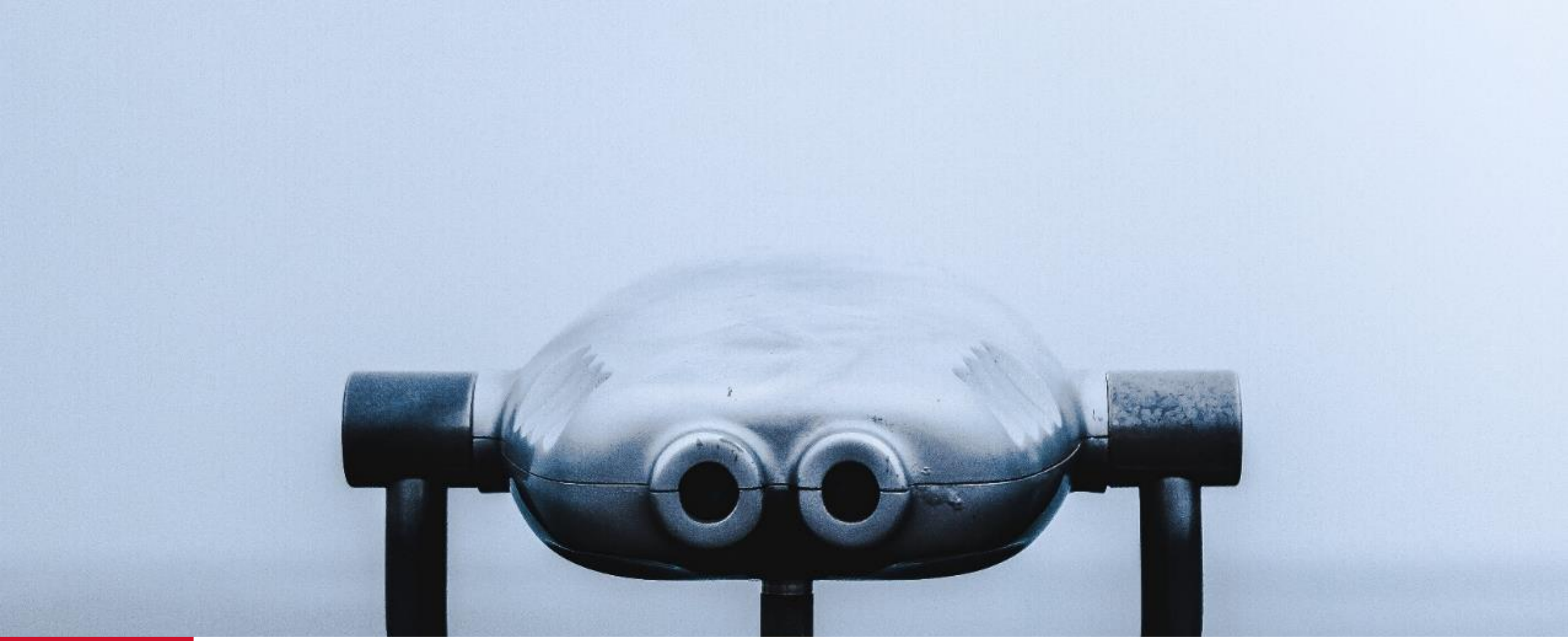


Deteksjon av hendelser i OT

Løsninger og utfordringer

Jon-Martin Storm

Digital sikkerhet, NVE

23.10.2024, Nettalliansen

Tillitssliden / aka please trust me

HØGSKOLEN I BERGEN

UNIVERSITETET I BERGEN

BI

UNIVERSITETET I OSLO

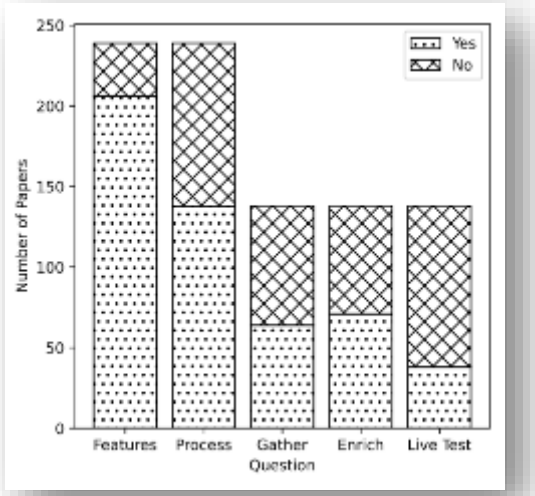
- 2+ år kraftsystemanalyse
- 8 år Sikkerhet og Beredskap
  - Driftskontroll (OT-sikkerhet)
  - IKT (IT-sikkerhet)
  - KSI (Kraftsensitiv informasjon)
  - Generell og fysisk

Hvorfor og hva slags forskningsarbeid?

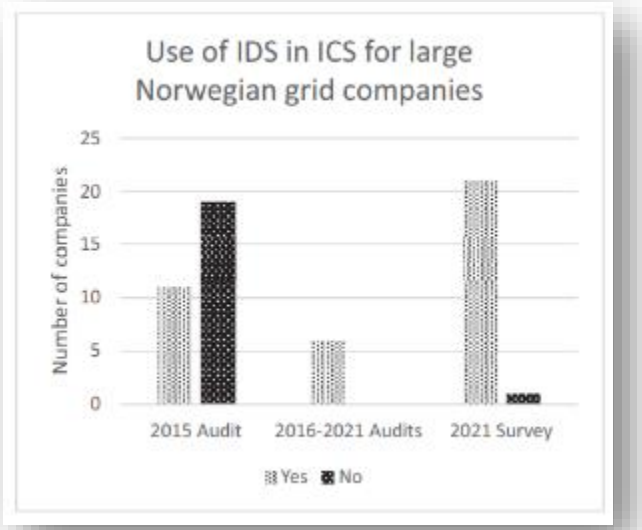
Photo by Sigmund on Unsplash

NVE

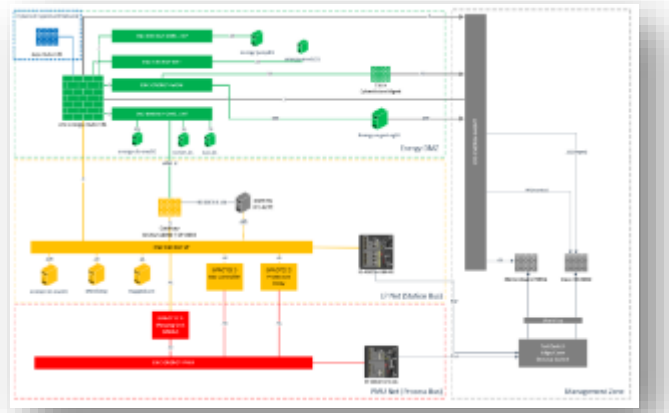
Litteraturstudie



Etterlevelse?



Eksperimenter



Case studie

Suksess!

Deteksjon 101

UNIVERSITETET
I OSLO

Photo by James Sloan on Unsplash

Sikkerhetsovervåkning og deteksjon

«Sikkerhetsovervåkning og deteksjon er aktiviteter som **skal avdekke illegitime handlinger** gjennom å **prosessere og analysere metadata og data om informasjonssystemets bruk**.»

Bergsjø, Windvik, Øverlier - Digital sikkerhet (universitetsforlaget.no)

Oppdage / detektere

Hvordan oppdager vi angrep?

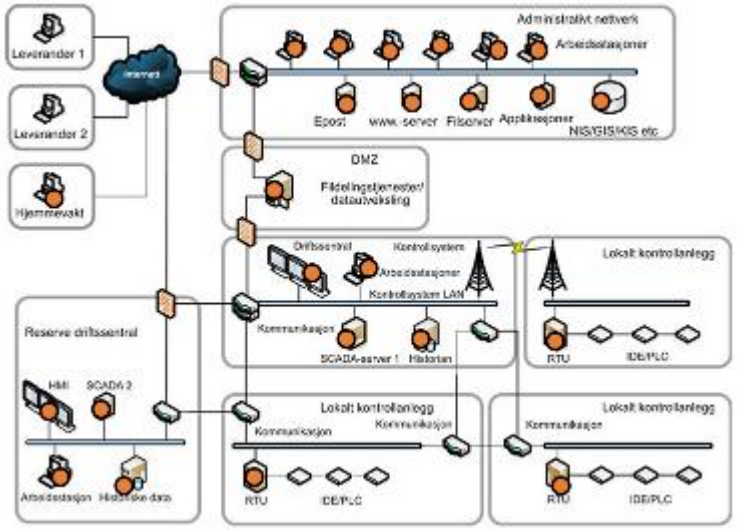
- Hente inn data
- Prosessere
- Handle

Photo by Louis Reed on Unsplash

IDS – Intrusion Detection System

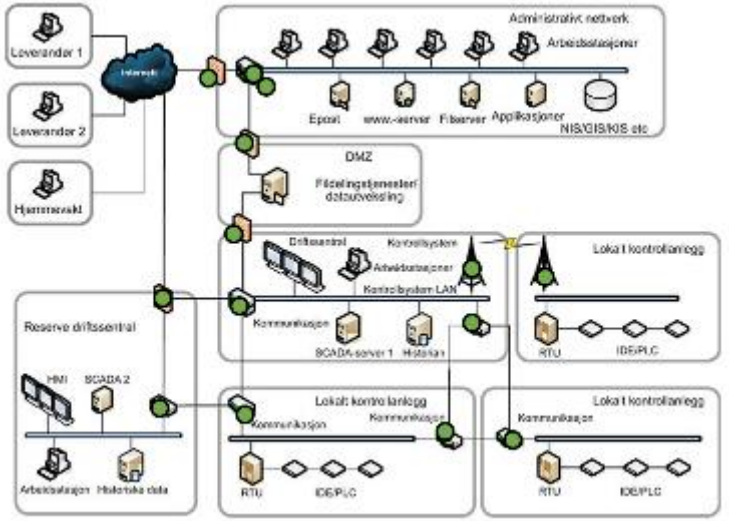
Endepunkt (Host)

