Sikkerhetsarkitektur for norske driftssentraler

Vahiny Gnanasekaran,

CINELDI-webinar, 13.11.2024

Teknologi for et bedre samfunn

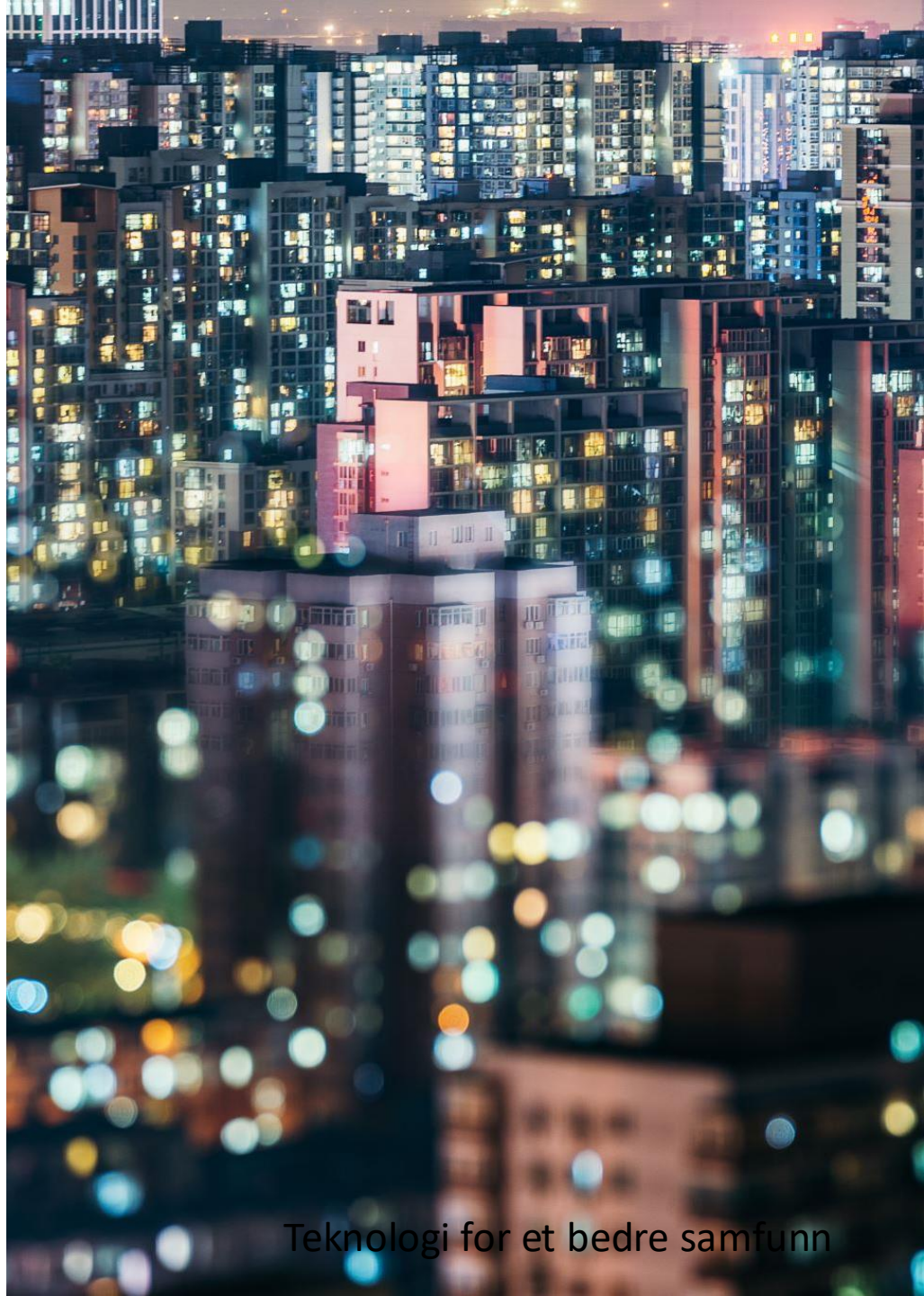
POLITICO

ar in Ukraine | Israel-Hezbollah war | US election | Newsletters | Podcasts | Poll of Polls | Policy ne

