UNIVERSITETET I OSLO

Smartgrid cybersecurity

Janne Hagen
Adjunct Associate Professor/

Director Head of OT | Gritera Security

5 March 2026



About NVE

- Established in 1921
- Directorate under the Ministry of Energy
- Manages water systems, promote efficient energy markets and cost-effective energy systems
- Ensure that the development of Norwegian hydropower is environmentally friendly, as well as beneficial to the Norwegian society at large



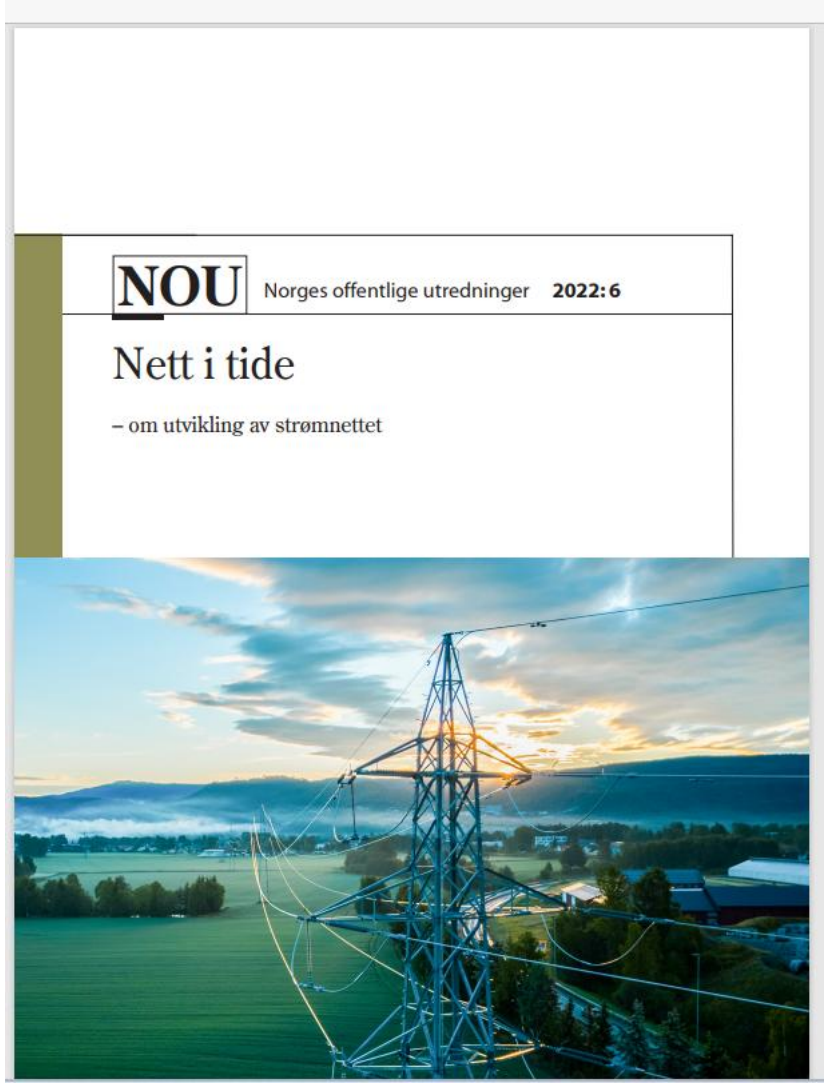


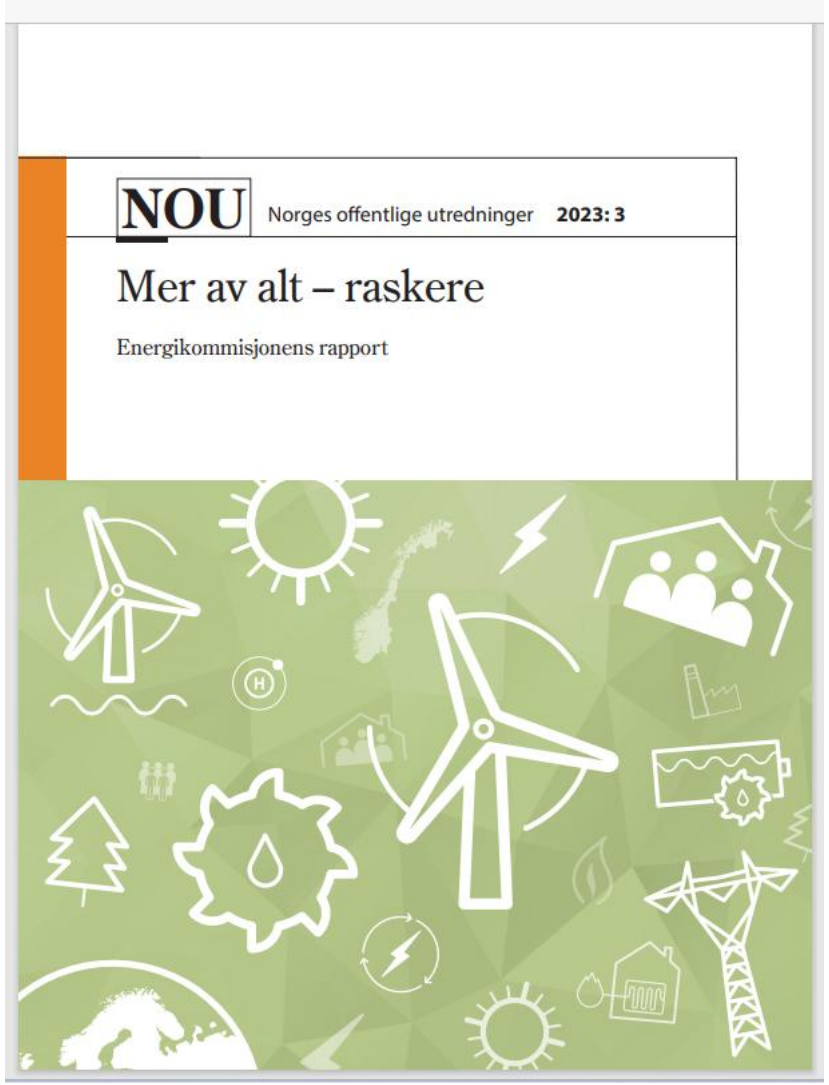
The green deal




LISTA
Vindkraftverk
Foto: S. Oldani, NVE 2020

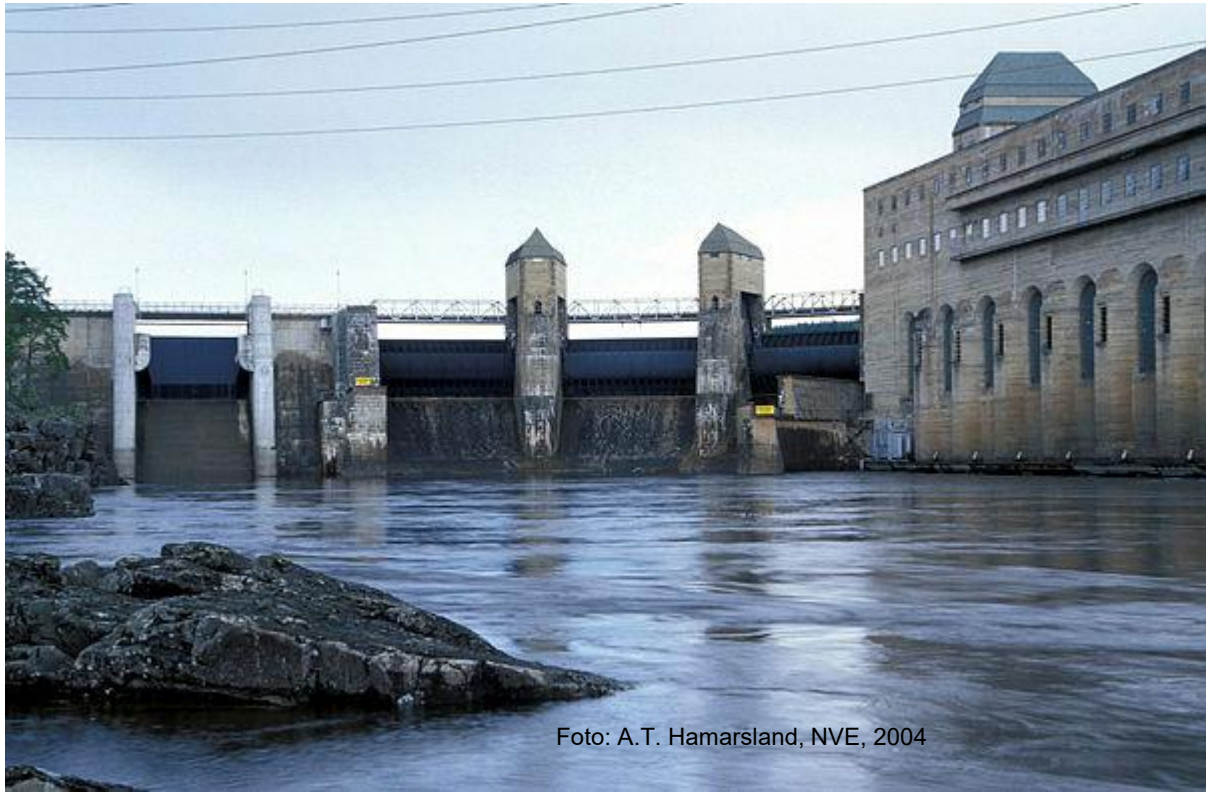
Norwegian renewable energy policies





Water built our country

