Utfordringer av forsyningssikkerheten ved økt cybertrussel

Lars Erik Smevold (Statnett / KraftCERT)
John Eidar Simensen (Inst. For Energiteknikk)

ESRA Seminar
1 Sept. 2021

Statnett

01	CybWin project
02	Threat landscape of the powergrid

IFE Digital Systems

From sensors to decisions

Departments:

- Control Room & Interaction Design
- Virtual & Augmented Reality
- Applied Data Science
- Humans & Automation
- Human Centered Digitalization
- Risk, Safety, & Security
- Applied Nuclear Science

Spinoffs since 2000:

VISAVI TECHNOLOGY

wirescan

First Sensing as

AUGMENTI™

International projects > 72%
> 150 ongoing projects

76% 24%

HALDEN PROJECT HTO

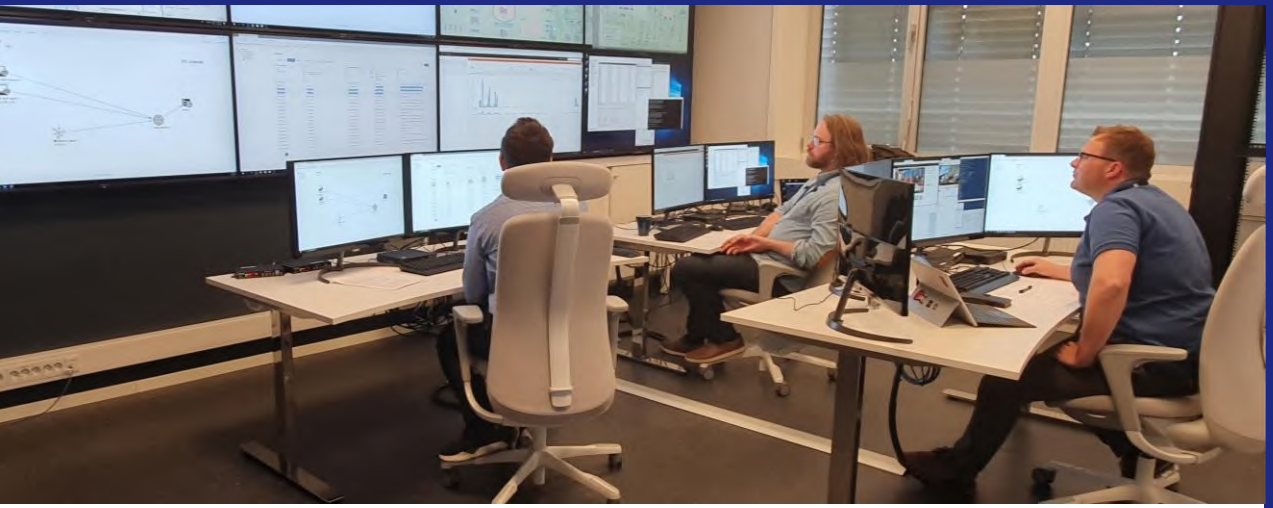
11 Laboratories

- HAMMLAB - Human-Machine Lab
- HVRC - VR/AR lab
- Future lab
- Human-Centred Sensing lab
- Digitalization lab
- Sensor & Mechatronic lab
- 4 Decommissioning labs
- HADRON Robotics lab (under construction)

2 Centres:

- Cybersecurity Centre
- IAEA Nuclear Decommissioning Centre

IFE Cybersecurity Centre



Cyber center serves and supports projects comprising (e.g.):

Statnett, AVINOR, Høgskolen i Østfold, NTNU, SECURENOK, University of St.Gallen, VIRGINIA TECH, REINER LEMOINE INSTITUT, Universitat de Girona, EUROCONTROL, VTT, KAIST, BORG HAVN, CREESC, GECO Global, Schneider Electric, SMART INNOVATION NORWAY, Inycom, BSES, HALDEN PROJECT HTO

Capabilities:

- Fully customizable environment
  - Full freedom physical and virtual servers and machines
  - Customizable network infrastructure
- Enclaves for customer equipment
- Possibility for onsite access
- Secure remote access
- Technical and operational scalability

What we do:

- Assessments and testing
- Simulation and modelling
- Incident detection and response
- Awareness and training

CybWin Project

Cybersecurity Platform for Assessment and Training for Critical Infrastructures – Legacy to Digital Twin

