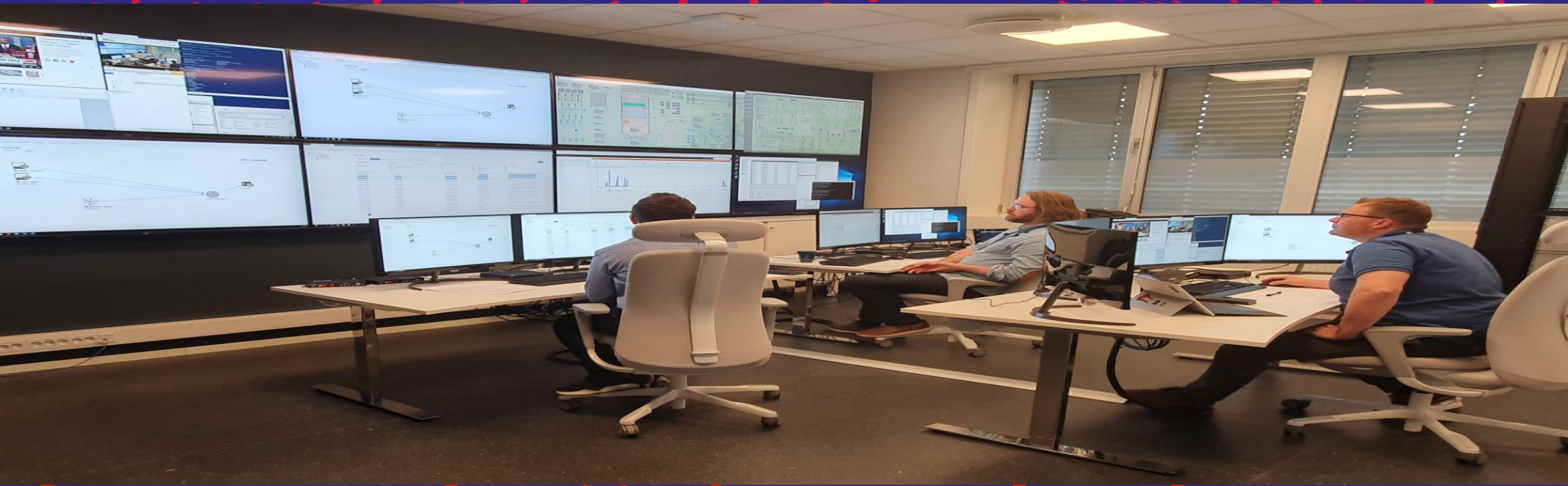
Research for a better future

Vikash Katta & John Eidar Simensen

23-11-2020

CybWin project

Towards a platform for ATM cybersecurity incident simulation and training



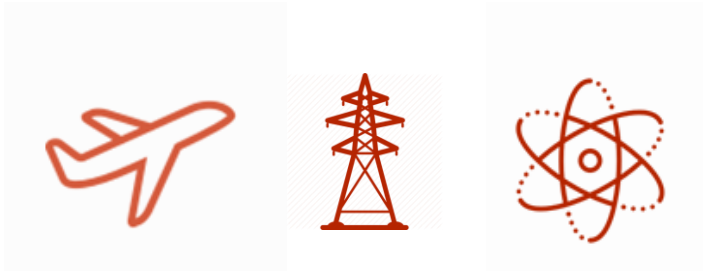
CybWin Project

- **Funded** by The Research Council of Norway – IKTPLUSS Programme
- **4 Year project** (December 2018 – November 2022)
- **Aim** is to develop a cybersecurity platform for assessment and training for critical infrastructures. Emphasizes the role of humans in cybersecurity by investigating human preparedness and training.
- **Target groups** – incident responders (controllers/operators, security team, system engineers,..); critical infrastructure (aviation, energy distribution, nuclear power plant)