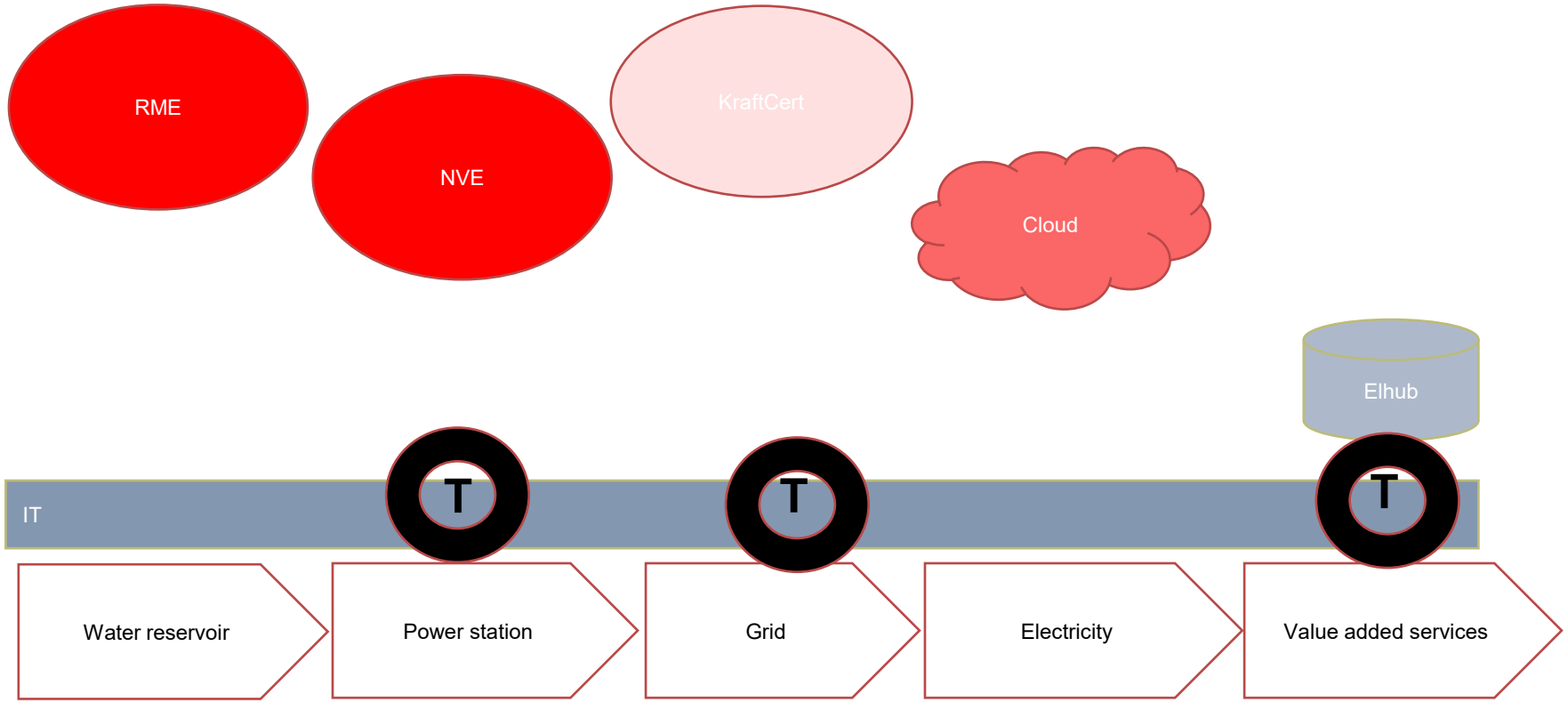
- 1 681 hydropower plants
- More than 1000 hydropower storage reservoirs
- 90% hydropower production
- 10% from 50+ wind farms, 30 thermal power plants and solar power


Foto: A.T. Hamarsland, NVE, 2004


POWER LINES
West-Norway
Foto: V.A Mook, NVE 2017

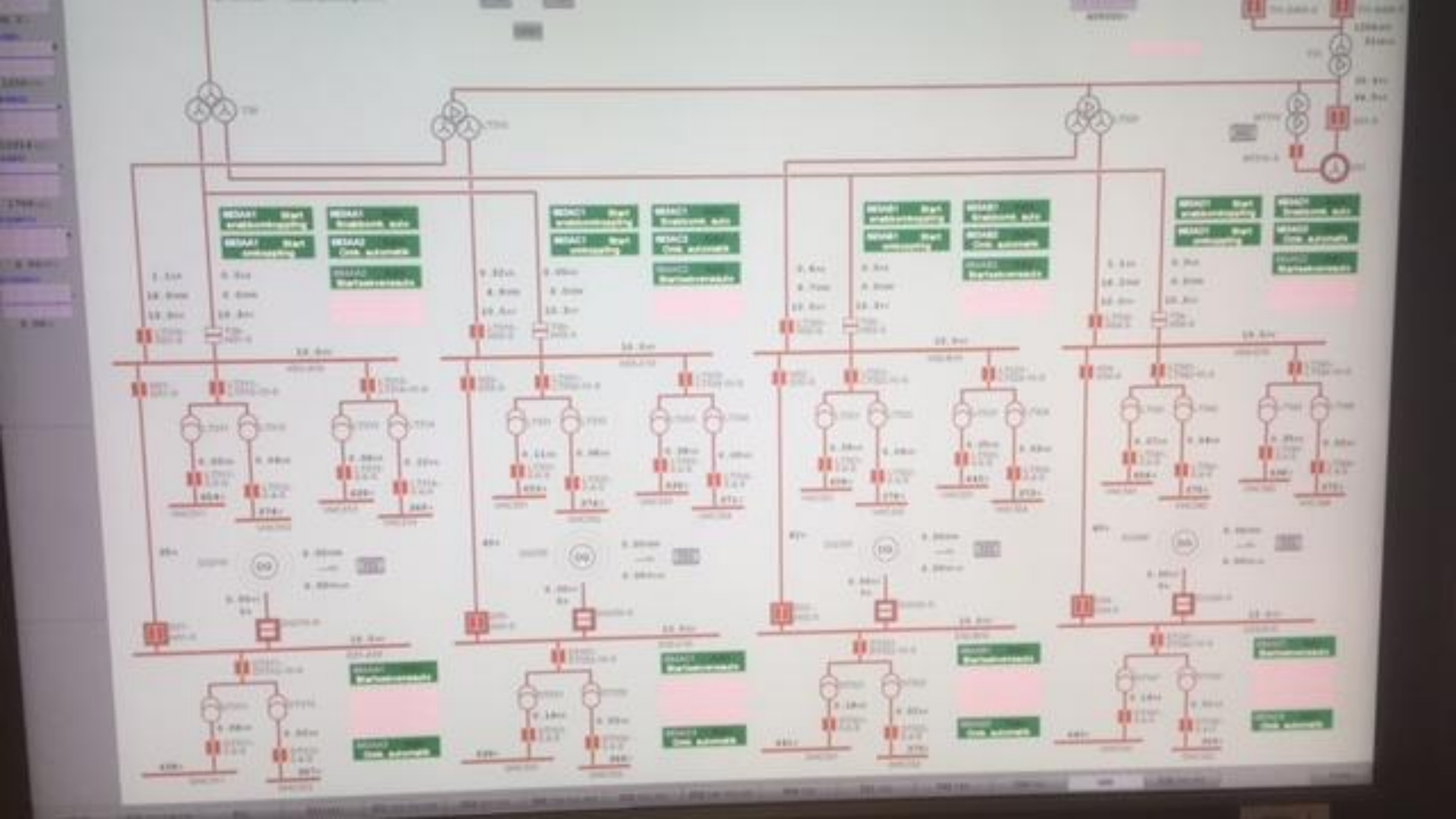
Cyber-physical system, OT in the power system