Norwegian research council project

Project timeline 2019-2022

Total budget:
28 million Norwegian kroner

CybWin – domains and use cases

- CybWin's three different domains; nuclear, aviation and power grid/supply comprise different:
  - systems and critical infrastructure, different procedures and processes, different people, knowledge, culture, …
  - all of which relates against the respective domains' threat picture

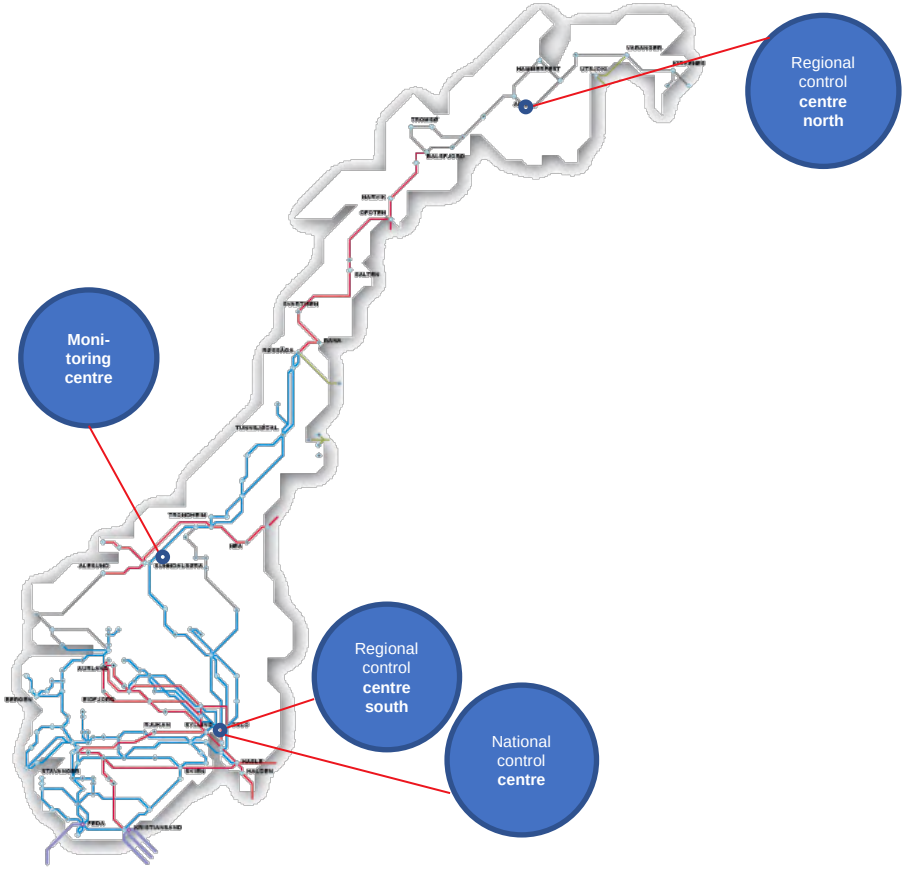
Threat Landscape of Power Grid Substations

Lars Erik Smevold, KraftCERT
Siv Hilde Houmb, Statnett SF

Statnett

This is **Statnett**

- Statnett is the system operator of the Norwegian power system.
- Statnett operates around **11,000** km of high-voltage power lines, **166** substations and **1,400** km of subsea and land cables across Norway.
- The National and Regional Control Centres continuously monitor the grid to ensure stable power supply.
- Statnett is also responsible for interconnectors to Sweden, Finland, Russia, Denmark and the Netherlands.