NEWS > ENERGY AND CLIMATE

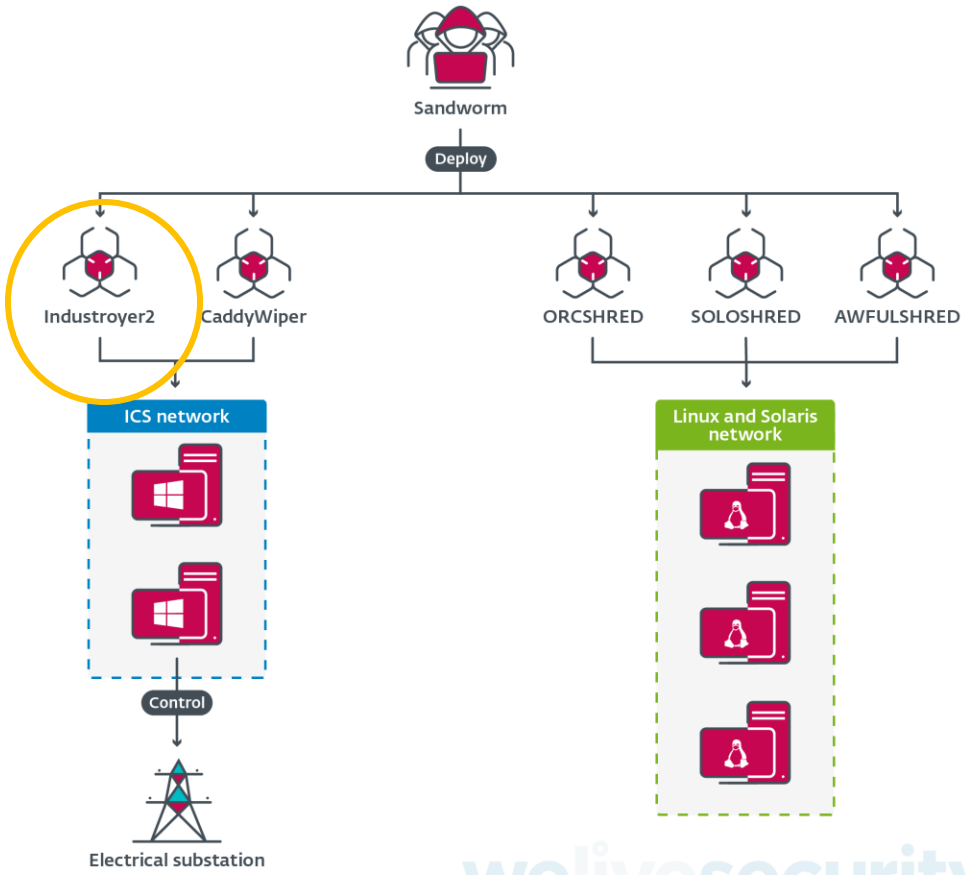
Europe's grid is under a cyberattack deluge, industry warns

Cyberattacks against the energy sector have spiked. The sector needs to sp up, chief officials say.



