Research for a better future

Bjørn Axel Gran
John Eidar Simensen

Fagseminar om cybersikkerhet i kraftsektoren
3. november 2021

IFE Cybersecurity lab – trening, trening og trening

IFE Digitale Systemer

Fra sensorer til beslutning

Avdelinger:

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

International projects > 72%
> 150 ongoing projects

76% 24%

OECD Halden Reactor Project

11 Laboratorier

- 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

2 sentre:

- Cybersecurity Centre
- IAEA Nuclear Decommissioning Centre

Spinoffs since 2000:

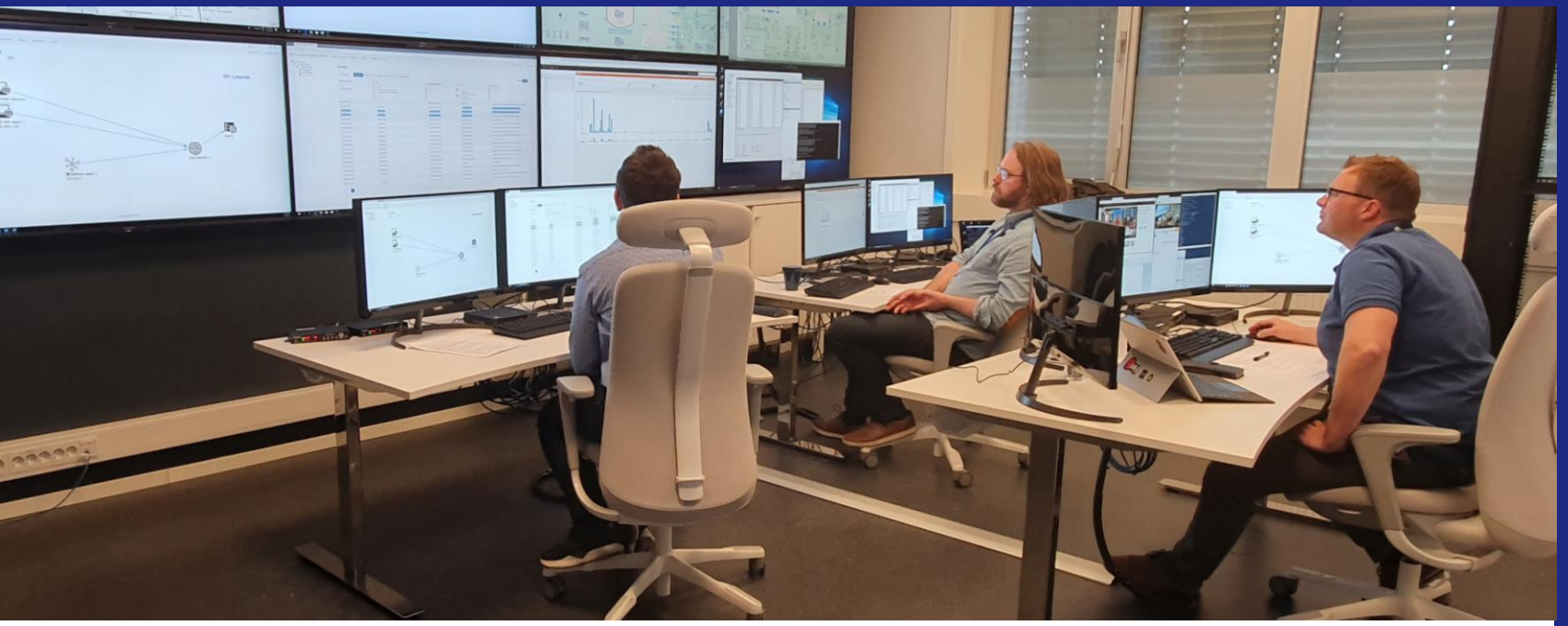
VISAVI TECHNOLOGY

wirescan

First Sensing as

AUGMENTI™

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, EUROCONTROL, Universitat de Girona, GECO Global, VTT, KAIST, BORG HAVN, JOTRON, indra, BSES, ЕНЕРГОАТОМ, Schneider Electric, Inycom, REINER LEMOINE INSTITUT, CREESC, SMART INNOVATION NORWAY, РІВНЕНСЬКА АЕС

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

Trening, trening, trening

- Ofte er treningsfokus på operatører, men prosjektene i cybersikkerhetssenteret indikerer treningsverdi fra:
  - Arbeide med prosjekter som omfatter reelle systemer samt operasjonell erfaring.
  - Peer-diskusjoner med "allierte" interessenter som utviklere og leverandører, CERTs, og myndighetsaktører.
  - Samarbeid med ekspertise på prosess- og menneskelige faktorer for å utvikle og informere om beste praksis og måter å jobbe på.