KraftCERT/InfraCERT

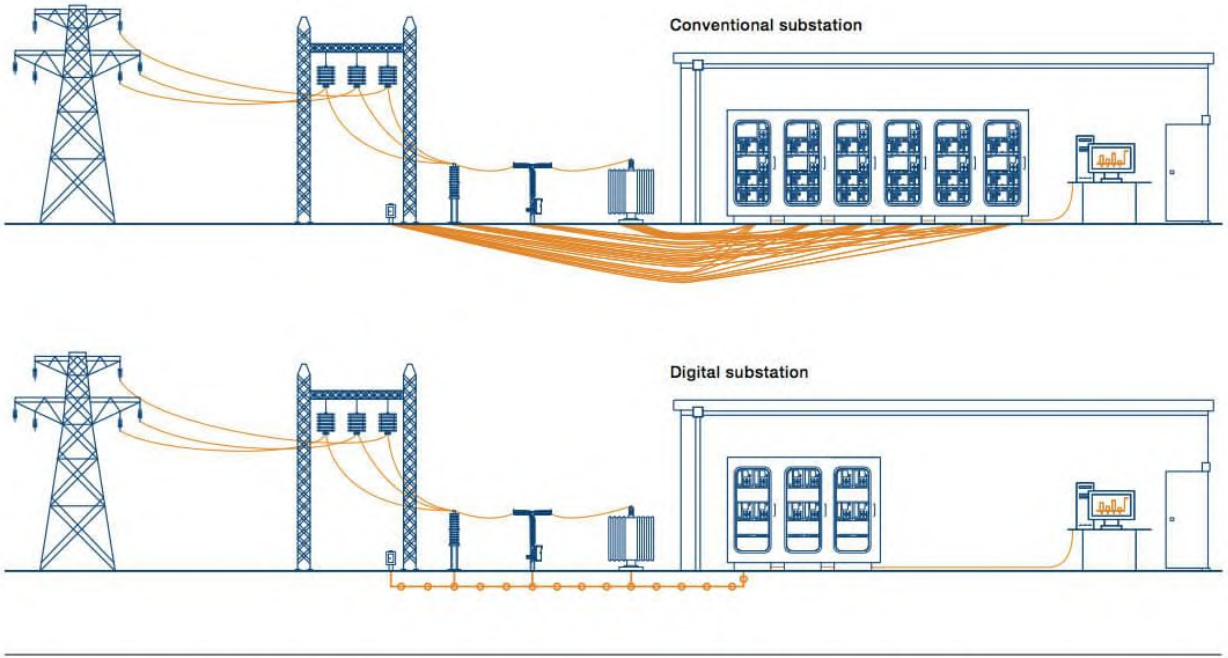
Norwegian Energy Sector and Control System CERT

- Initative from NCSC.no and The Norwegian Water Resources and Energy Directorate.
- Independent, non-profit corporation.
- Part of the national response function for sectors.
- Industrial Control Systems
  - Electrical, Oil&Gas, Process, Water&Waste and other ICS related industry.
- Owners: Statnett(TSO), Statkraft(Generation) and Elvia(DSO).

Digitalization of Power Lines

Digital Substation

Digital substations replace many point-to-point copper cables with a single fiber-optic process bus.



*The digital process bus is managed by the IEC 61850-2 subsection of the standard for digital substation communication. It underpins the true digital substation and requires a new approach to substation architecture, design and construction.

https://www.windpowerengineering.com/going-digital-look-modern-substation/

Smart Grid - Digitalization

- Substations:
  - Digitalization all the way out to the switchyard (fiber and IP).
  - Instrumentation and data gathering in substations.
  - From box/hardware to functions (software).
  - Multiple functions in one box (IED).
  - Cloud services.
- Power lines:
  - Sensors and IIoT devices on power lines.
  - Cloud services.

Huge increase in the amount of data gathered for various types of analysis, but also to support operations and management of the grid.

Anything to Worry About?

Attackers and their **Capabilities**

Security Level	Target	Skills	Motivation	Means	Resources
SL4	Nation State, Contractors	ICS Specific	High	Sophisticated (Campaign)	Extended (Multidisciplinary Teams)
SL3	Hacktivist, Terrorist	ICS Specific	Moderate	Sophisticated (Attack)	Moderate (Hacker Group)
SL2	Cybercrime, Hacker	Generic	Low	Simple	Low (Isolated Individual)
SL1	Casual or coincidental violations	No Attack Skills	Mistakes	Non intentional	Individual

Based on IEC 62443

Threat Picture

- Random infections have led to profiling, which can lead to targeted attacks.
- ICS is a major asset for the attackers:
  - Malware can have ICS functionality.
  - Attack on Safety Instrumented Systems (SIS).
  - Supply chain attacks.
  - …

Low hanging fruit´s are still important for an attacker.

Cybersecurity Standards of Relevance

- **IEC 62443** is the leading standard within cybersecurity for control and automation systems.
  - IEC 62443 covers all aspects of cybersecurity for IACS (organization, system, component).

- **IEC 62351** defines security controls for power grid communication, such as IEC 104 and IEC 61850.
  - Scope is securing communication.
  - Covers encryption, certificates, PKI, RBAC.