- Sensorer på pcer/enheter
- Eksisterende logger, egen app



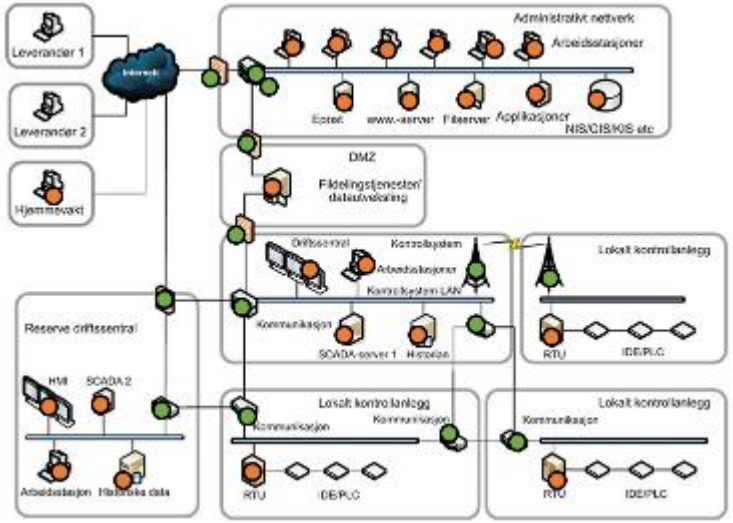
Nettverk (Network)

- Analyserer nettverksdata
- Speilport (SPAN), avtapping (tap)



Hybrid (Hybrid)

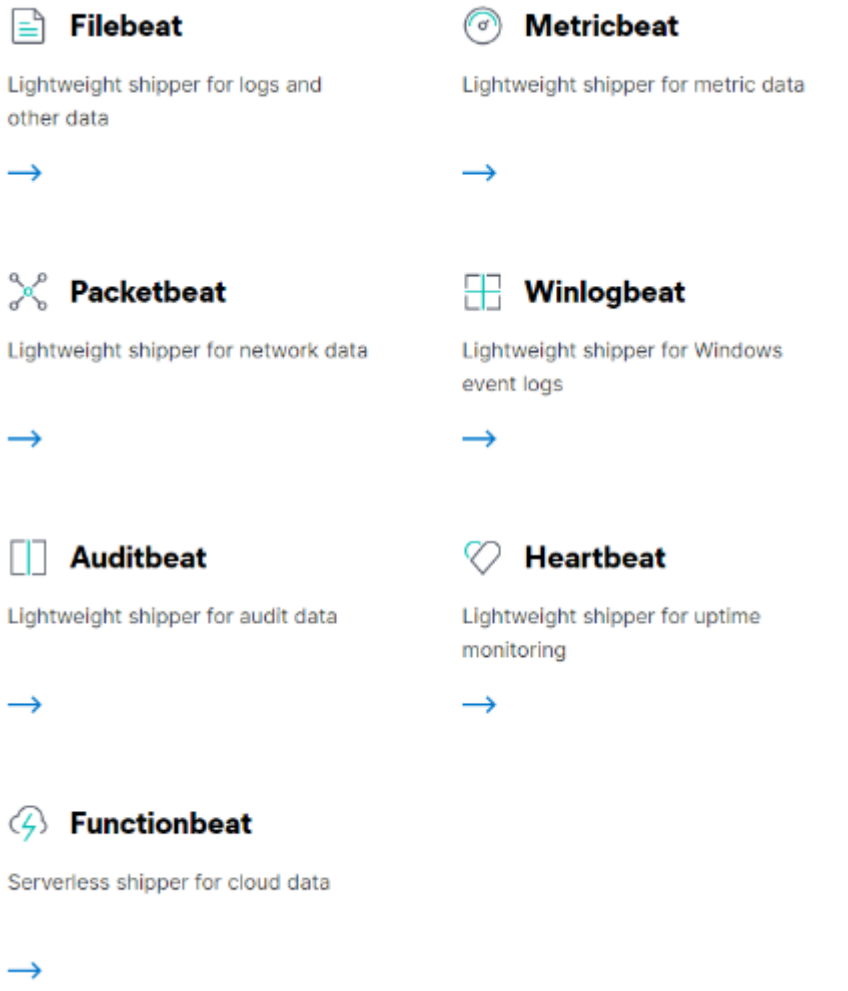
- Kombinasjon av begge



Hente inn data

Konkrete eksempler

- Logfiler på endepunkt (PLC, smart sensor, pc)
  - Syslog
  - Windows Event log
  - Sysmon filer
- Opptak av nettverkstrafikk
  - PCAP
  - Nettverk tap
  - SPAN port



Beats: Data Shippers for Elasticsearch | Elastic

Prosessere og analysere

Regelbasert

- Har et predefinert sett med regler som kildene sammenlignes med
- Ved treff så varsles det
- Bruk av signaturer, for eksempel en Hash
- Kan kun detektere på det vi kjenner til

Anomalibasert

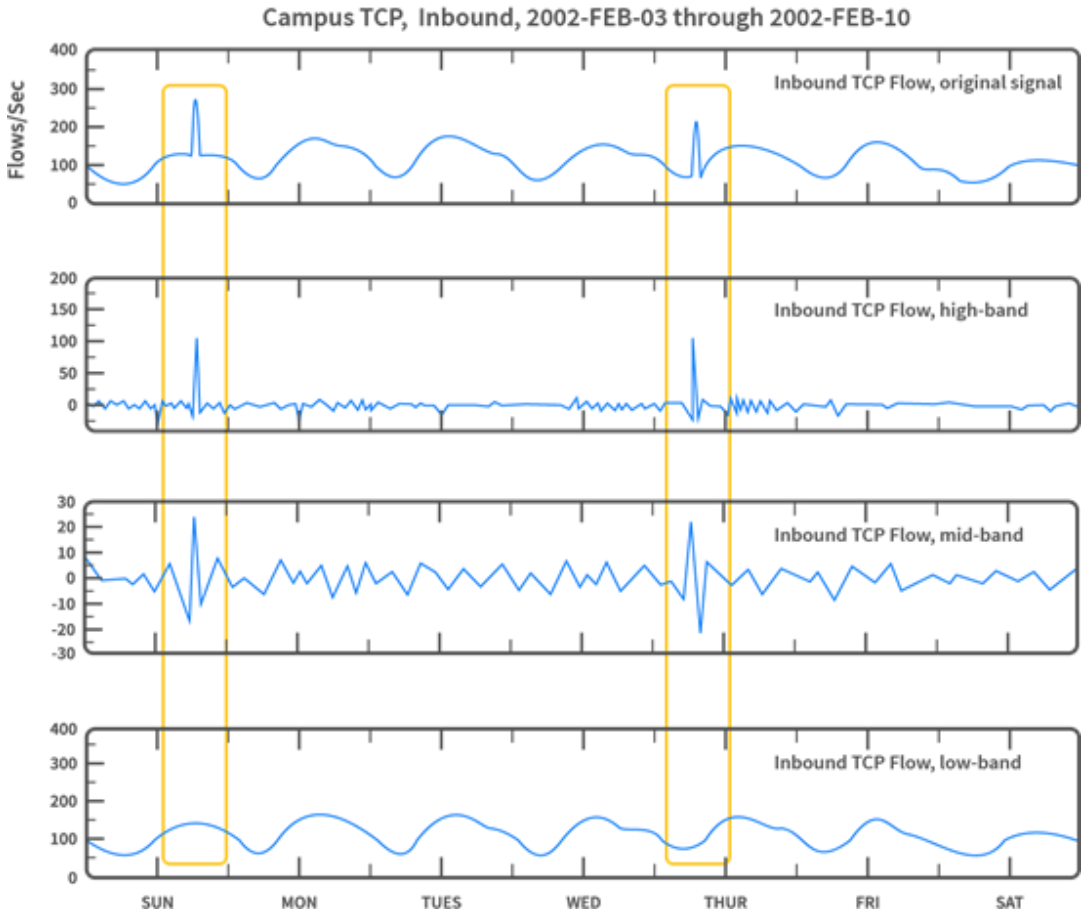
- Opererer ut ifra en normaltilstand på nettverket/systemene, ofte kalt en Baseline
- Sammenligner informasjonen med denne normaltilstanden og varsler på det som er «unormalt»
- Kan finne hittil ukjente angrep
- Har ofte en del falske positive, altså det er mye unormalt som er normalt

Eksempel – Prosessere og analysere

Signatur i Snort – Detektere TCP SYN flom

```
alert
tcp any any -> 192.168.10.5 443
(
msg: “TCP SYN flood”;
flags:!A;
flow: stateless;
detection_filter: track by_dst,
count 70, seconds 10;
sid:2000003;
)
```