CybWin Project

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

- Utfør simulering av angrep på komponenter for å fastslå
  - Effekt av angrep og systematferd
  - Identifikatorer på angrep og relevante data
- Forskjellige IDS- og deteksjonssystemer blir brukt og evaluert
- Overordnet mål om å nå informert beste praksis på
- Responsprosedyrer
- Støtte prosesser (organisasjon)
- Opplærings- og kompetansekrav

AVINOR EUROCONTROL Statnett VTT KAIST

SECURENOK NTNU IFE

Finanisert av forskningsrådet

Tidslinje 2019-2022

Total budsjett:
28 millioner kroner

Statnett tester cyberangrep på mini-kontrollanlegg

- CybWin prosjekt støttet av Forskningsrådet
- Statnett samarbeider med KraftCERT og IFE
- Et isolert laboratoriet av et kontrollanlegg (mini-kontrollanlegg) til bruk for simulering av cyber-angrep og uttesting av sikkerhetsløsninger.
- Disse angrepsscenarioene inkluderer både SCADA-grensesnittet (IEC 104) og selve kontrollanlegget og stasjonsbussen (IEC 61850).
- Laboratoriet er unikt i Norge og bygget opp iht. erfaringer og råd fra NIST og NCCoE.

https://www.linkedin.com/feed/update/urn:li:activity:6810160705933713408/

Siv Hilde Houmb (PhD) • 1st
Senior Advisor Digital Security at Statnett SF
2d •

Statnett tester cyberangrep på mini-kontrollanlegg

Statnett samarbeider med KraftCERT og Institutt for Energiteknikk (IFE) i FoU-prosjektet CybWin. CybWin er et cybersikkerhetsprosjekt som støttes av Forskningsrådet. Statnett sitt fokus i prosjektet er å få etablert et isolert laboratoriet av et kontrollanlegg (mini-kontrollanlegg) til bruk for simulering av cyber-angrep og uttesting av sikkerhetsløsninger. Laboratoriet er unikt i Norge og bygget opp iht. erfaringer og råd fra det amerikanske sikkerhetsmiljøet hos National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE). NIST NCCoE er et verdensledende miljø innenfor cybersikkerhet og har bygget laboratorier og angrepsscenarioer for en rekke markedssegmenter, inkludert kraft. CybWin-prosjektet kobler også Statnett tettere til Norges ledende sikkerhetsmiljø, Center for Cyber and Information Security (CCIS) på NTNU Gjøvik.