The practical approach in CybWin R&D

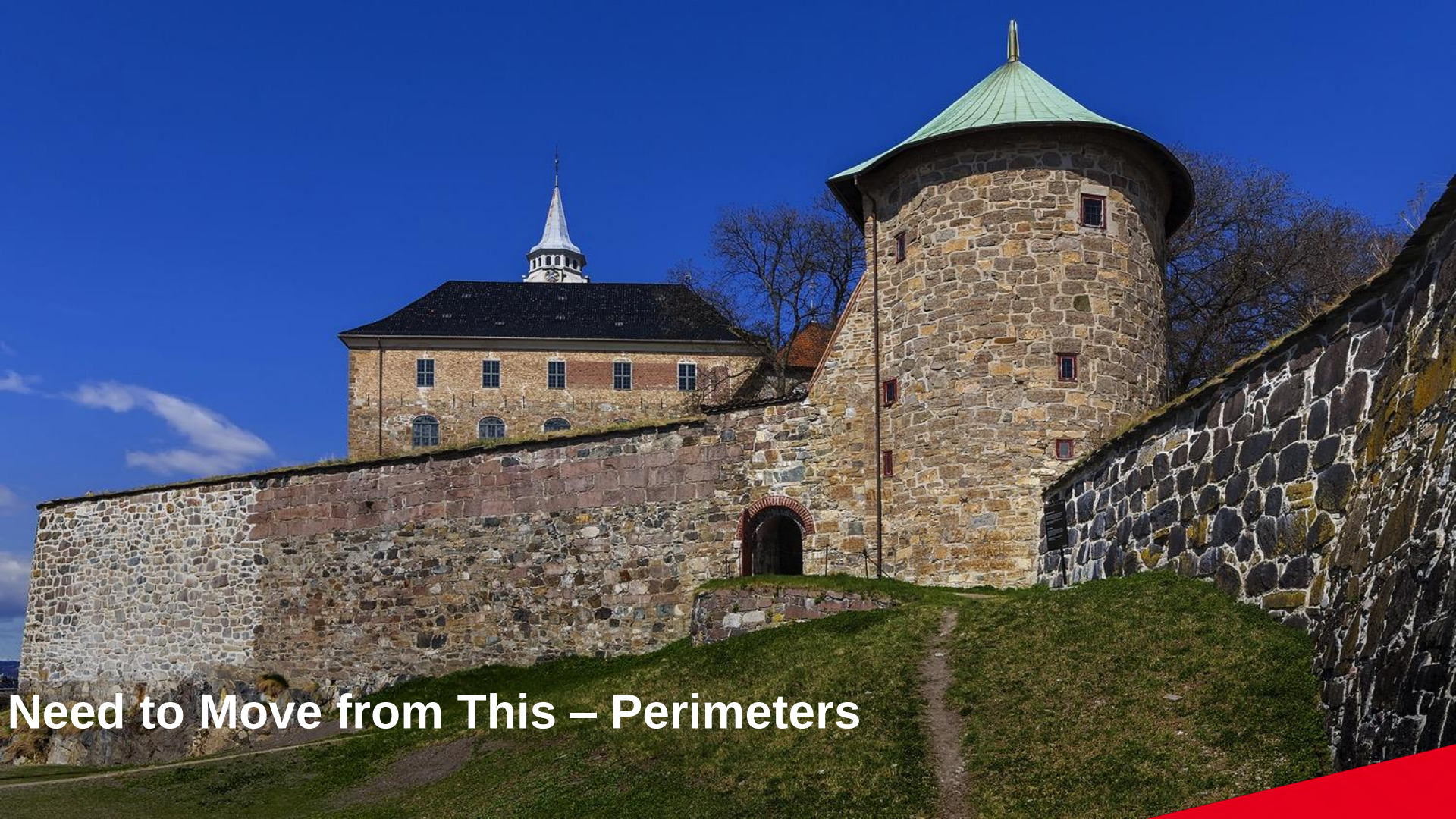
The theory needs support from practice.

More valuable insight and knowledge.
As close to real time systems as possible.

Attackers view vs Defenders view.

- Systematic approach based on real attacks.
- The possibilities of other attack vectors
- Enhance our incident response and defending perspectives.

- Human factors when an incident occurs.
  - Human behavior in an ICS environment during Cyber incident.
  - Practical solutions/how to – playbooks, procedures, processes…



Need to Move from This – Perimeters

And Build Security Based on a New Reality

Statnett

The Future is Electric