Anomali

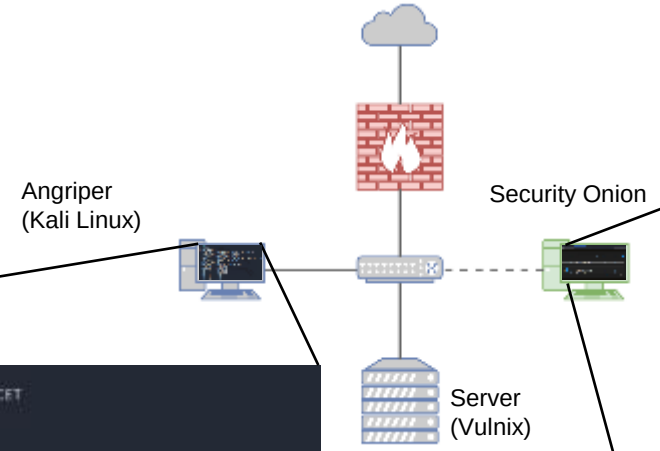


Kilde: https://www.flowmon.com/en/blog/science-of-network-anomalies

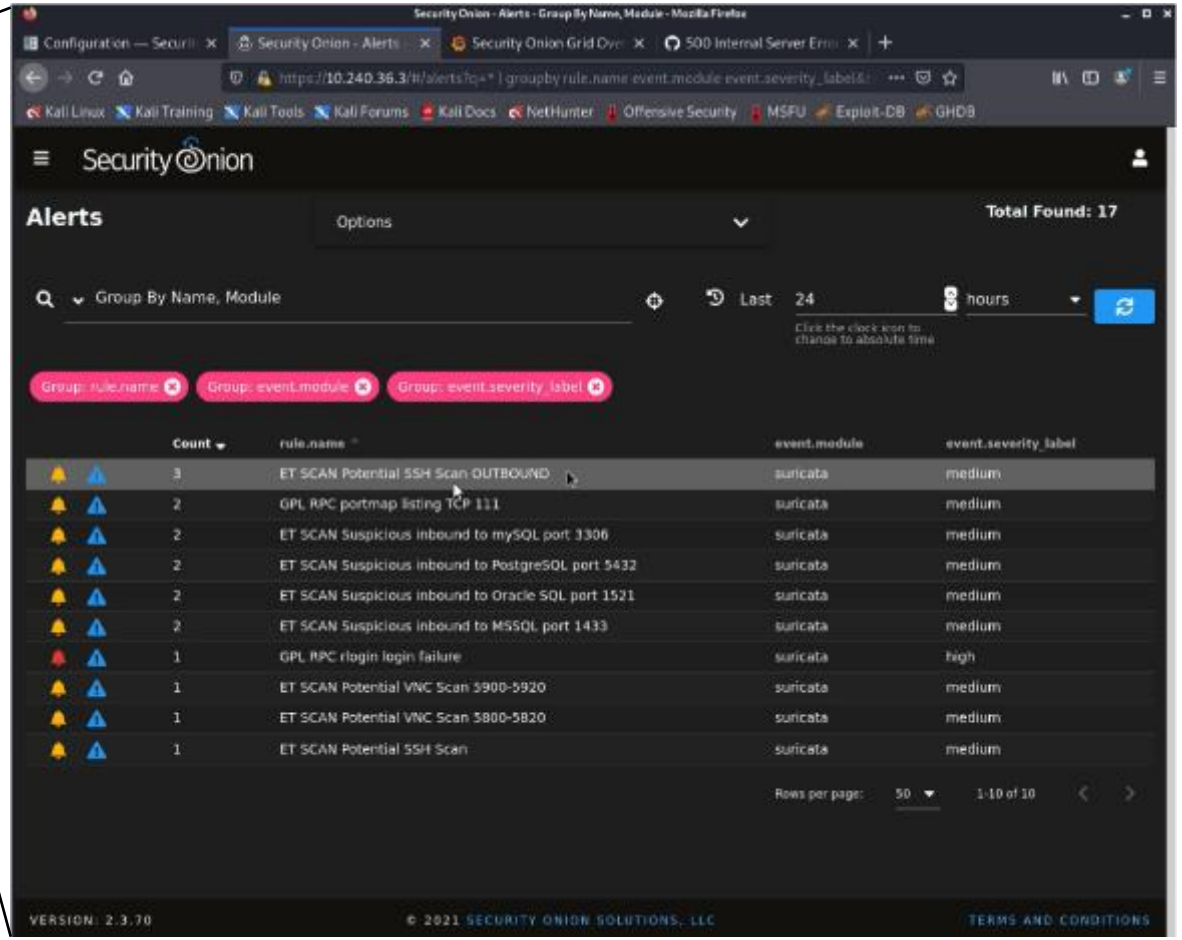
Samle inn og overvåke alarmene

Kilde: https://www.youtube.com/watch?v=cUP_ZRn5rro

Eksempel Security Onion




```
┌──$ nmap -sC -sV 10.66.66.3
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-14 15:15 CET
Nmap scan report for 10.66.66.3
Host is up (0.00027s latency).
Not shown: 988 closed ports
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 10:cd:9e:a0:e4:e0:30:24:3e:bd:67:5f:75:4a:33:bf (DSA)
|   2048 bc:f9:24:07:2f:cb:76:80:0d:27:a6:48:52:0a:24:3a (RSA)
|_  256 4d:bb:4a:c1:18:e8:da:d1:82:6f:58:52:9c:ee:34:5f (ECDSA)
25/tcp   open  smtp       Postfix smtpd
|_smtp-commands: vulnix, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8
BITMIME, DSN,
|_ssl-date: 2021-11-14T14:15:47+00:00; 0s from scanner time.
79/tcp   open  finger     Linux fingerd
|_finger: No one logged on.\x0D
110/tcp  open  pop3       Dovecot pop3d
|_pop3-capabilities: UIDL PIPELINING STLS RESP-CODES CAPA SASL TOP
|_ssl-date: 2021-11-14T14:15:47+00:00; 0s from scanner time.
111/tcp  open  rpcbind    2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/tcp6  nfs
|   100003  2,3,4       2049/udp   nfs
|   100003  2,3,4       2049/udp6  nfs
|   100005  1,2,3      34470/tcp   mountd
|   100005  1,2,3      39696/tcp6  mountd
```



Erfaringer fra deteksjon i OT

Bilde: NVE

Litteraturgjennomgang

Photo by John-Mark Smith on Unsplash

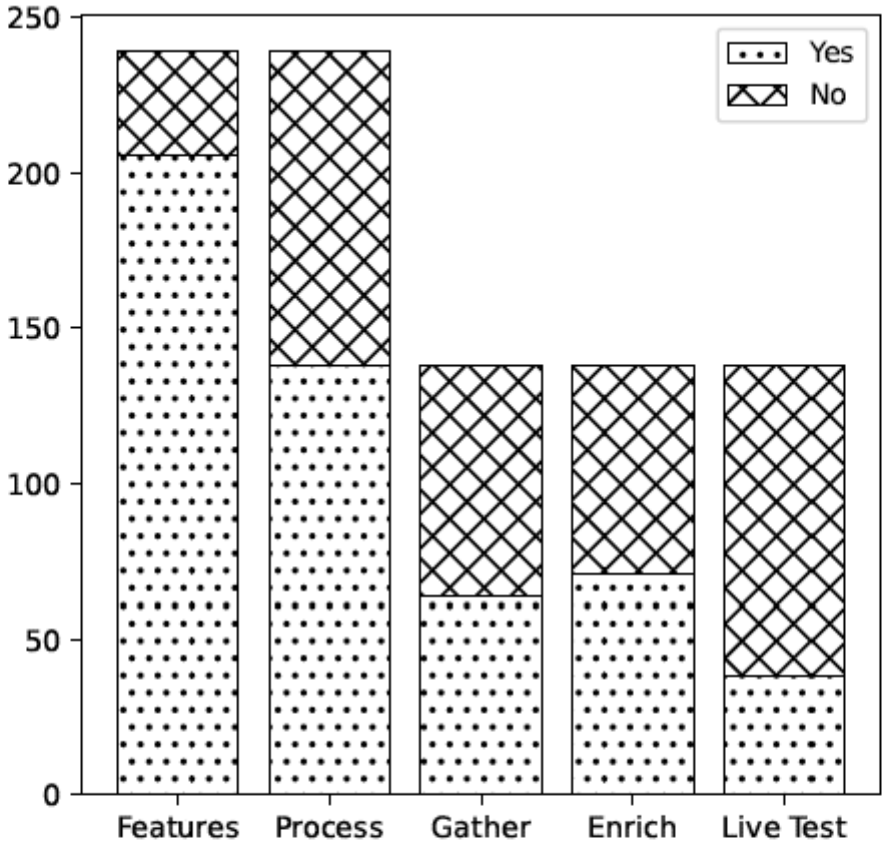


Fig. 1: Overview of the answers from the surveyed articles. This figure shows the number of papers; that address features of ICS in the proposed detection method, where the proposed detection method is designed to use data from a physical process that explain from where and how they gather physical process data, where the process data is enriched with other information sources and where the method has been tested on a system in operation or live test environment.