Digital value chains



Operational Technology (OT) encompasses a broad range of programmable systems and devices that interact with the physical environment (or manage devices that interact with the physical environment) (NIST).

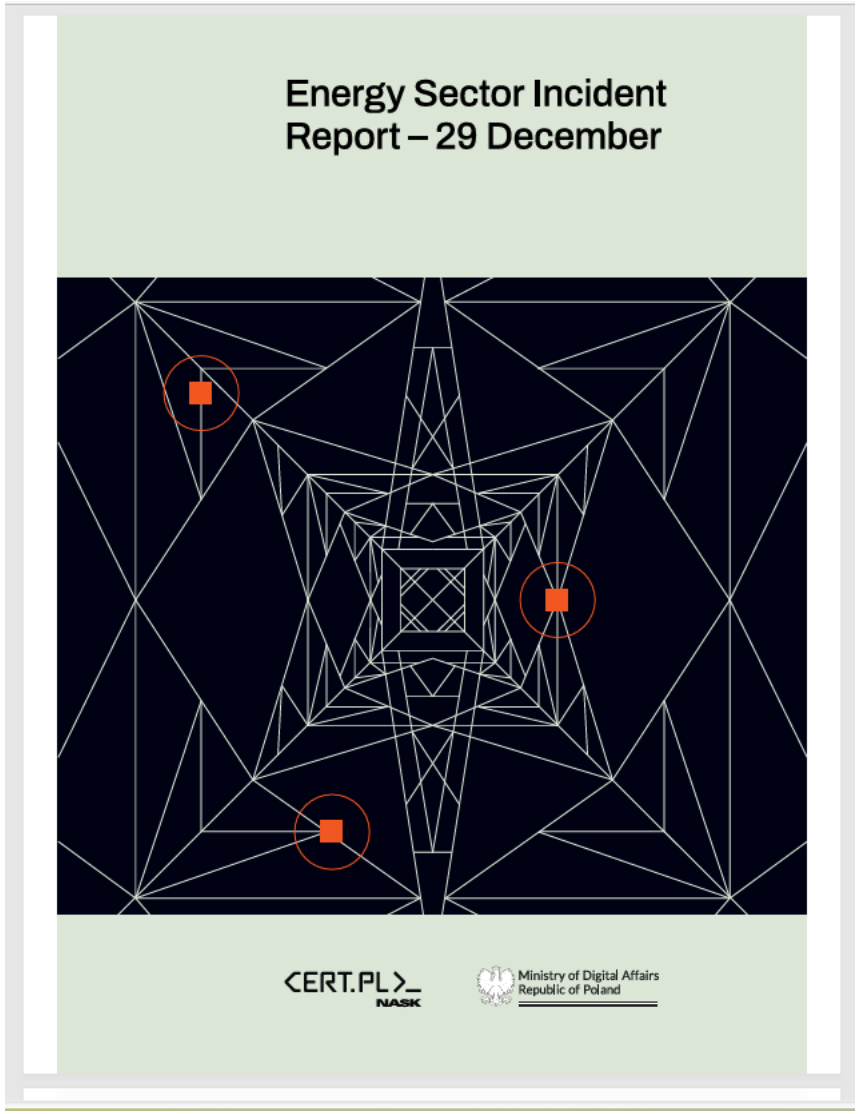
NIST SP 800-82r3 (2023)




"During the next decade, cybersecurity risks will become harder to assess and interpret due to the growing complexity of the threat landscape, adversarial ecosystem and expansion of the attack surface."
in ETL 2020
enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