Teknologi for et bedre samfunn

Tidligere angrep: industroyer2



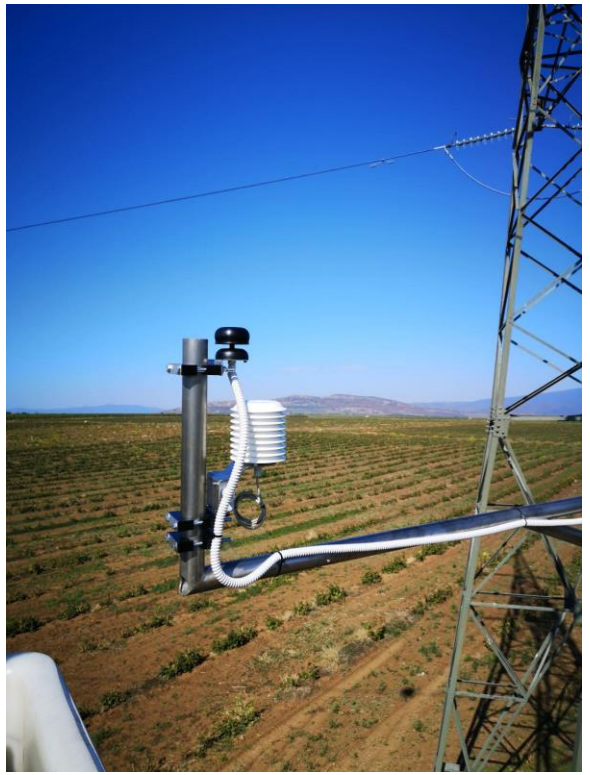
- Tidligere cyberangrep på det ukrainske strømnettet ble forsøkt modifisert
- Cyberangrepet var ikke vellykket
- Kunne forårsaket strømbrudd for to millioner kunder

https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

Sensorer

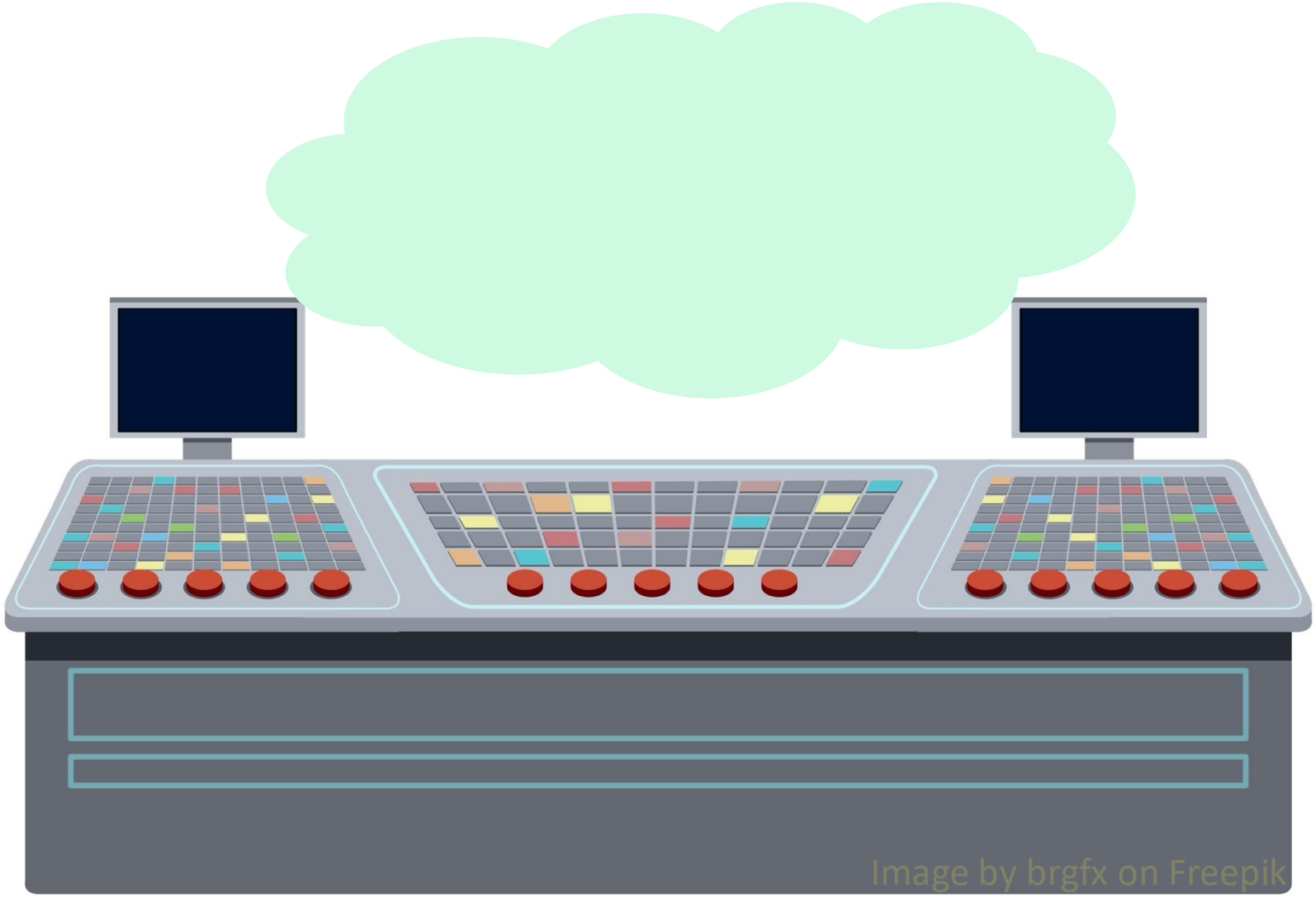
https://heimdallpower.com/system-wide-with-elvia/