The Research Council of Norway

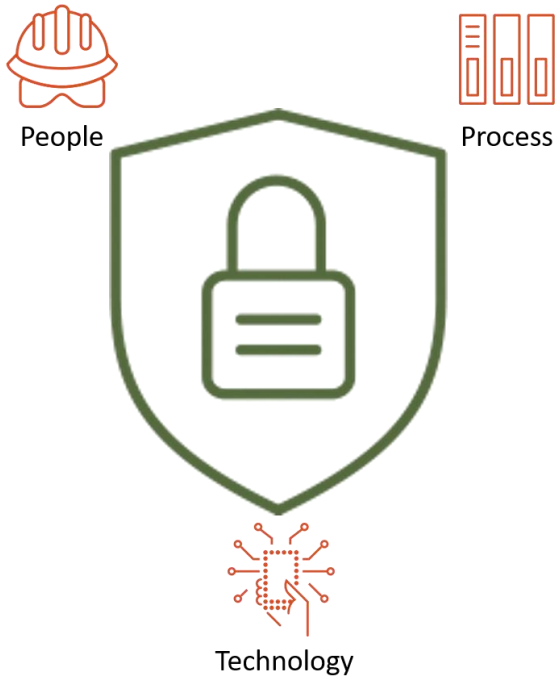
Consortium

- Institute for Energy Technology
- Norwegian University of Science and Technology
- Secure-NOK
- Avinor Air Navigation Services
- EUROCONTROL
- VTT Technical Research Centre of Finland Ltd
- Korea Advanced Institute of Science and Technology
- Statnett



Background

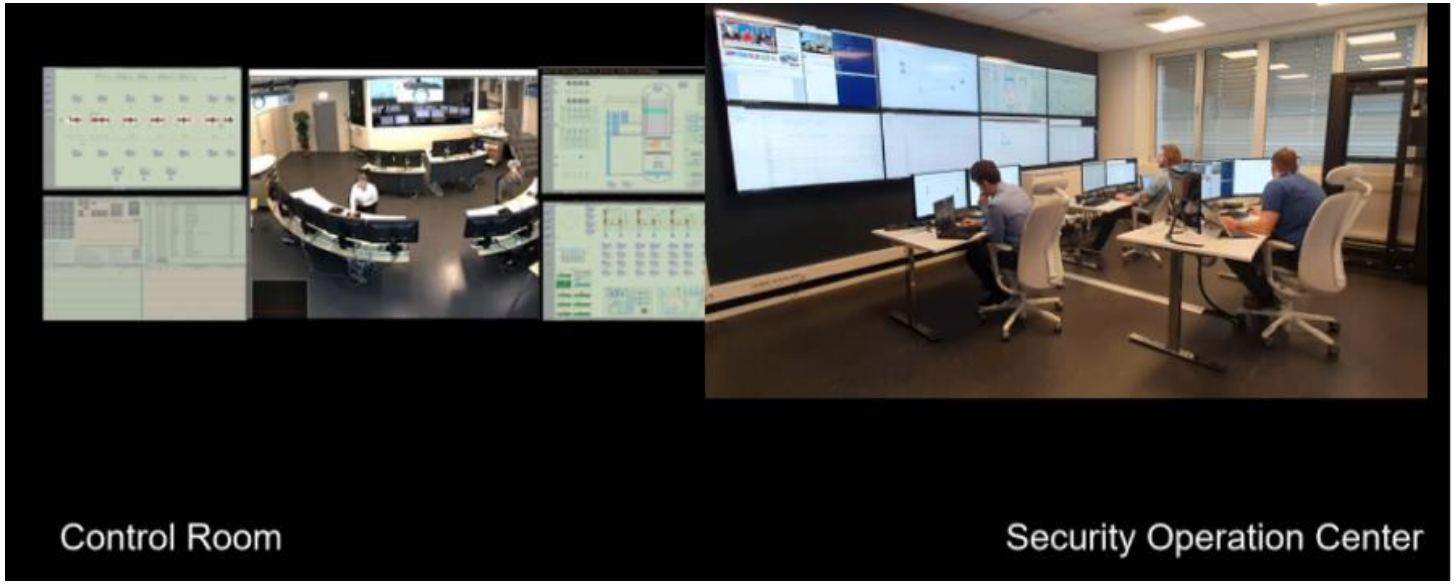
- Lack of cybersecurity facilities (ranges, testbeds, simulators)
  - Investigate cybersecurity of critical infrastructure
    - Not only to investigate **technology**, but also **people** and **processes**
  - Available testbeds are predominantly for academic purpose, while some testbeds are closed for national security or military purpose
  - For aviation/ANS domain, how many testbeds are available?



- Lack of realistic cybersecurity attack scenarios, and experts to plan and investigate these scenarios
  - Need a multidisciplinary team – security engineers, system engineers, human factors experts, process experts, controllers, …..