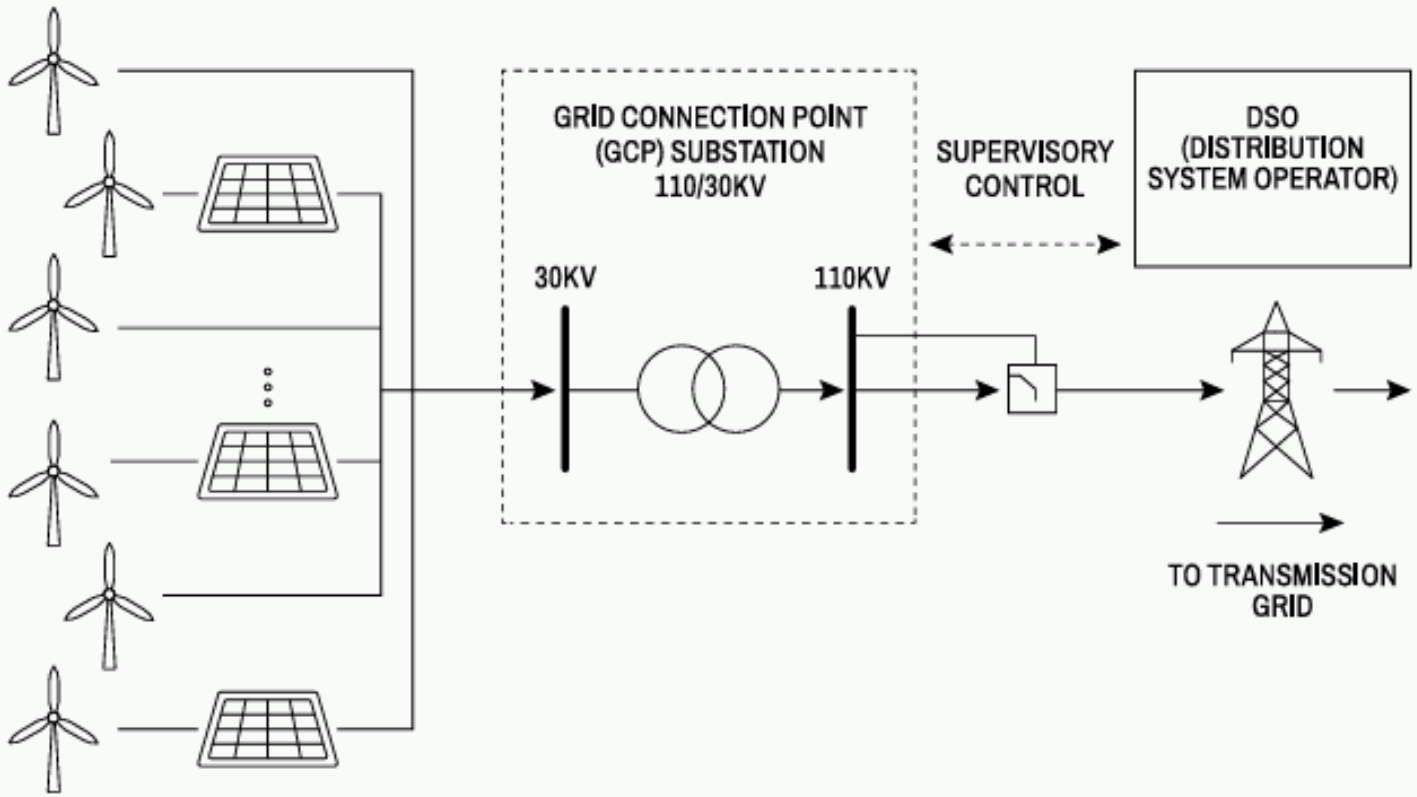

RESEARCH
DISCOVERY
VULNERABILITY EXPLOIT
MAINTAIN ACCESS
ACCESS ESCALATION
COVERING TRACKS
Compromise (Confidentiality, Integrity, Availability)

Case: Cyberattack against Polish renewable energy (29 Dec. 2025)



- Attack against 30 renewable energi facilities (solar and wind) and combined heat and power plant
- Affected IT and OT
- Loss of communication between facilities and DSOs
- Destructive but did not threat the system balance
- Attack coincided with low temperatures and snow-storms