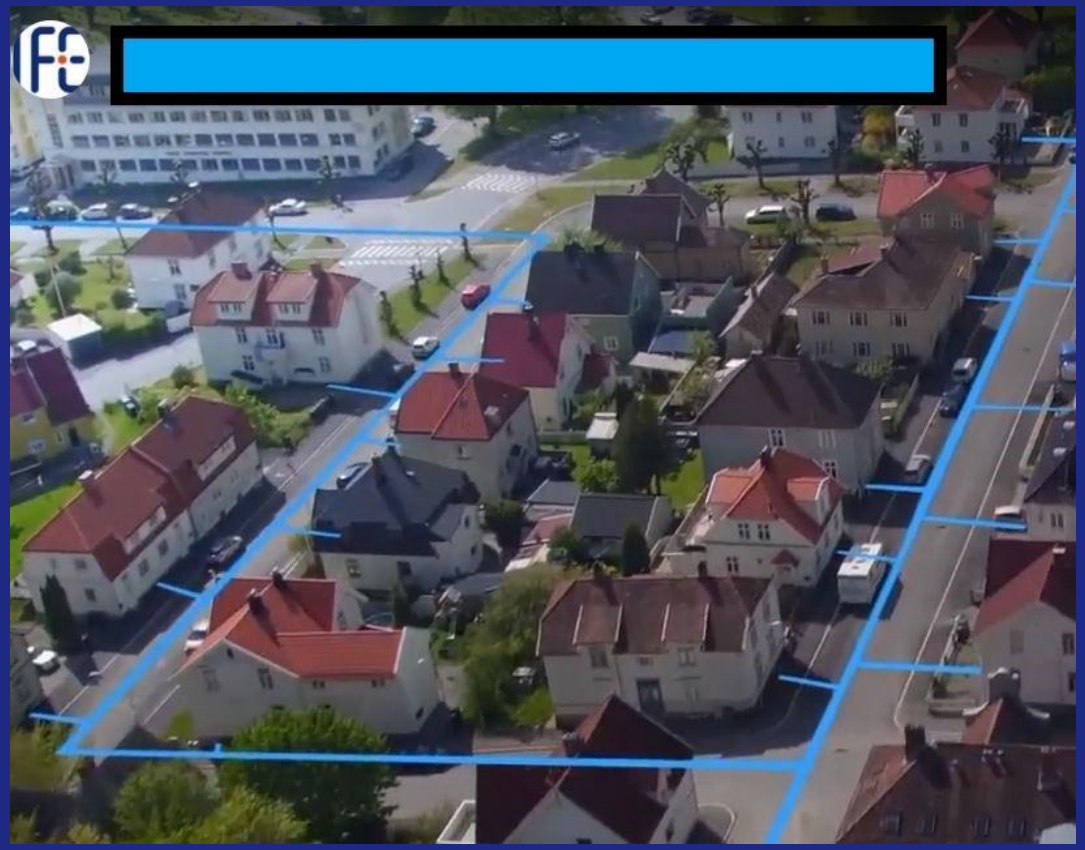
Laboratoriet er nå snart klart og da skal Statnett og KraftCERT kjøre angrepsscenarioene som er utviklet. Disse angrepsscenarioene inkluderer både SCADA-grensesnittet (IEC 104) og selve kontrollanlegget og stasjonsbussen (IEC 61850).

See translation

Sikkerhet er enkelt

Alt man trenger er å sørge for at **TEKNOLOGI**

- er bortimot umulig å hacke
- kontinuerlig oppdateres og patches slik at man ligger foran potensielle trusler
- ikke har avhengighet til andre systemer
- har påvirkningsmulighet fra et annet system
- Har tilstrekkelig redundans i infrastruktur, f.eks. nettverk, rutere, switcher, brannmurer
- helst ikke er tilkoblet internett…



Sikkerhet er enkelt

Og sørge for at **MENNESKENE**

- ikke gjør noe feil
- alltid er tro mot arbeidsgiver
- har nok kunnskap til å fungere som en barriere og ikke en medvirkende årsak
- ikke har noe imot å la være å ta snarveier for å nå et mål
- følger håndbøker og retningslinjer til punkt og prikke
- melder alle avvik perfekt og tide
- alltid er oppdatert på på seneste trusler og sårbarheter