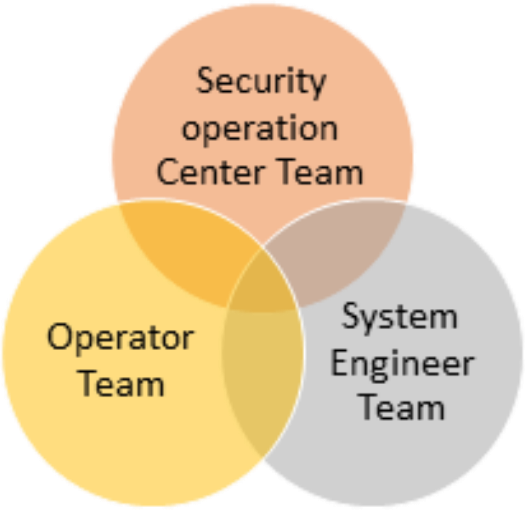
Main deliverables

- Develop a **cybersecurity platform** for assessment and training for critical infrastructures
  - integrated safety and security risk models for incident response
  - cyber-attack monitoring and detection methods and tools
  - highly configurable testbed with realistic depiction of real-world Norwegian critical infrastructure and threat environment
    - high-fidelity simulation technologies for cybersecurity- and RAMS- incident prediction and response
    - support assessments of human perception and decision-making during incident response
    - plug-in modules to other simulators on operational process, safety and training thereby providing the possibility to study cybersecurity aspects as a part of the existing environment



Given a cyber incident scenario, what kind of mechanisms (process, tool, approach, model) for communication facilitates common situation and risk awareness between relevant stakeholders (technical, cyber, operator) and support them in taking effective and efficient decisions

TITLE	C1	C2	C3	C4	C5	C6	C7	C8
Cyber Security Incident Handling, Warning and Response System for the European Critical Information Infrastructures (CyberSANE)	PS	PS	S	S	S	S	PS	PS
Examining Cybersecurity of Cyberphysical Systems for Critical Infrastructures Through Work Domain Analysis	S	NS	S	PS	S	PS	PS	PS
Integrating a Security Operations Centre with an Organisation's Existing Procedures, Policies and Information Technology Systems	PS	PS	NS	PS	PS	PS	PS	PS
A collaborative cyber incident management system for European interconnected critical infrastructures	PS	PS	S	S	S	S	S	S
Secured Transactions Technique Based on Smart Contracts for Situational Awareness Tools	PS	S	PS	PS	PS	PS	PS	PS
SecMonQ: An HSM based security monitoring approach for protecting AUTOSAR safety-critical systems	PS	NK	PS	NS	NK	NK	NK	NK
Manipulating Residents' Behaviour to Attack the Urban Power Distribution System	NK	PS	S	NS	PS	PS	PS	NS
Urban resilience in the making? The governance of critical infrastructures in German cities	PS	NS	S	PS	PS	PS	NS	NS
Threat intelligence platform for the energy sector	PS	PS	PS	PS	PS	PS	PS	PS
A stealth monitoring mechanism for cyber-physical systems	PS	PS	PS	PS	PS	PS	NK	NK
Call to Action: Mobilizing Community Discussion to Improve Information-Sharing About Vulnerabilities in Industrial Control Systems and Critical Infrastructure	S	PS	S	PS	S	PS	PS	PS
BRIoT: Behaviour Rune Specification-Based Misbehaviour Detection for IoT-Embedded Cyber-Physical Systems	PS	S	NK	PS	PS	PS	NS	NS
A FORENSIC LOGGING SYSTEM FOR SIEMENS PROGRAMMABLE LOGIC CONTROLLERS	PS	PS	PS	PS	NS	PS	PS	PS
CYBER SECURITY MANAGEMENT MODEL FOR CRITICAL INFRASTRUCTURE	NK	NK	S	NS	PS	PS	NS	PS
CSIRT Management Workflow: Practical Guide for Critical Infrastructure Organisations	PS	S	S	PS	S	PS	PS	PS
TOWARDS VALIDATING A SECURITY SITUATION MANAGEMENT CAPABILITY	PS	PS	S	S	S	PS	PS	NK
Event-Triggered Watermarking Control to Handle Cyber-Physical Integrity Attacks	PS	PS	NK	PS	PS	NS	NS	PS
A structural design for a pan-European early warning system for critical infrastructures	PS	PS	S	S	S	S	S	S
Operational response model for physically attacked water networks using NSGA-II	PS	PS	PS	NS	S	PS	NK	PS