FIG. 1 — Illustrative renewable energy farm and the location of the GCP



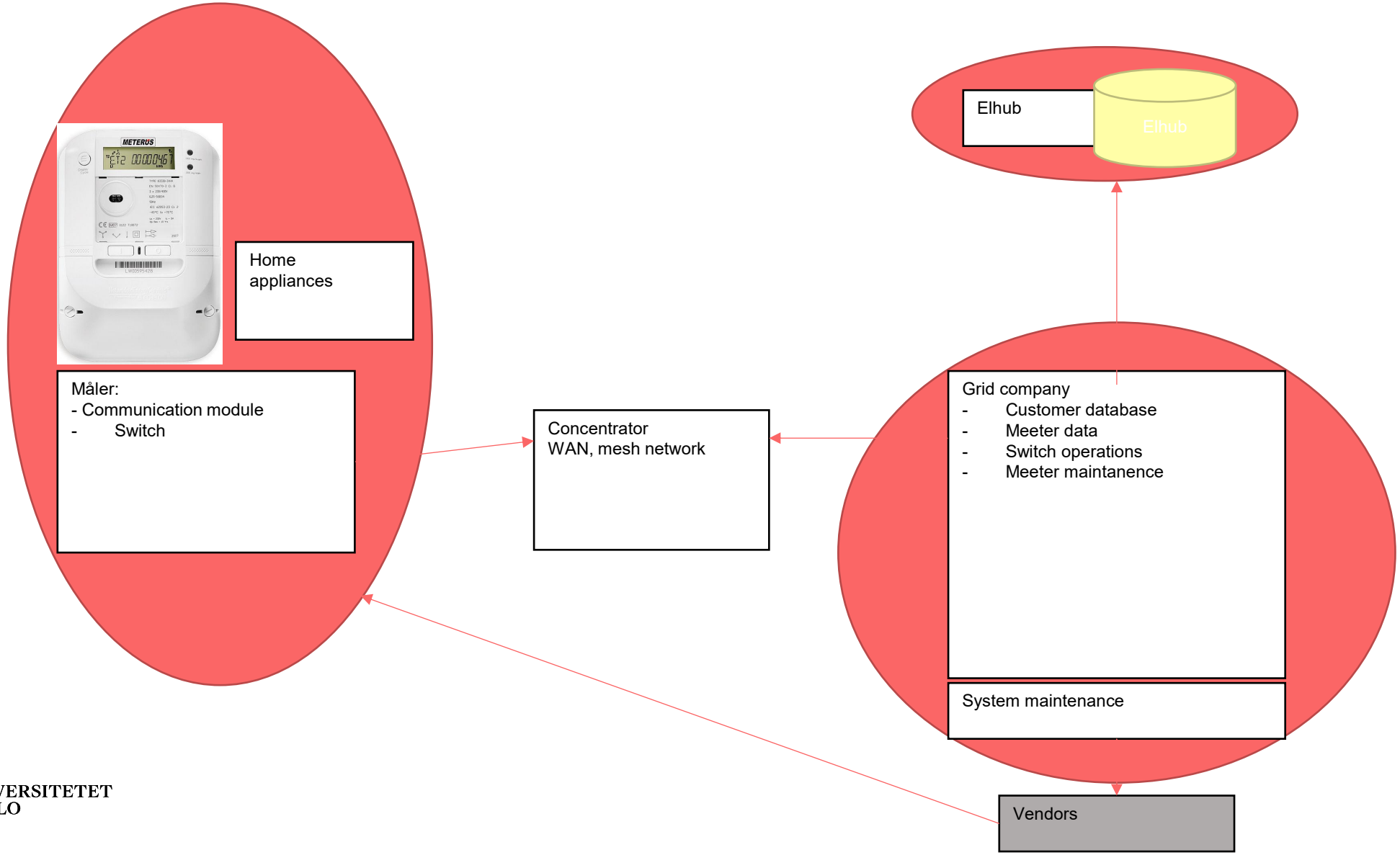
Vulnerabilities – sub station

- Fortigate VPN and firewall, VPN exposable from the Internet
- No multi-factor authentication
- Some devices was vulnerable to remote code execution
- Same passwords and accounts were reused at several facilities
- Devices were configured with default credentials
- The attacker had achieved privileged rights and could easily escalate his access further despite of network segmentation
- Secure update feature (signature) was not enabled
- IED default FTP was mot disabled

The attack

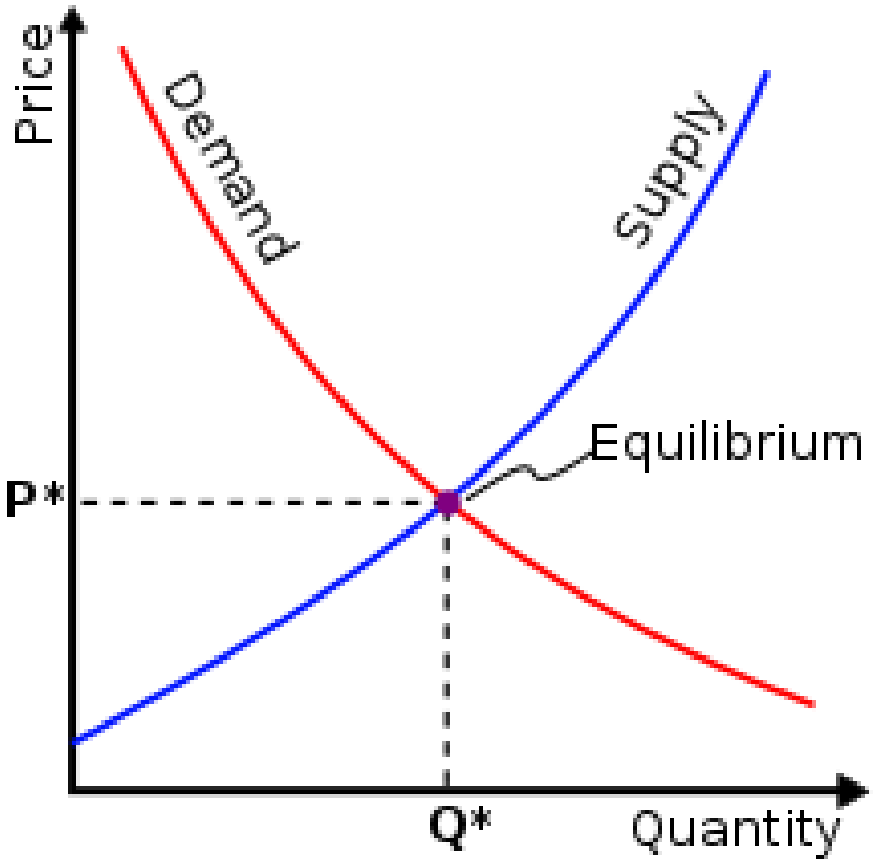
- Attack was carried out by logging into the default account with default credentials
- The account had permissions to modify the device firmware and was used to upload the corrupted firmware
- Attacks seemed to be automated in ascending IP addresses order, reset RTUs to factory configuration

Advanced meetering infrastructure



«The art of balancing»…we must all work together

- Transmission system operator (TSO)
- Distribution system operator (DSO)
- Producers of electricity
- Energy exchanges
- Consumers
- Prosumers
- Aggregators
- Regulators



Wikimedia Commons

Bolig | Smarthus

Smarthuset deres ble hacket: - Dummere hus får man ikke

De bygget smarthus for et enklere liv. Så sluttet huset å fungere. Ta disse syv forholdsreglene om du har smartutstyr.