https://www.smart-energy.com/industry-sectors/new-technology/siemens-smart-infrastructure-launches-enhanced-grid-sensor-tech/

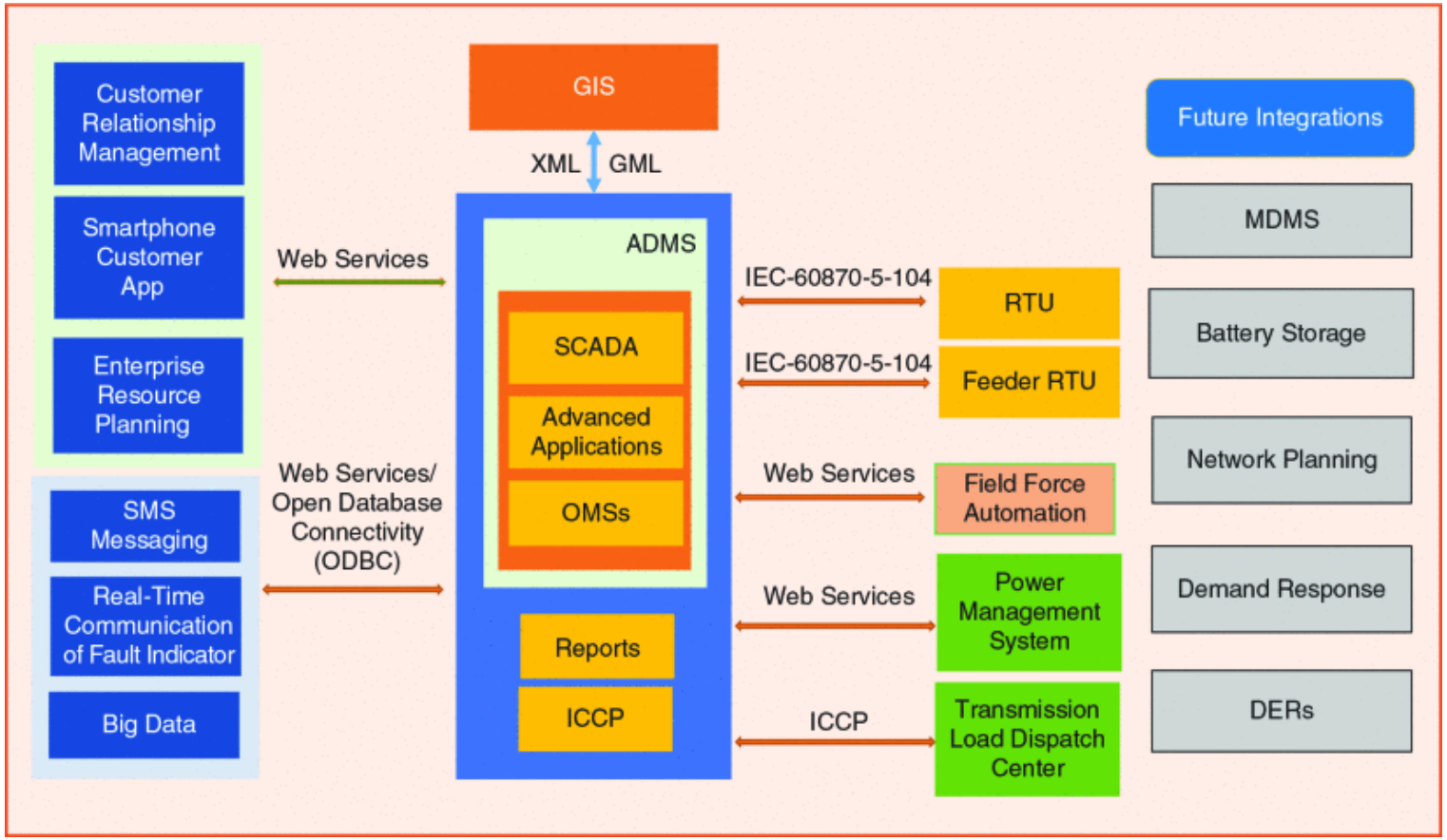


https://gridguard.systems/products-services

Skyløsninger i driftssentralen



Advanced Distribution Management System (ADMS)



P. Devanand *et al.*, "Advanced Distribution Management System: Improving Distribution Efficiency Through an Integrated Approach," in *IEEE Power and Energy Magazine*, vol. 18, no. 1, pp. 55-62, Jan.-Feb. 2020, doi: 10.1109/MPE.2019.2945345.

SINTEF

Agenda