Criteria	
ID	**Description**
C1	**Role-based**: The candidate solution can identify people and person, their belonging to a team and their disciplines (Security expert, Operations expert…).
C4	**Real-Time Information**: The candidate solution supports and organise real-time information sharing of the incident, security data, operations data and system data.
C6	**Incident Decision making:** The candidate solution supports and organise the decision making in an easy to understand manner to resolve the incident based on the incident information
C2	**Phase and Time**: The candidate solution references phase and time activity for the incident and communication
C3	**Contextualised**: The candidate solution can fit to the context, location and the domain of the organisation, and level of criticality.
C7	**Communication mean**: The candidate solution permits the use of different channel and medium
C8	**Secure and legal**: The candidate solution supports secure and legal information sharing (for example in terms of confidentiality, integrity, availability, and non-repudiation)
C5	**Risk evaluation**: The candidate solution evaluates the ongoing situation with a risk assessment such as an impact analysis.

CybWin - Aviation case

- Aviation case provides an opportunity to address operational cybersecurity
  - Focus towards the operational
  - Build capabilities and experience step-wise through the project
  - Perform experiment on cyber in ATM

- Access to
  - An air navigation system used in Air Traffic Management
  - SNOK IDS-system
  - ATCOs, OPSUP, TECHSUP and ATM system specialists
  - Cyber security experts
  - Human Factor experts