Tanken var å lage et smarthus med velferdsteknologi. Det har fungert bra siden 2013, men i november begynte det å skje ting i huset. *Foto: Morten Uglum*

Aftenposten 13. des. 2021

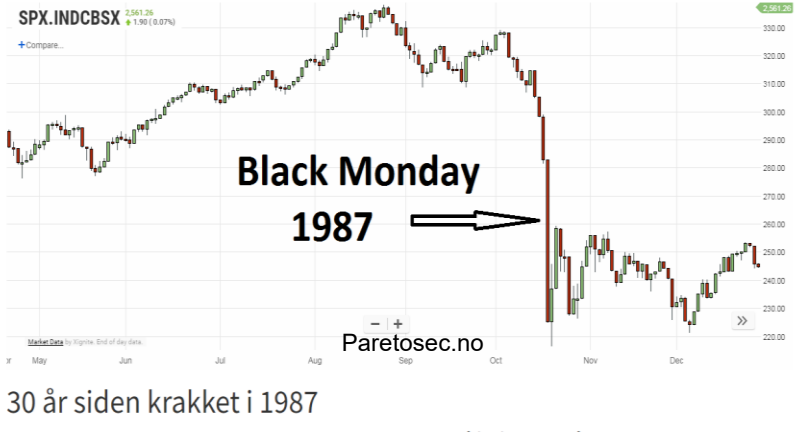
Smart home turned
into a stupid home - did not work according to intentions

24. February 2022

Security politics



Economic outlook



30 år siden krakket i 1987

Critical resources



Refugees



Politics –Norge EU



Regulation

- EEA – National regulatory authority (NRA)
- National regulation – national competent authority (NCA)





Pixabay.com

EU Policy and legislation



ec.europa.eu/

- NIS I and NIS II Directives – general cybersecurity requirements
- Cyber Security Act strengthen ENISA and emphazises standardization
- Cyber Resilience Act bolster more secure HW and SW
- Network Code on Cybersecurity strengthen cross-border security

MAF § 4-6 Security requirements for AMI (content extract)

- Access control
- Network security
- Software security
- Change management
- Incident response



Regulation on security and emergency preparedness in the power supply system

§ 5-3 Securing classified installations

Only KBO-units are allowed to operate classified installations

- All classified installations shall be designed, positioned, constructed, equipped, secured, operated and maintained in such a way that
- risk of damage, breakdown, and malfuction as well as other unwanted incidents and actions are kept to a <u>minimum</u>

Energy Act § 9-3 Everyone has a duty to prevent other than legitimate users from gaining access to or knowledge of sensitive information about the power supply.

§ 6-1 Identification of Sensitive Power System Information and Legitimate Users

- Sensitive power information refers to spesific and detailed information on the power system that can be used to harm installations, systems etc. or in other ways affect the power supply
- The KBO-unit decides whether there is a legitimate need to pass on sensitive information to others outside their own business
- Users granted access to sensitive power system information are not allowed to redistribute the information

§ 6-9 Digital information systems

- Requirement to maintain confidentiality, integrity and availability
- Requirement to apply baseline security according to recognised standards and norms
- Requirements apply to all digital systems