- Hva er en sikkerhetsarkitektur?
- Tidligere arbeider
- Standarder og rammeverk
- Hvordan har vi gjort det?
- Resultater
- Implikasjoner av fremtidig teknologi i driftssentralen

Hva er en sikkerhetsarkitektur?

"en detaljert beskrivelse av alle aspekter i et system som relateres til cybersikkerhet, sammen med en liste av prinsipper til å veilede designet"

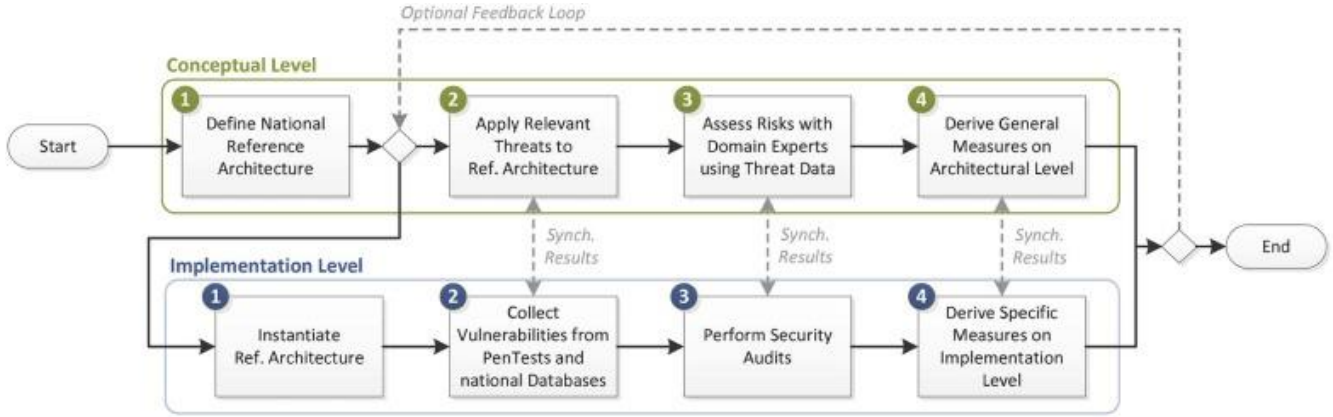
CEN/CENELEC/ETSI Joint Working Group: Final report of the CEN/CENELEC/ETSI Joint Working Group on Standards for Smart Grids. Tech. rep., CEN/CENELEC/ETSI (2011)