AVINOR EUROCONTROL Statnett VTT KAIST SECURENOK NTNU IFE

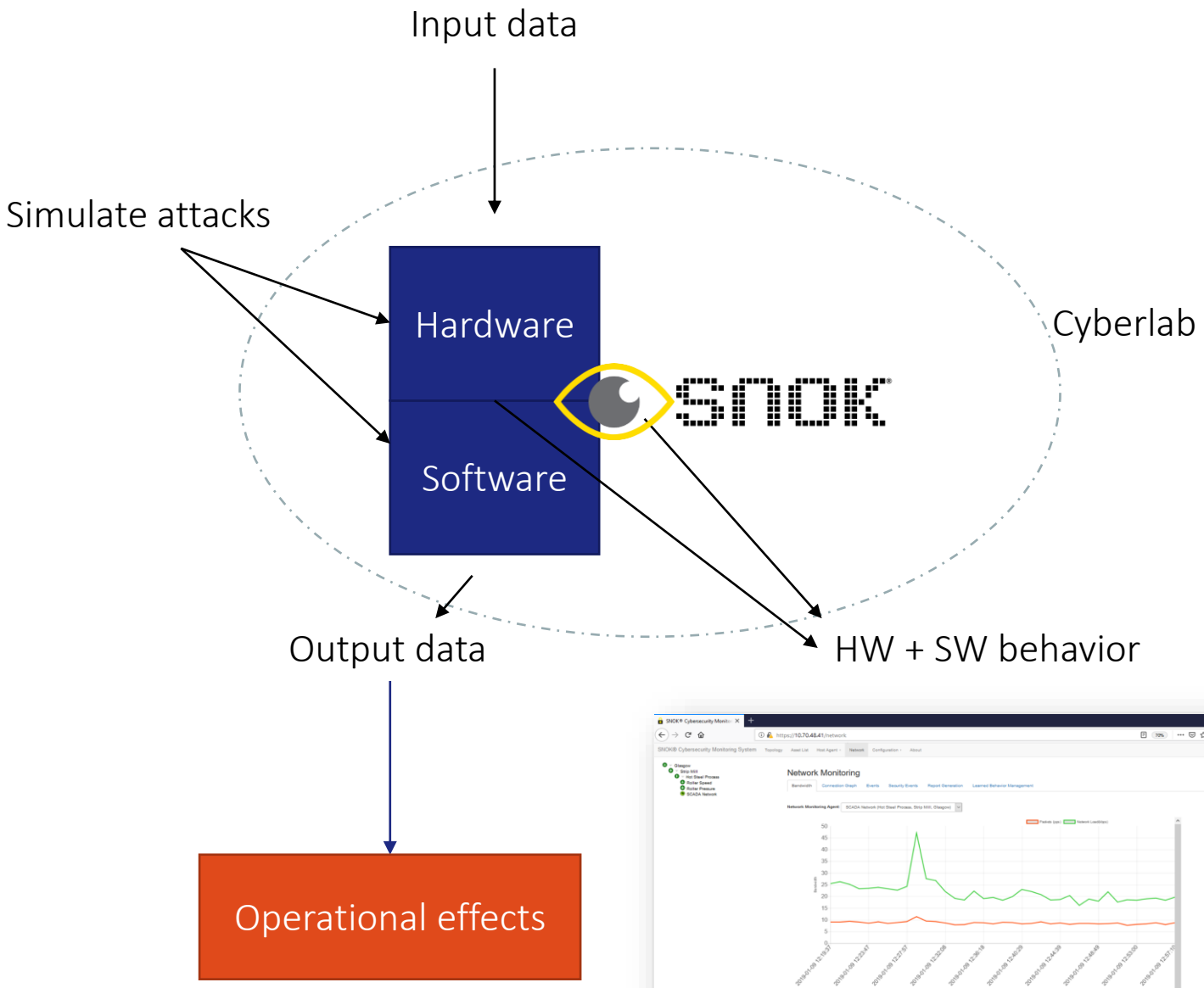
Examples of relevant ATM experience

- Eye-Tracking for Training of ATCO's (2015)
- Remote Tower center – main control room design for Avinor (2017)
- *Designing Radar Display Graphics to Mitigate Controlled Flight into Terrain* (Journal 2018) [1]
- *Experiences from implementing and testing an approach for cybersecurity event detection in a critical aviation system (2019)* [2]
- *The Concept of Cybersecurity Culture (2019)* [3]
- *What happens in a control room during a cybersecurity attack?: Preliminary observations from a pilot study (2020)* [4]

1: Braaseth et. al.: Journal of Air Transportation / Air Research Central: https://arc.aiaa.org/doi/10.2514/1.D0152
2: Engum & Simensen: Proceedings of the 30th European Safety and Reliability Conference(ESREL), ISBN: 978-981-14-8593-0
3: Reegaard et al: Proceedings of the 29th European Safety and Reliability Conference(ESREL): http://rpsonline.com.sg/proceedings/9789811127243/html/0761.xml
4: Nystad et al: ICSEW'20: Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops –available: https://dl.acm.org/doi/10.1145/3387940.3391454

Technical experiment

- Simulate typical attacks through controlled scripts
- Expected results:
  - Effect on output traffic data / software behavior
  - Hardware effects/behavior
  - SNOK (IDS) learning and adjustment
- Input to the operational experiments and in particular more complex scenarios