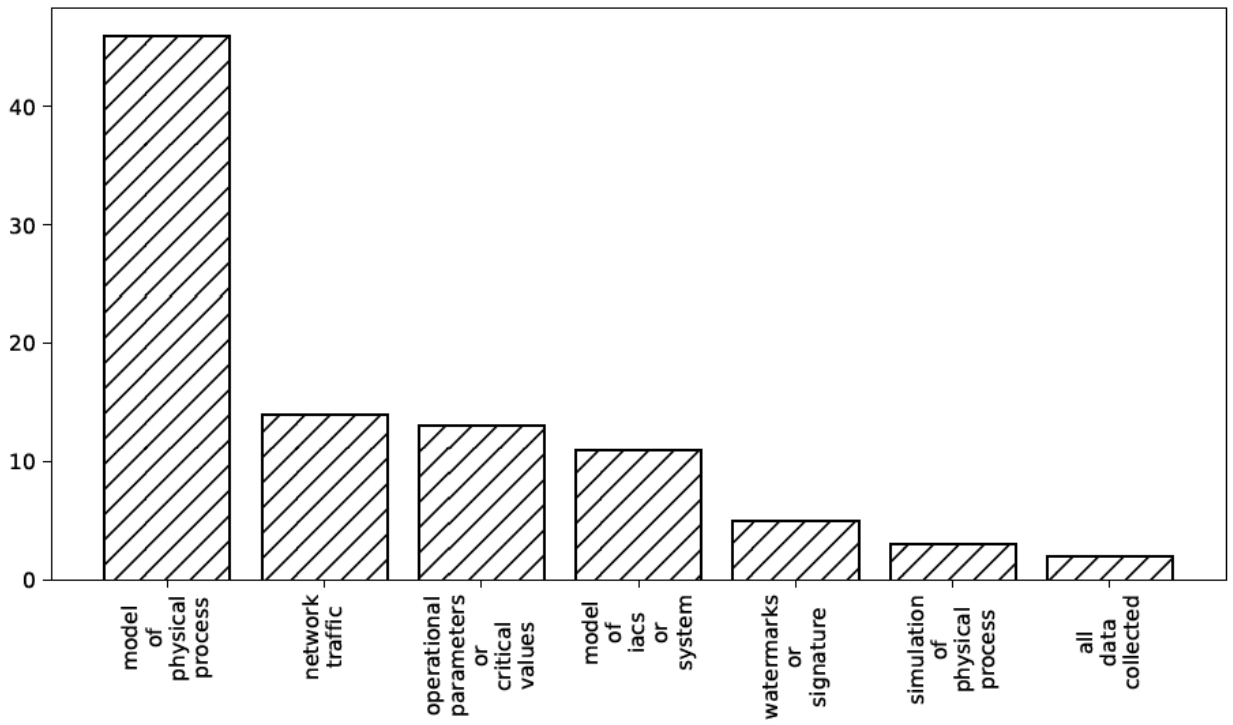


Fig. 6: An overview of other information sources used if the proposed detection method is designed to use process data, and also enriches the process data with other information sources.

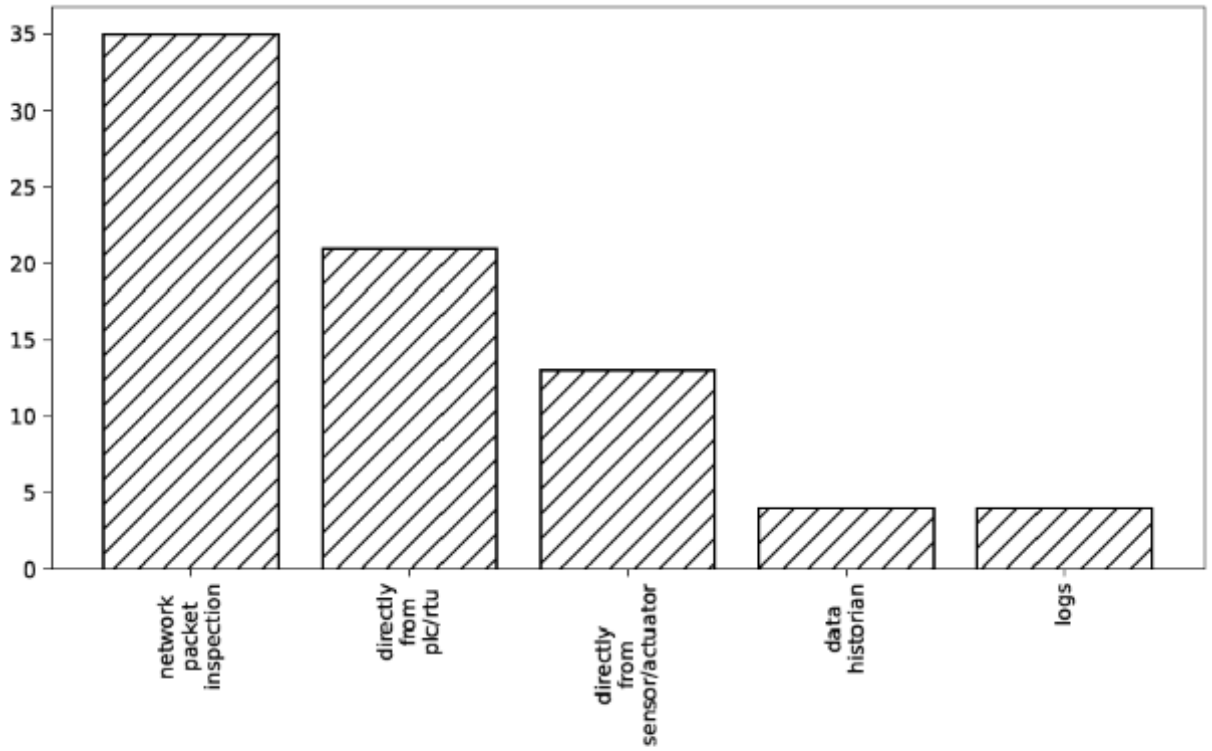


Fig. 5: An overview of where and how do the survey papers gather or propose to collect physical process data if they do.

Hjelper det med krav?