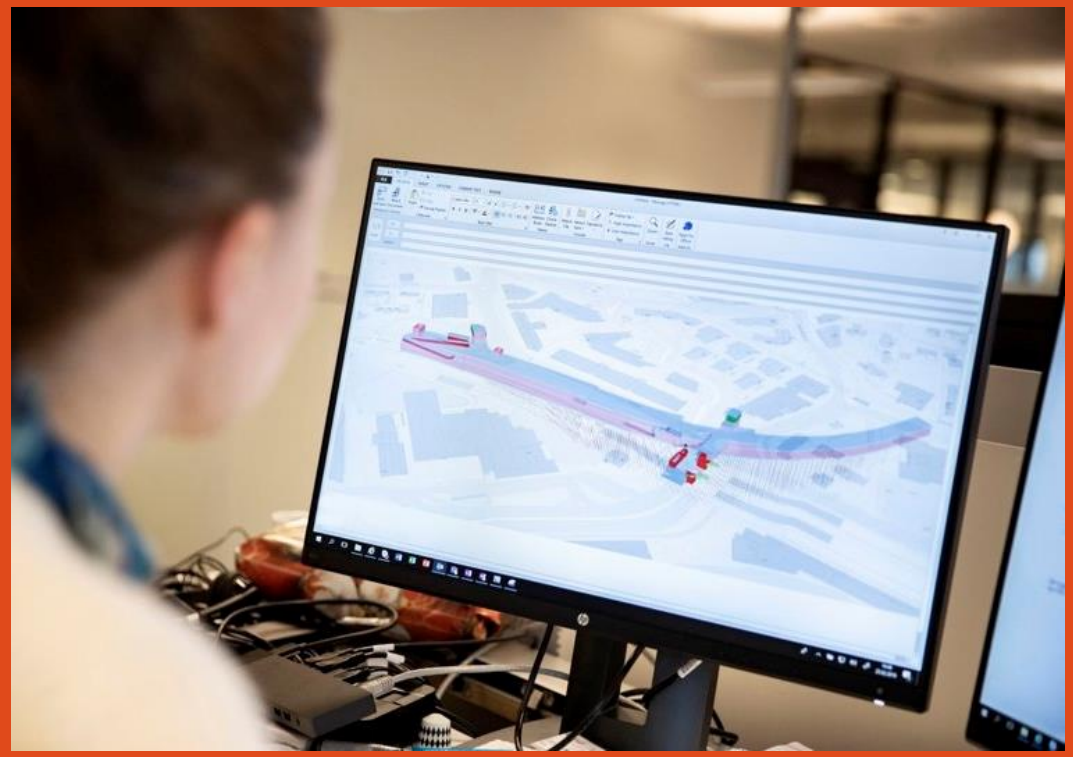


Foto: Thomas Haugersveen

Sikkerhet er enkelt

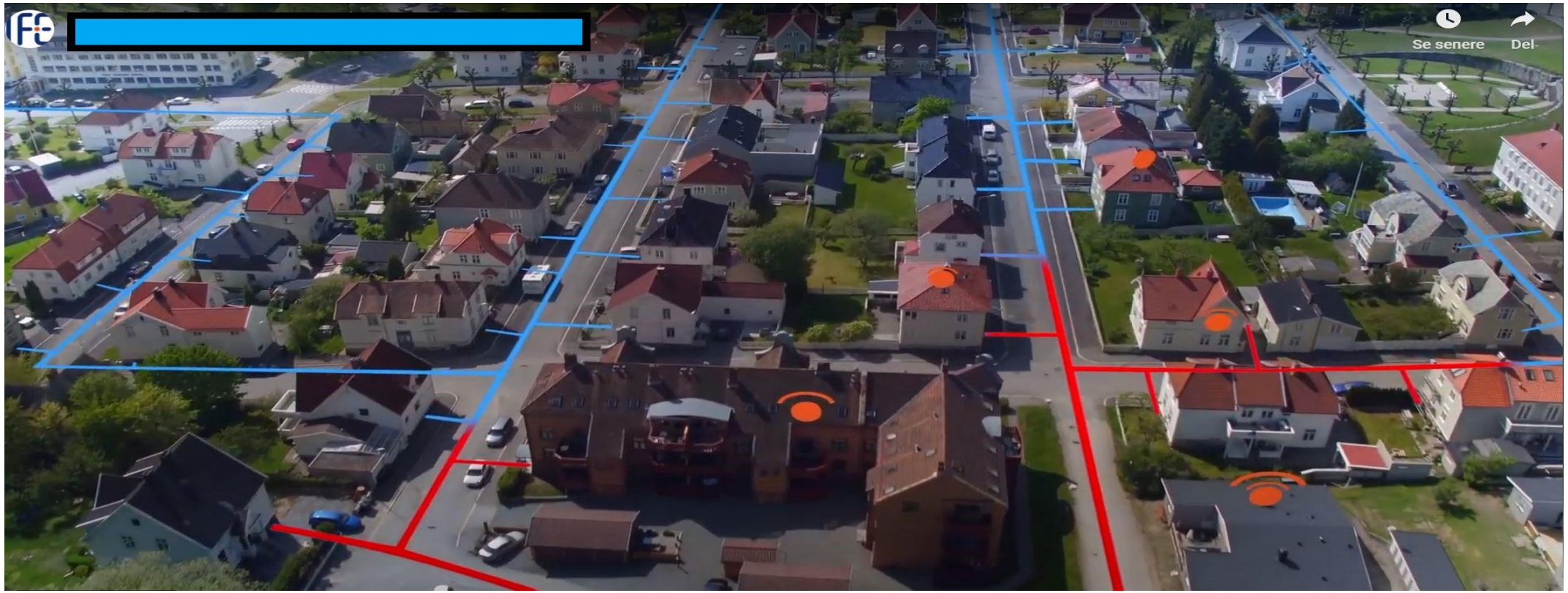
Og sørge for at ORGANISASJONEN

- Har alle prosedyrer på plass for å
  - oppdatere og patche systemer
  - koordinere med andre aktører
  - besørge at standarder etterfølges
- Trener beredskapsorganisasjonen
- Trener også på Cyber sikkerhet
- Kurser spesialister
- Har klare roller og ansvarsfordelinger
- Har egen SOC eller kjøper SOC-tjenester
- Setter av tilstrekkelige midler til
  - oppdatering av systemer og mennesker
  - knytte til seg nødvendige eksperter
- Jobber systematisk alle ledd hele tiden