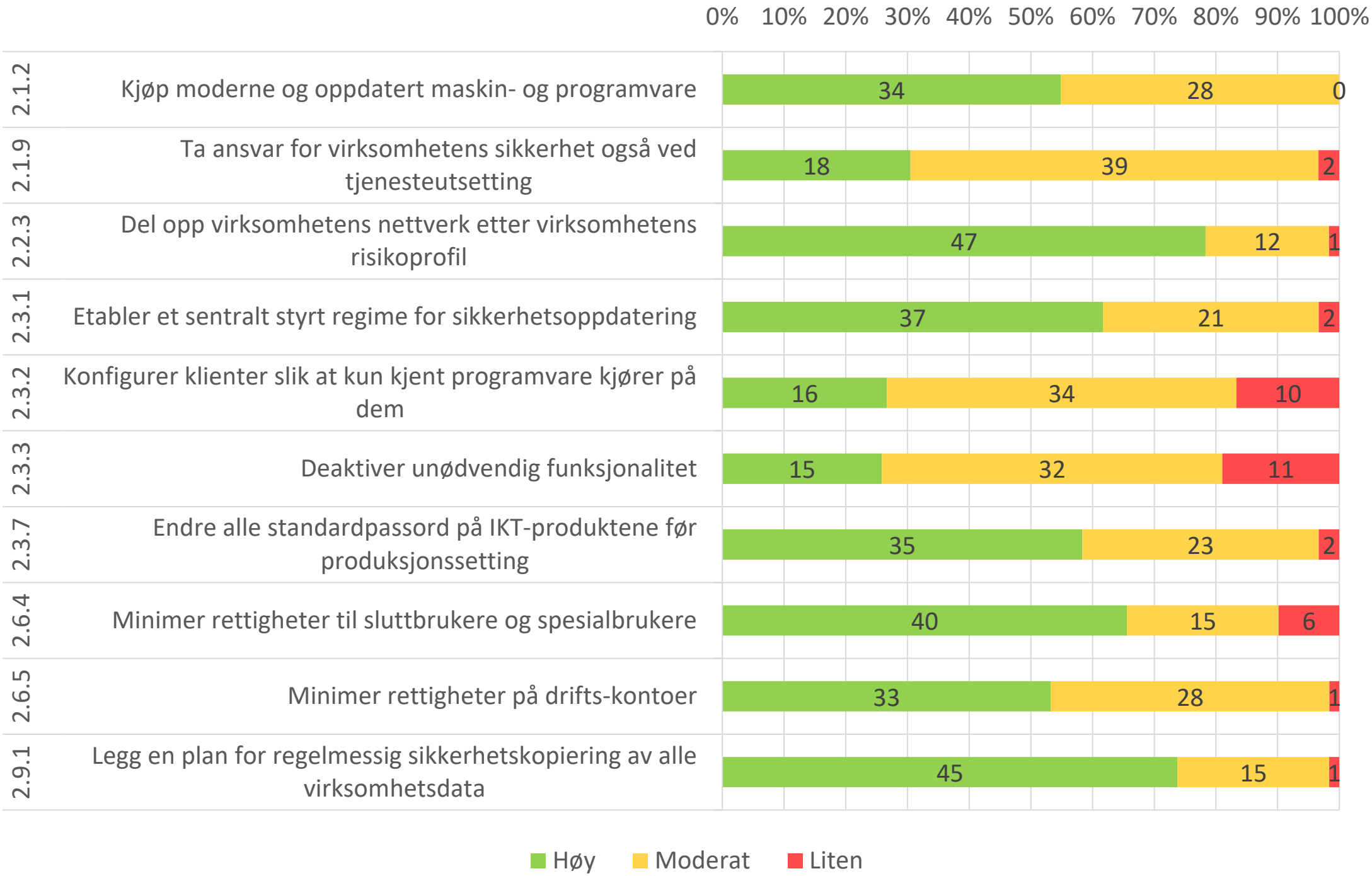
Kbf § 6-9 Baseline Security

- **Identify and Document**
- Risk assessment
- **Secure and Detect**
- **Manage and Restore**
- Outsourcing
- Security Audit



NSMs Grunnprinsipper for IKT-sikkerhet (Security baseline)

Benytt valgene som ligger i drop down menyen i kolonne F i spørreskjema. Her velges vurdering ihht kriterier gitt nedenfor.	
Høy grad	Det finnes flere og gode overlappende sikringstiltak som beskytter verdiene
Moderat grad	Det eksisterer sikringstiltak som beskytter verdien, men de er mangelfulle
Liten grad	Det eksisterer få eller ingen sikringstiltak som beskytter verdien og/ eller sikringstiltakene er mangelfulle
Ikke relevant	Prinsipp ikke relevant for systemet som vurderes.
Ikke vurdert	Standardverdi når prinsipp ikke er vurdert. Prinsippet blir ikke med i videre totalvurdering


0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%
2.1.2
Kjøp moderne og oppdatert maskin- og programvare
34
28
0
2.1.9
Ta ansvar for virksomhetens sikkerhet også ved tjenesteutsetting
18
39
2
2.2.3
Del opp virksomhetens nettverk etter virksomhetens risikoprofil
47
12
1
2.3.1
Etabler et sentralt styrt regime for sikkerhetsoppdatering
37
21
2
2.3.2
Konfigurer klienter slik at kun kjent programvare kjører på dem
16
34
10
2.3.3
Deaktiver unødvendig funksjonalitet
15
32
11
2.3.7
Endre alle standardpassord på IKT-produktene før produksjonssetting
35
23
2
2.6.4
Minimer rettigheter til sluttbrukere og spesialbrukere
40
15
6
2.6.5
Minimer rettigheter på drifts-kontoer
33
28
1
2.9.1
Legg en plan for regelmessig sikkerhetskopiering av alle virksomhetsdata
45
15
1
Høy
Moderat
Liten

What you should think about in innovation projects and smart grid?

- Understand the context - *energy security by design*
- Understand the legal requirements

What you should think about in innovation projects and smart grid?

- Understand the context - *energy security by design*
- Understand the legal requirements
- Assess risk, analyse threats and business impact of the proposed solution
- Use relevant frameworks for security development lifecycle

Security challenges

- Legacy
- Transparancy
- Complexity
- Wide reaching long digital value chains/supply chains and data flows
- Hidden dependancies
- Unknown hardcoded passwords
- Lack of authentication
- Lack of accountability

Energy act § 9-2 Emergency preparedness measures

The emergency prepardness authority can decide that in ekstraordinary situations operations shall be conducted from Norwegian territory

References

- https://energifaktanorge.no/en/norsk-energiforsyning/kraftproduksjon
- https://www.aftenposten.no/bolig/i/5GyPJO/smarthuset-deres-ble-hacket-dummere-hus-faar-man-ikke
- https://publikasjoner.nve.no/eksternrapport/2021/eksternrapport2021_19.pdf
- https://www.nve.no/energi/tilsyn/kraftforsyningsberedskap/veiledning-til-kraftberedskapsforskriften/
- NVE lanserer digital veiledning til kraftberedskapsforskriften - NVE