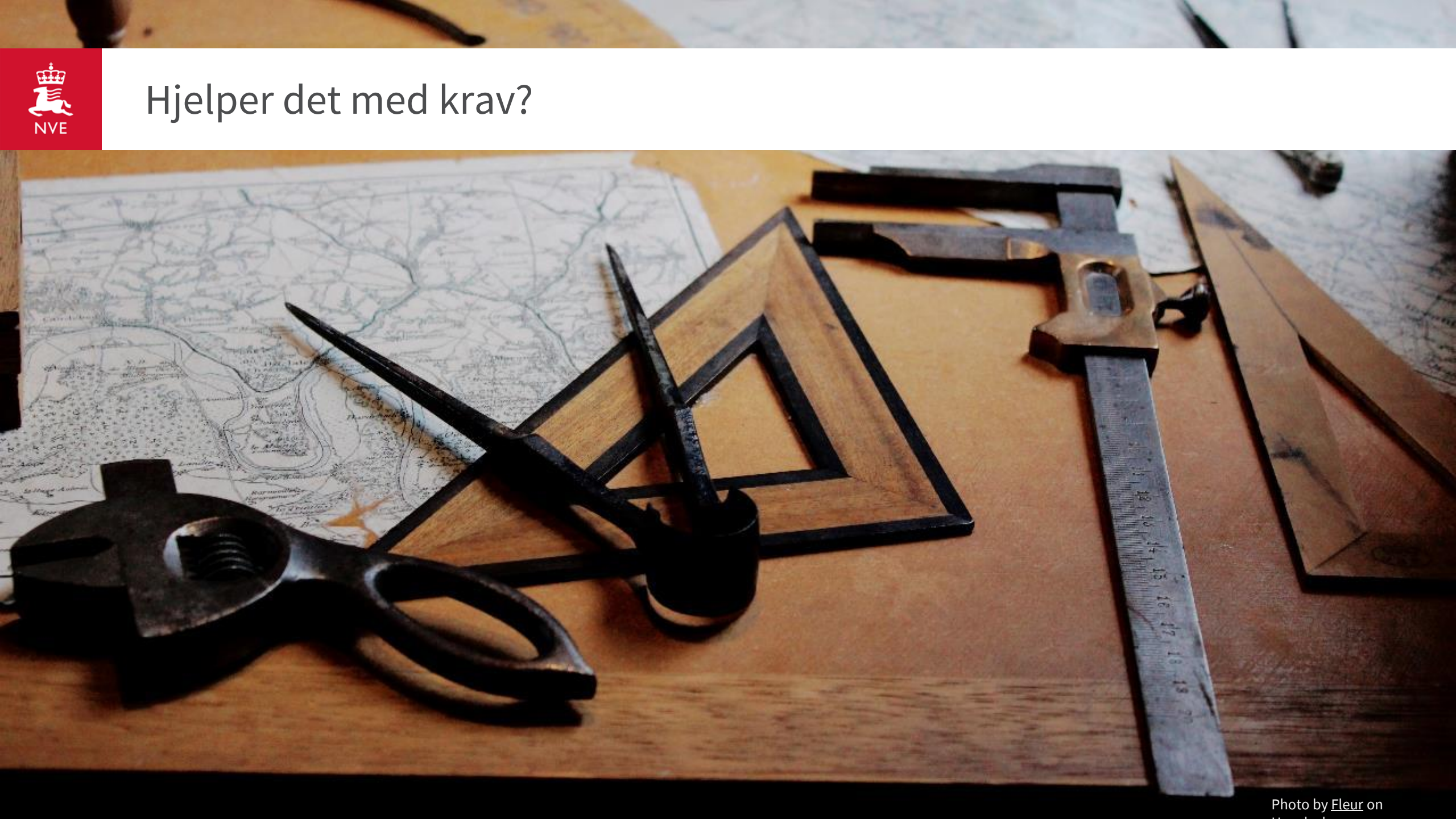
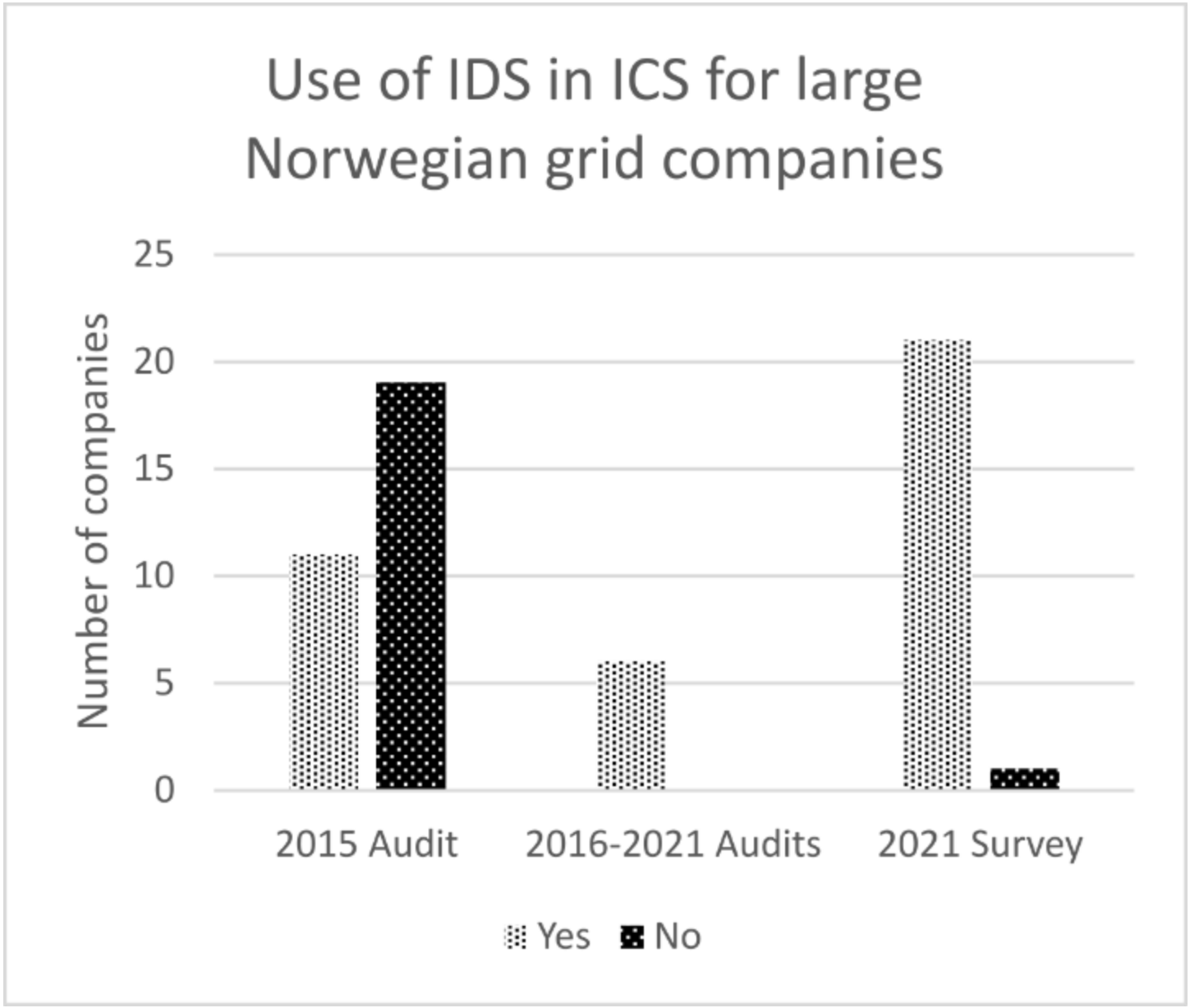
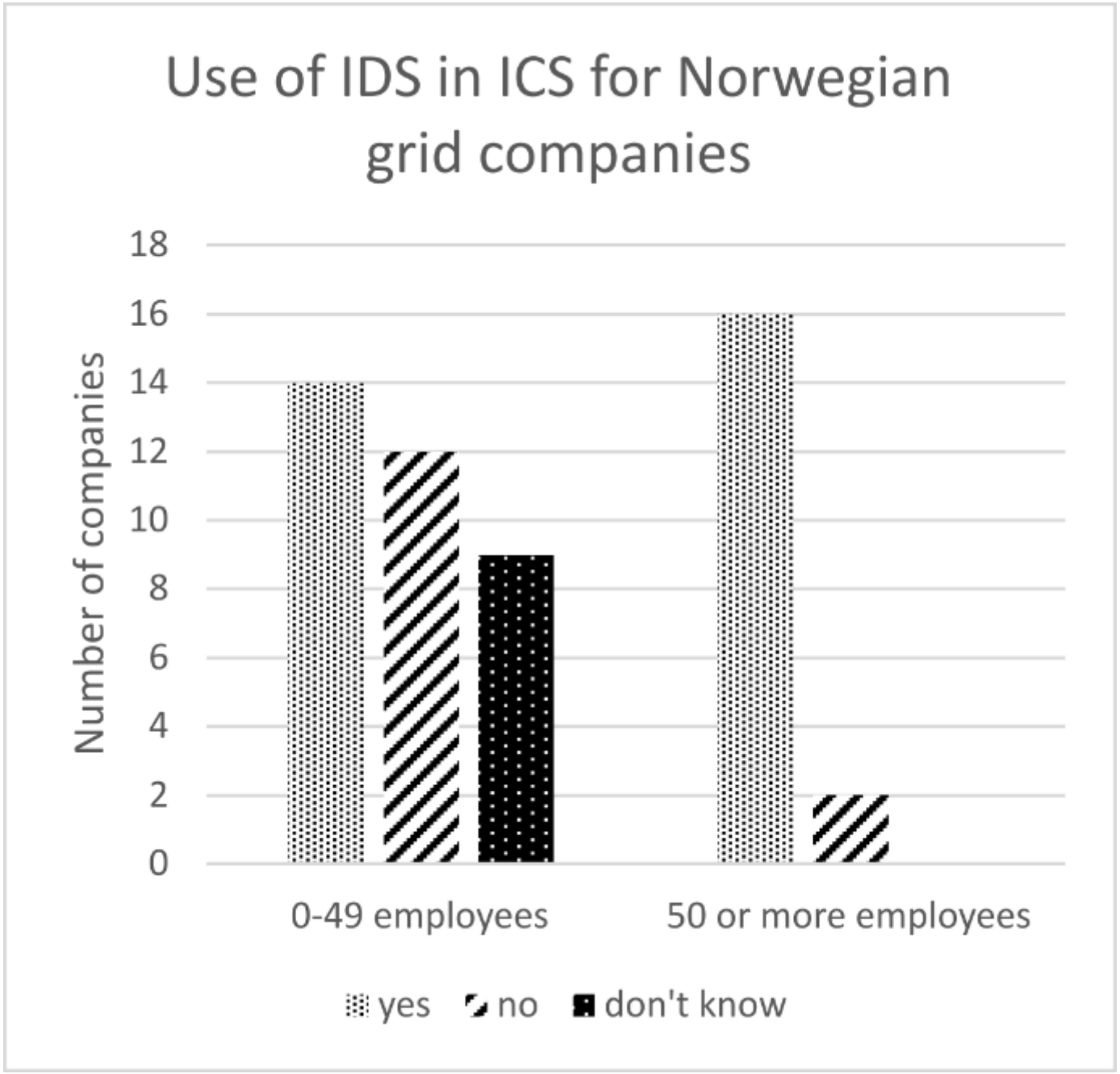


Photo by Fleur on


Use of IDS in ICS for large Norwegian grid companies
Number of companies
25
20
15
10
5
0
2015 Audit
2016-2021 Audits
2021 Survey
Yes
No


Use of IDS in ICS for Norwegian grid companies
Number of companies
18
16
14
12
10
8
6
4
2
0
0-49 employees
50 or more employees
yes
no
don't know