Problemet er bare at …

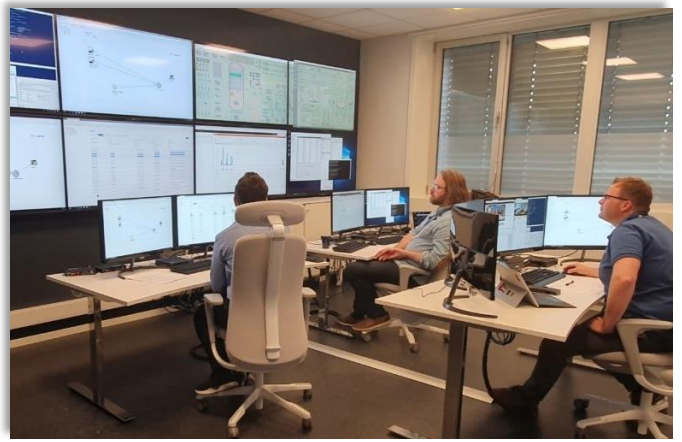
- Mesteparten av infrastruktur allerede eksisterer
  - Er bygget med fokus på safety, har prosedyrer designet for å besørge safety, og eksisterer i organisasjoner som er skrudd sammen for safety
- Cybersikkerhet er i kontinuerlig bevegelse
  - Trusselaktørene er mange og vanskelig å forutsi
  - Trusler utvikler seg fortere enn forsvarsmekanismer
- Kunnskap er mangelvare
  - Antallet som uteksamineres med datasikkerhetsgrader er en brøkdel av behovet
  - Behovet vokser langt raskere enn inntaket av nye studenter
  - Mangel på en “tjeneste/vare” driver prisene opp