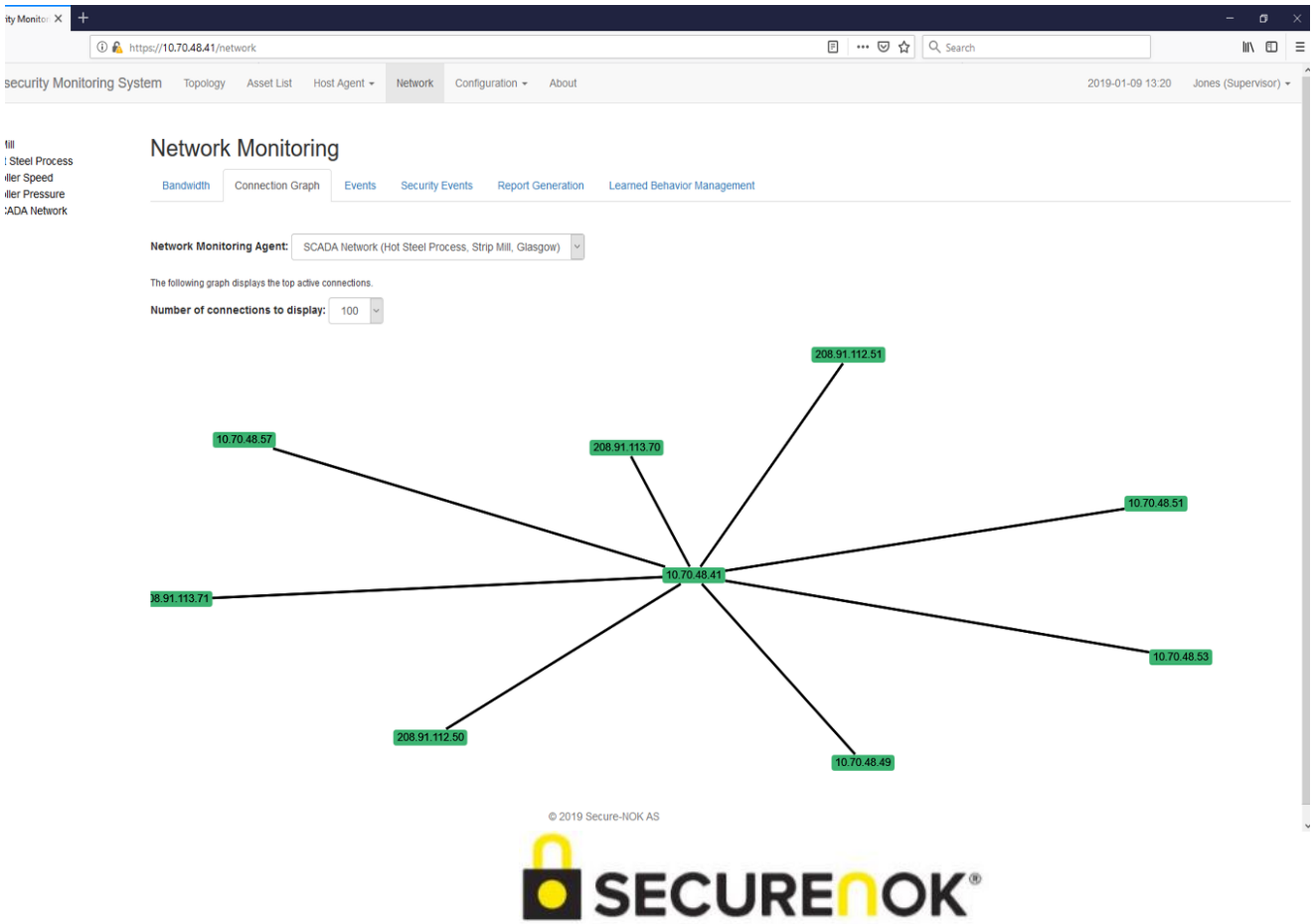
Technical experiment

SNOK – **I**ncident **D**etection **S**ystem from Secure-NOK

- Host & Network Behavioral Anomaly Detection capabilities
  - Software agents at nodes
  - Network tap
  - Analysis platform appliance

SNOK learning algorithm

- Learns normal behavior over time
- Flags everything not “normal”
- Allows for further detailing of flags – what is allowed outside of “normal”



*Text and picture from presentation of Engum & Simensen: Proceedings of the 30th European Safety and Reliability Conference(ESREL), ISBN: 978-981-14-8593-0

Operational experiments

1. *Investigate how a controller will behave and handle a safety incident when compared to a cyber-attack.*

2. *Investigate how a controller will behave and handle a cyber-attack when organization is equipped with solutions, tools, procedures, training, etc. for early detection capabilities.*

Operational Experiment 1

- Investigate how a controller will behave and handle a safety incident when compared to a cyber-attack

- ATCO in focus
  - under ‘normal’ (non-cyber) conditions/events
  - and when cyber is the initiating event
- Several goals:
  - Establish scenario descriptions and develop templates
  - Establish data gathering protocols, interview guides etc.
  - Establish experiment guides and check lists
  - Gather experience on the scenario for the researchers/planners
- First ‘experiment’ - remote observation by HF experts and researchers, data gathering both local and from remote

Operational Experiment 2

- Investigate how a controller will behave and handle a cyber-attack when organization is equipped with solutions -tools, procedures, training, etc. for early detection capabilities

- Control room in focus: ATCO + OPSUP (+ Techsup)
  - Technical experiment provides realistic conditions/failure modes
  - Developing cyber conditions/situation
  - More complex scenario where the event develops dynamically so that the ATCO and OPSUP not immediately will go to ‘safe mode’/close airspace
  - All participants co-located (i.e. non-remotely)
- Interaction and procedures in the control room between defined stakeholders now part of the experiment

Thank you

Vikash Katta
Senior Research Scientist

Vikash.Katta@ife.no