Barrierer for implementering

Foto: NVE/Knut Ove Hillestad

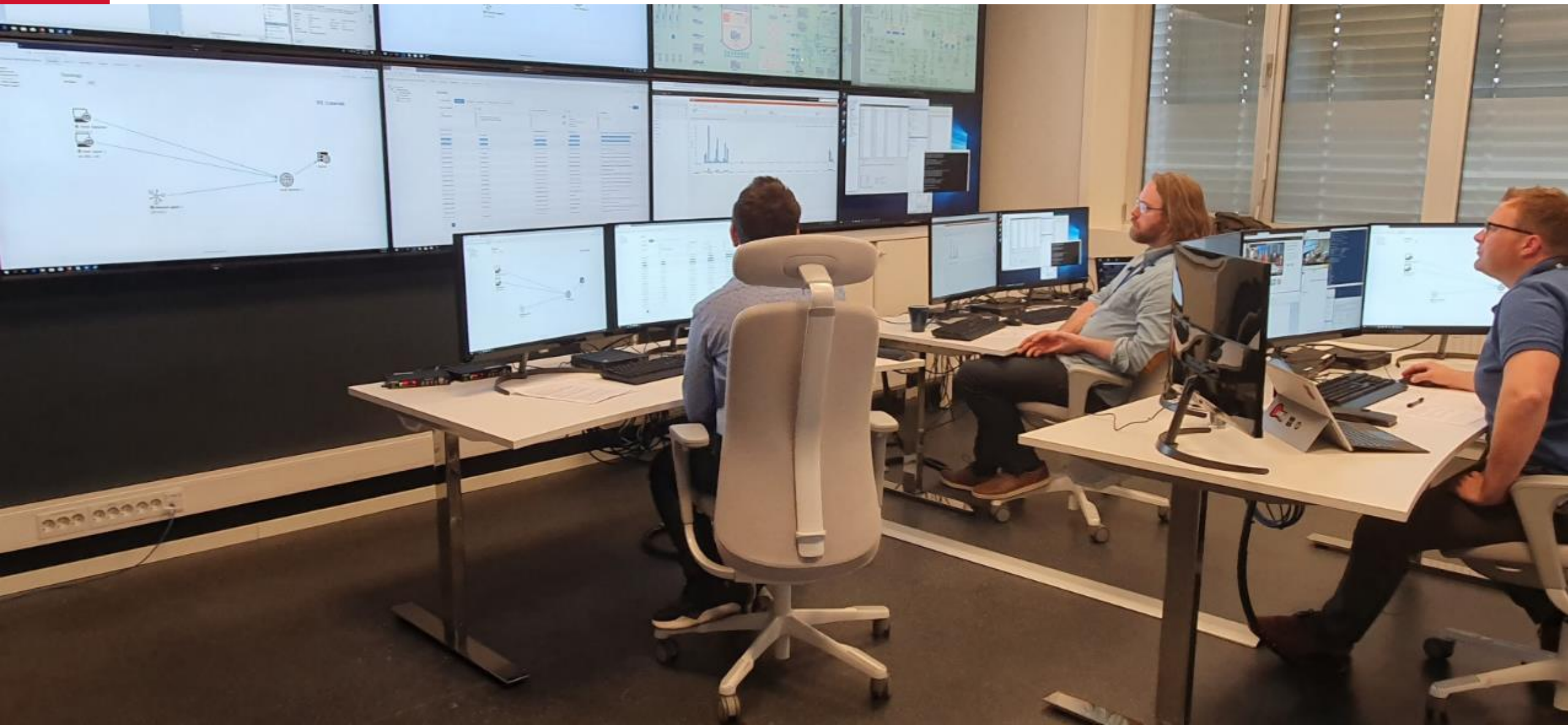
Funn

- Hva mener sikkerhetsfolka i kraftselskap er deteksjon i OT?
  - For det meste andre tiltak enn IDS
- Er mangelen på live-testet IDS for ICS i forskningen en barriere for å implementere deteksjon i OT i kraftselskapene?
  - Ingenting tyder på dette
- Hva er de største barrierene for implementering av deteksjonskontroller i OT hos de vi spurte?
  - Mangel på tid og menneskelige ressurser