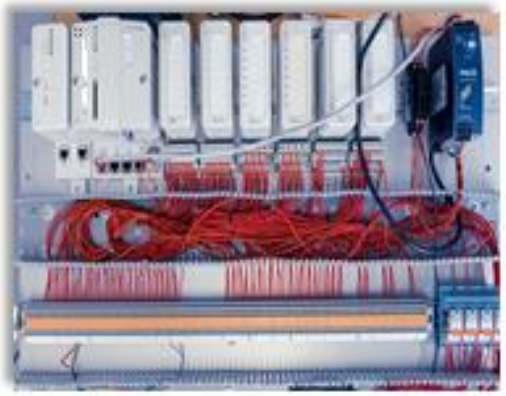
Så hendelser vil inntreffe …

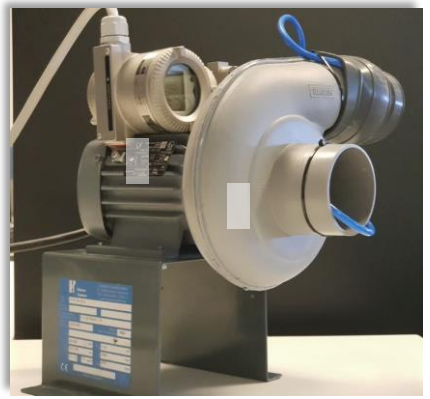


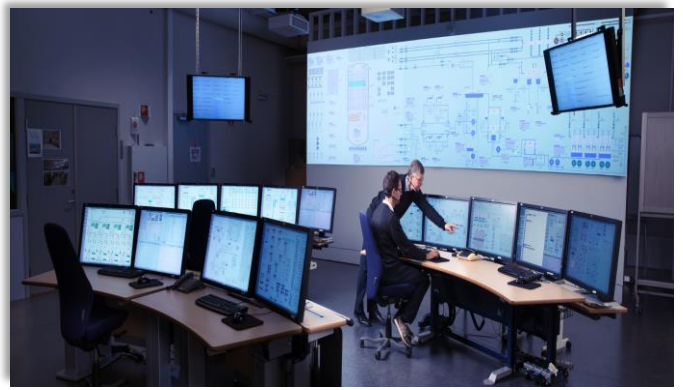
What happens in control room of an industrial plant/process during a cyber-attack?

- Hardware-in-the-loop simulation of power plant
- Man-In-The-Middle attack on turbine pressure control system
  - generally not classified as a safety-critical system
- Impact on
  - systems and plant process
  - human – operators and security team









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

PLC: Programmable Logic Controller

Felles “Trussel -landskap” webinar 29 April

- Mellom 4 prosjekter:
  - Rivne NPP – Cybersecurity project Ukrainian NPP
  - CybWin – operational cyber security in power grids, aviation and nuclear
  - RECYCIN – cyber security collaboration research and education – USA and Norway
  - Halden HTO Project – Chapter 7 Cyber Security for Main Control Room

- 49 deltagere fra 7 land og 17 organisasjoner.
  - F.eks: USNRC, INL, EPRI, Virginia Tech, Snerdi, IRSN, KraftCERT, Statnett

Input from joint “Threat picture” webinar April 29th

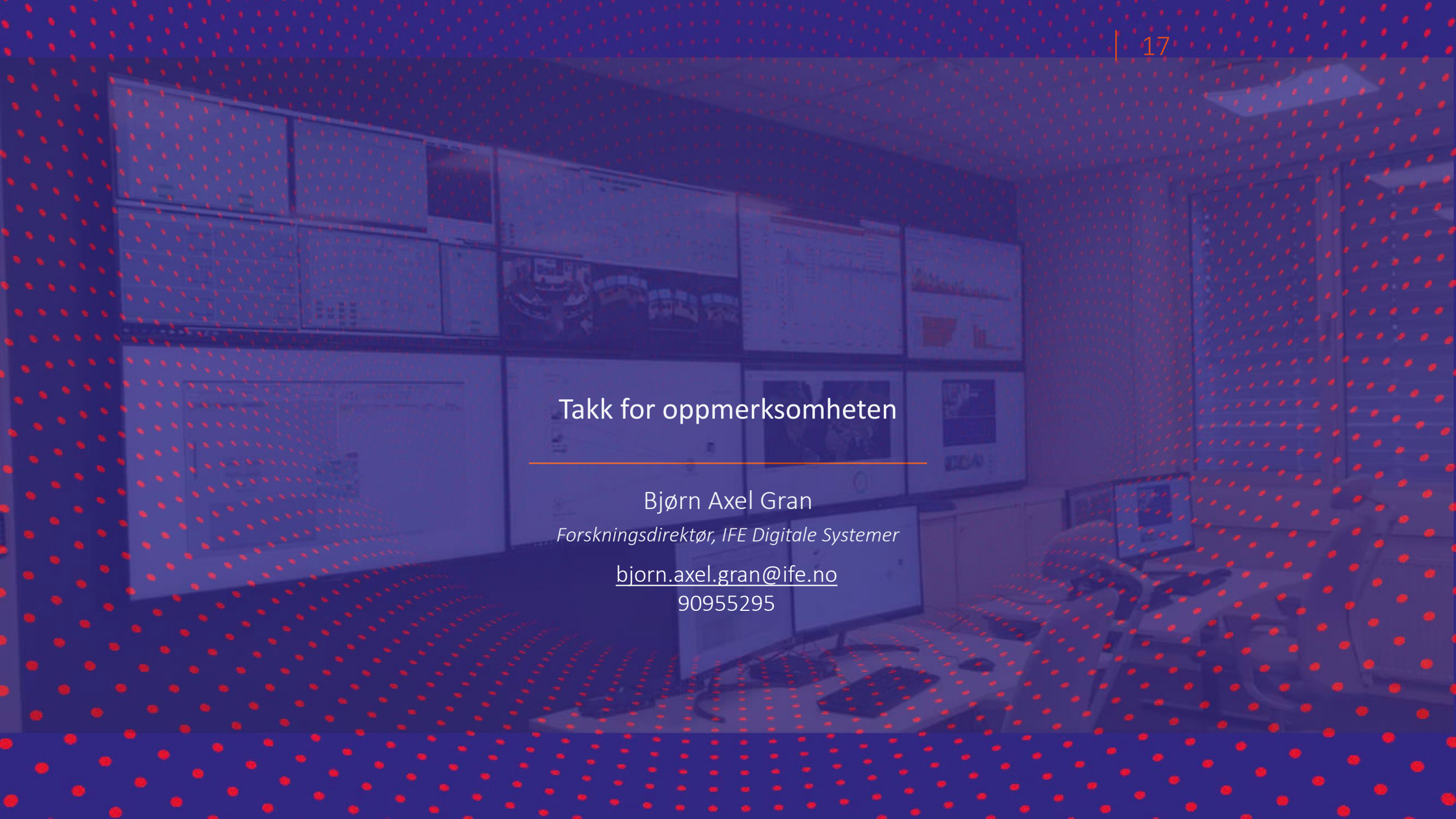
- Høydepunkter
  - IRSN og IFE delte informasjon om trussel-landskapet innen kjernekraft
  - Statnett delte trussel-landskapet til Digital kontrollstasjon og overgangen fra analoge til digitale kontrollsystemer
  - INL presenterte rollen til operatører i cyberhendelser som en del av «forsvar i dybden»
  - Virginia Tech presenterte sin utdanning innen cybersikkerhets
- Kommentarer gitt:
  - Gjør operatører til prosesseksperter, men gi dem kunnskap om cyber- og cyberscenarier.
  - Operatører var frustrerte da systematferden de opplever i cyberscenarier "ikke var mulig".
  - Gode ressurser: MITER ATT&CK, Shodan, Kaspersky (og andre sikkerhetsselskapsressurser)

Trening, trening, trening

- Cyber Center muliggjør tilkobling av laboratorier og simulatorer
- Å bruke kunnskap om systematferd under cyberforhold og replikere dette i simulatorer
- Operatører i Kontrollrom (sikkerhet) kan samhandle med SOC-personell under cyber-hendelser
  - Trene under realistiske forhold
  - Teste og utvikle prosedyrer
  - Evaluere prosedyrer og menneskelig ytelse

Input from joint “Threat picture” webinar April 29th

- Rivne NPP: https://ife.no/en/project/establishment-of-ukrainian-qualification-body-and-test-bed-for-qualification-of-personnel-performing-ultrasonic-ut-and-eddy-current-et-testing-of-vver-reactor-pressure-vessel-rpv/
- CybWin project: https://ife.no/prosjekt/cybwin-cybersecurity-platform-for-assessment-and-training-for-critical-infrastructures-legacy-to-digital-twin-2/
- RECYCIN project: https://ife.no/en/project/recycin-reinforcing-competence-in-cybersecurity-of-critical-infrastructures-a-norway-us-partnership/
- Halden HTO: https://ife.no/en/the-halden-project-continues-new-period-in-2021/
- And more the information about some of our labs:
  - Hammlab: https://ife.no/en/laboratory/hammlab/
  - Cybersecurity Center: https://ife.no/en/laboratory/cybersecurity-centre/



Takk for oppmerksomheten

Bjørn Axel Gran

Forskningsdirektør, IFE Digitale Systemer

bjorn.axel.gran@ife.no

90955295