Endelig det praktiske

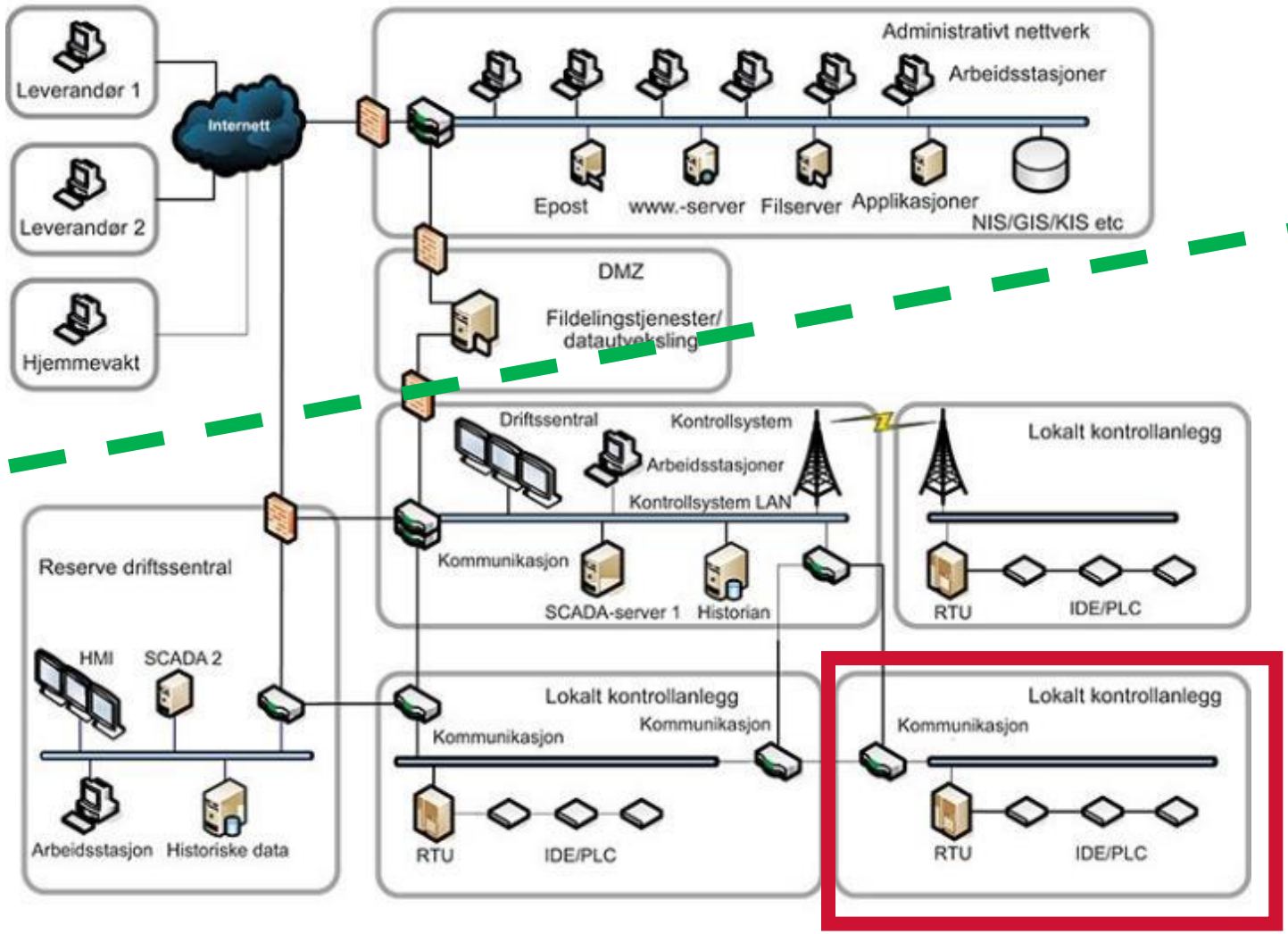
Photo by Jakob Owens on Unsplash

Lab ved IFE i Halden

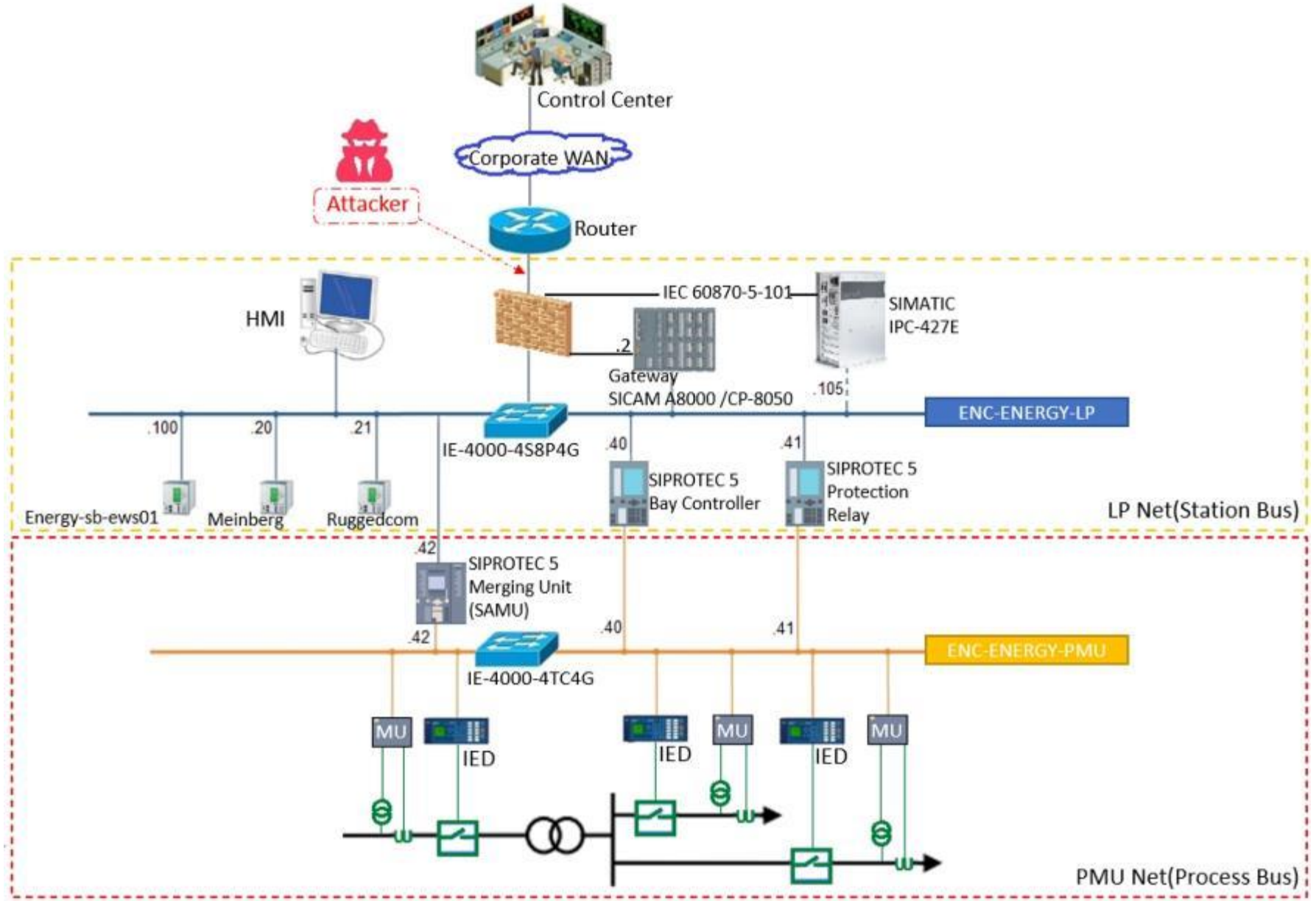


Transformatorstasjon

IT

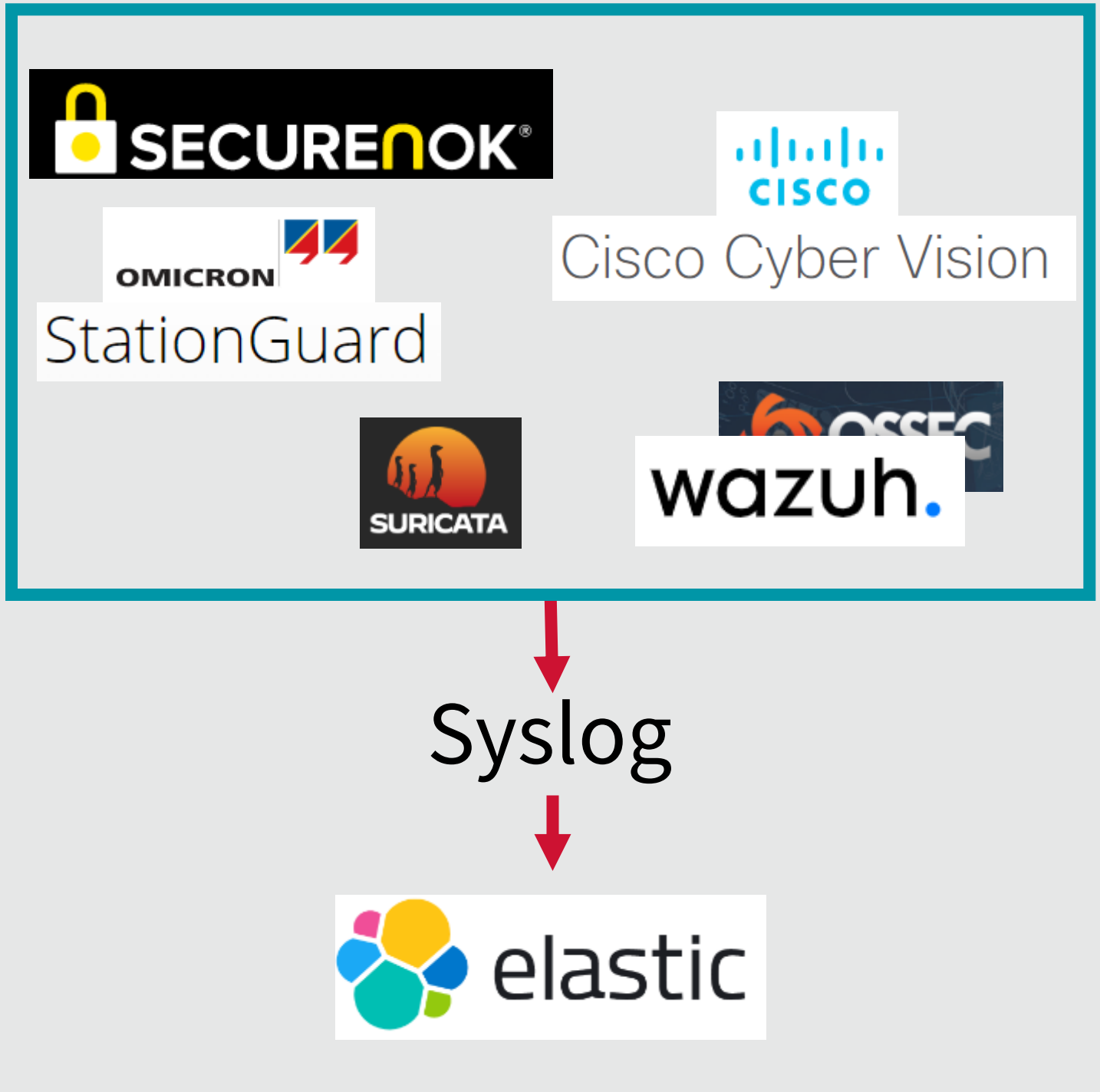

Leverandør 1
Leverandør 2
Hjemmevakt
Internett
Administrativt nettverk
Arbeidsstasjoner
Epost
www.-server
Filserver
Applikasjoner
NIS/GIS/KIS etc
DMZ
Fildelingstjenester/
datautveksling
Driftssentral
Kontrollsystem
Arbeidsstasjoner
Kontrollsystem LAN
Kommunikasjon
SCADA-server 1
Historian
Lokalt kontrollanlegg
RTU
IDE/PLC
Reserve driftssentral
HMI
SCADA 2
Arbeidsstasjon
Historiske data
Lokalt kontrollanlegg
Kommunikasjon
Kommunikasjon
RTU
IDE/PLC
Lokalt kontrollanlegg
Kommunikasjon
RTU
IDE/PLC

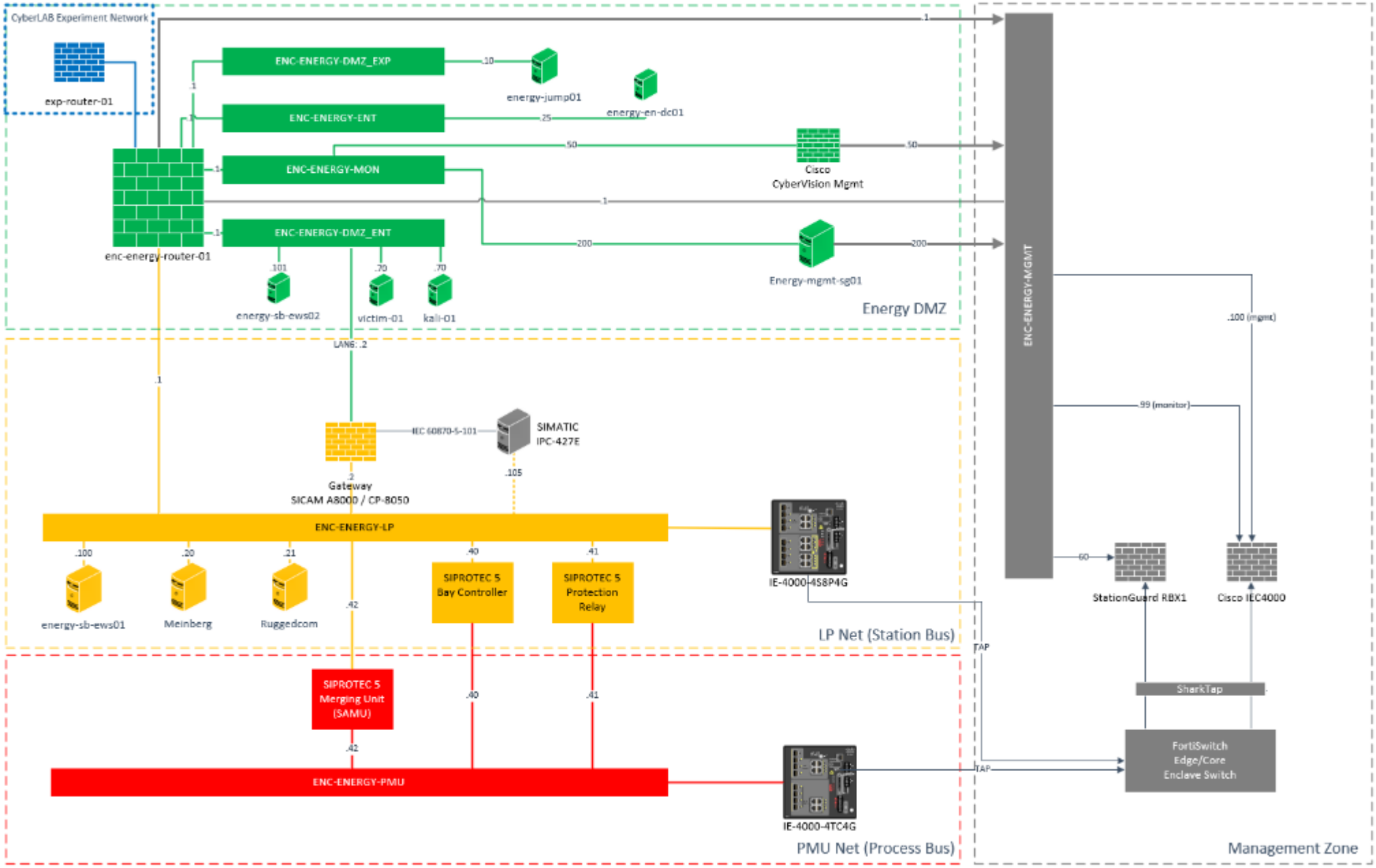
OT


Control Center
Corporate WAN
Attacker
Router
HMI
IEC 60870-5-101
.2
Gateway
SICAM A8000 /CP-8050
SIMATIC
IPC-427E
.105
ENC-ENERGY-LP
.100
.20
.21
IE-4000-4S8P4G
.40
.41
SIPROTEC 5
Bay Controller
SIPROTEC 5
Protection
Relay
Energy-sb-ews01
Meinberg
Ruggedcom
LP Net(Station Bus)
.42
SIPROTEC 5
Merging Unit
(SAMU)
.42
.40
.41
ENC-ENERGY-PMU
IE-4000-4TC4G
MU
IED
IED
MU
IED
MU
PMU Net(Process Bus)

Deteksjonssystemer

- 5 forskjellige IDSer
- 2 OSS «IT» IDSs
- 3 Kommersielle «OT» IDSs
- Samme hendelser til alle IDSer
- Host-agenter på samme maskiner
- Samme nettverksdata til alle

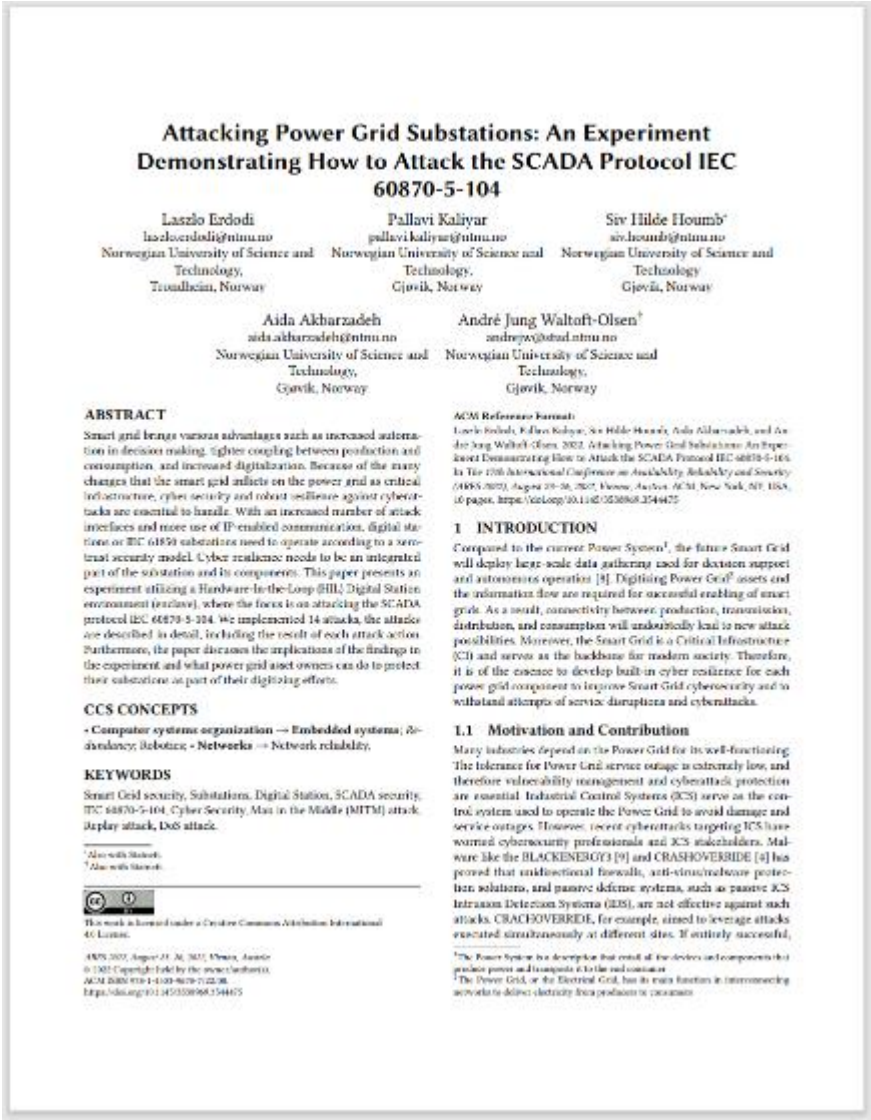




Experience from Performing Controlled Technical Cyber Experiments on Critical Infrastructure as Hybrid Events - John Eidar Simensen, Per-Arne Jørgensen, and Aleksander L. Toppe

Angrepene (IEC 60870-5-104)

- Passiv rekognosering
- Aktiv rekognosering
  - 104 Spesifikk
  - Person i midten (MITM)
- Bryteråpning ved pakke injeksjon
  - 104 spesifikk
- Bryteråpning ved ARP forgiftning
  - 104 spesifikk
- Tjenestenekt med reset meldinger
  - 104 spesifikk



Attacking Power Grid Substations: An Experiment Demonstrating How to Attack the SCADA Protocol IEC 60870-5-104

Laszlo Erdodi
laszloerdodi@ntnu.no
Norwegian University of Science and Technology,
Trondheim, Norway

Pallavi Kaliyar
pallavi.kaliyar@ntnu.no
Norwegian University of Science and Technology,
Gjøvik, Norway

Siv Hilde Houmb
siv.houmb@ntnu.no
Norwegian University of Science and Technology
Gjøvik, Norway

Aida Akbarzadeh
aida.akbarzadeh@ntnu.no
Norwegian University of Science and Technology,
Gjøvik, Norway

André Jung Waltoft-Olsen
andrewj@stud.ntnu.no
Norwegian University of Science and Technology,
Gjøvik, Norway

ABSTRACT

Smart grid brings various advantages such as increased automation in decision making, tighter coupling between production and consumption, and increased digitalization. Because of the many changes that the smart grid inflicts on the power grid as critical infrastructure, cyber security and robust resilience against cyber-attacks are essential to handle. With an increased number of attack interfaces and more use of IP-enabled communication, digital substations or IEC 61850 substations need to operate according to a zero-trust security model. Cyber resilience needs to be an integrated part of the substation and its components. This paper presents an experiment utilizing a Hardware-In-the-Loop (HIL) Digital Station environment (testbed), where the focus is on attacking the SCADA protocol IEC 60870-5-104. We implemented 14 attacks, the attacks are described in detail, including the result of each attack action. Furthermore, the paper discusses the implications of the findings in the experiment and what power grid asset owners can do to protect their substations as part of their digitizing efforts.

CCS CONCEPTS

• **Computer systems organization** → **Embedded systems**; *Redundancy*; Robotics; • **Networks** → Network reliability.

KEYWORDS

Smart Grid security, Substations, Digital Station, SCADA security, IEC 60870-5-104, Cyber Security, Man in the Middle (MITM) attack, Replay attack, DoS attack.

1 INTRODUCTION

Compared to the current Power System[1], the future Smart Grid will deploy large-scale data gathering used for decision support and autonomous operation [8]. Digitizing Power Grid[2] assets and the information flow are required for successful enabling of smart grids. As a result, connectivity between production, transmission, distribution, and consumption will undoubtedly lead to new attack possibilities. Moreover, the Smart Grid is a Critical Infrastructure (CI) and serves as the backbone for modern society. Therefore, it is of the essence to develop built-in cyber resilience for each power grid component to improve Smart Grid cybersecurity and to withstand attempts of service disruptions and cyberattacks.

1.1 Motivation and Contribution

Many industries *depend* on the Power Grid for its well-functioning. The tolerance for Power Grid service outage is extremely low, and therefore vulnerability management and cyberattack protection are essential. Industrial Control Systems (ICS) serve as the control system used to operate the Power Grid to avoid damage and service outages. However, recent cyberattacks targeting ICS have worried cybersecurity professionals and ICS stakeholders. Malware like the BLACKENERGY3 [9] and CRASHOVERRIDE [4] has proved that unidirectional firewalls, anti-virus/malware protection solutions, and passive defense systems, such as passive ICS Intrusion Detection Systems (IDS), are not effective against such attacks. CRASHOVERRIDE, for example, aimed to leverage attacks executed simultaneously at different sites. If entirely successful,

[1]The Power System is a description that entail all the devices and components that produce power and transports it to the end consumer.
[2]The Power Grid, or the Electrical Grid, has its main function is interconnecting networks to deliver electricity from producers to consumers

Erdődi, L., Kaliyar, P., Houmb, S.H., Akbarzadeh, A. and Waltoft-Olsen, A.J., 2022, August. Attacking Power Grid Substations: An Experiment Demonstrating How to Attack the SCADA Protocol IEC 60870-5-104. In *Proceedings of the 17th International Conference on Availability, Reliability and Security* (pp. 1-10).

Deteksjonen
Hva så de forskjellige IDSene i 2021?

Suricata / Wazuh

- Åpen kildekode «gratis»
- Suricata – Nettverk
- Wazuh – SIEM, men vi brukte kun endepunkt-IDS (OSSEC)
- **Så ingen av angrepene.**

Kommersiell IDS 1

- Nettverkbasert
- Hybrid analyse
- **Så flere av angrepene, men ikke alle**

Kommersiell IDS 2

- Nettverk- og endepunkts-basert
- Hybrid analyse
- **Så flere av angrepene, men ikke alle**

Kommersiell IDS 3

- Nettverksbasert
- Signaturbasert analyse
- **Så alle angrepene**
- **Varslet kun ved første tilfelle**

Læringspunkter

- Krever godt dokumentert system
- Egeninnsats og kunnskap om systemet er viktig i innkjøringen
- Kun IDSer for ICS detekterte ICS angrep.
  - Alle de testede har forbedringspotensial
  - Alle de testede er allerede gode
- Ikke en silver-bullet
  - Nødvendig for god sikkerhet
  - Må spille sammen med andre tiltak

Midjouyrney. Prompt: A bearded man with beard stuck in a mailbox

Photo by Adi Goldstein on Unsplash

Ta kontakt

Navn: Jon-Martin Storm
E-post: jomp@nve.no