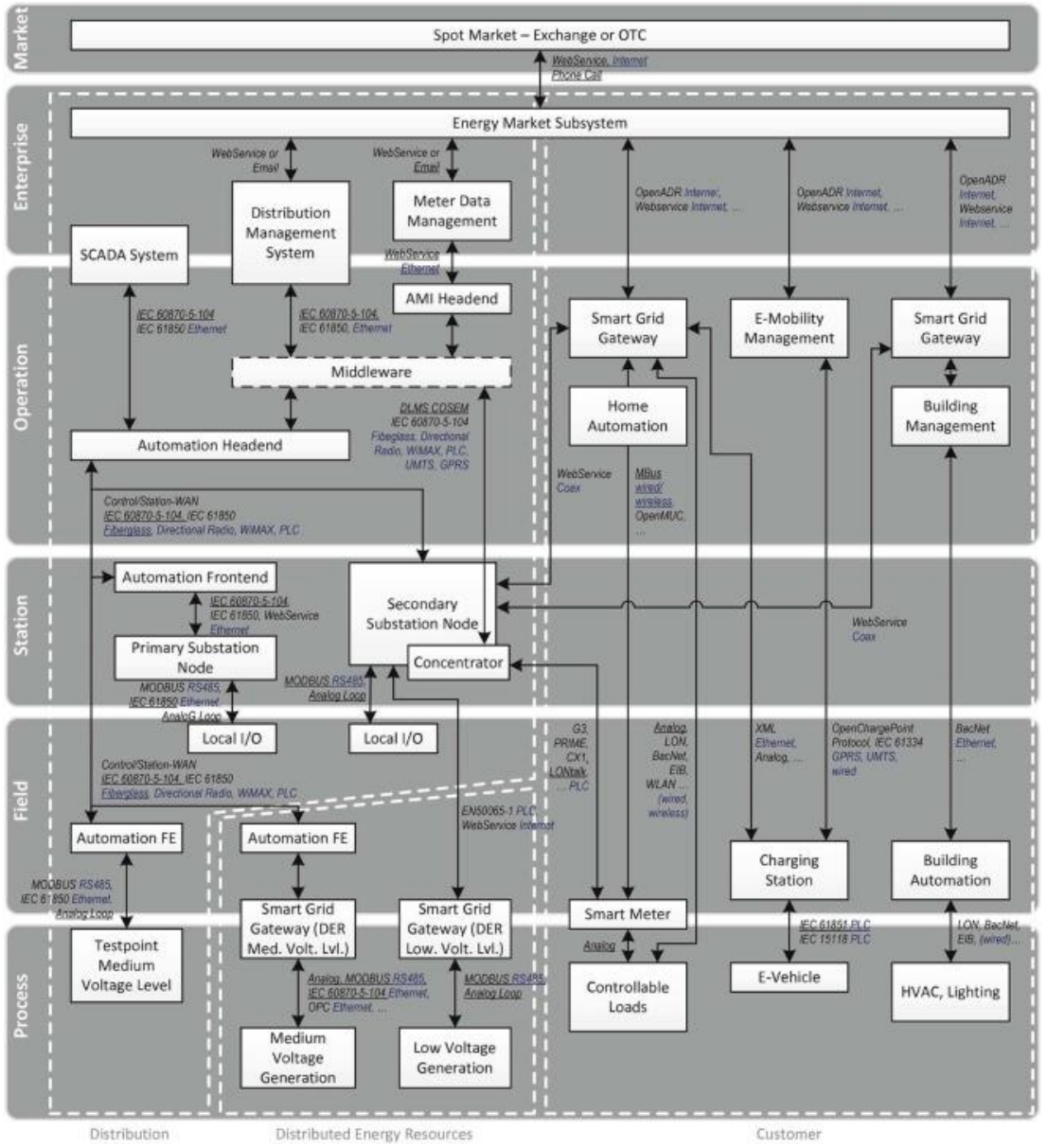
Tidligere arbeider

Computers & Security
Volume 62, September 2016, Pages 165-176

From old to new: Assessing cybersecurity risks for an evolving smart grid

Lucie Langer [a], Florian Skopik [a], Paul Smith [a], Markus Kammerstetter [b]





Langer, Lucie, et al. "From old to new: Assessing cybersecurity risks for an evolving smart grid." *Computers & Security* 62 (2016): 165-176. https://doi.org/10.1016/j.cose.2016.07.008

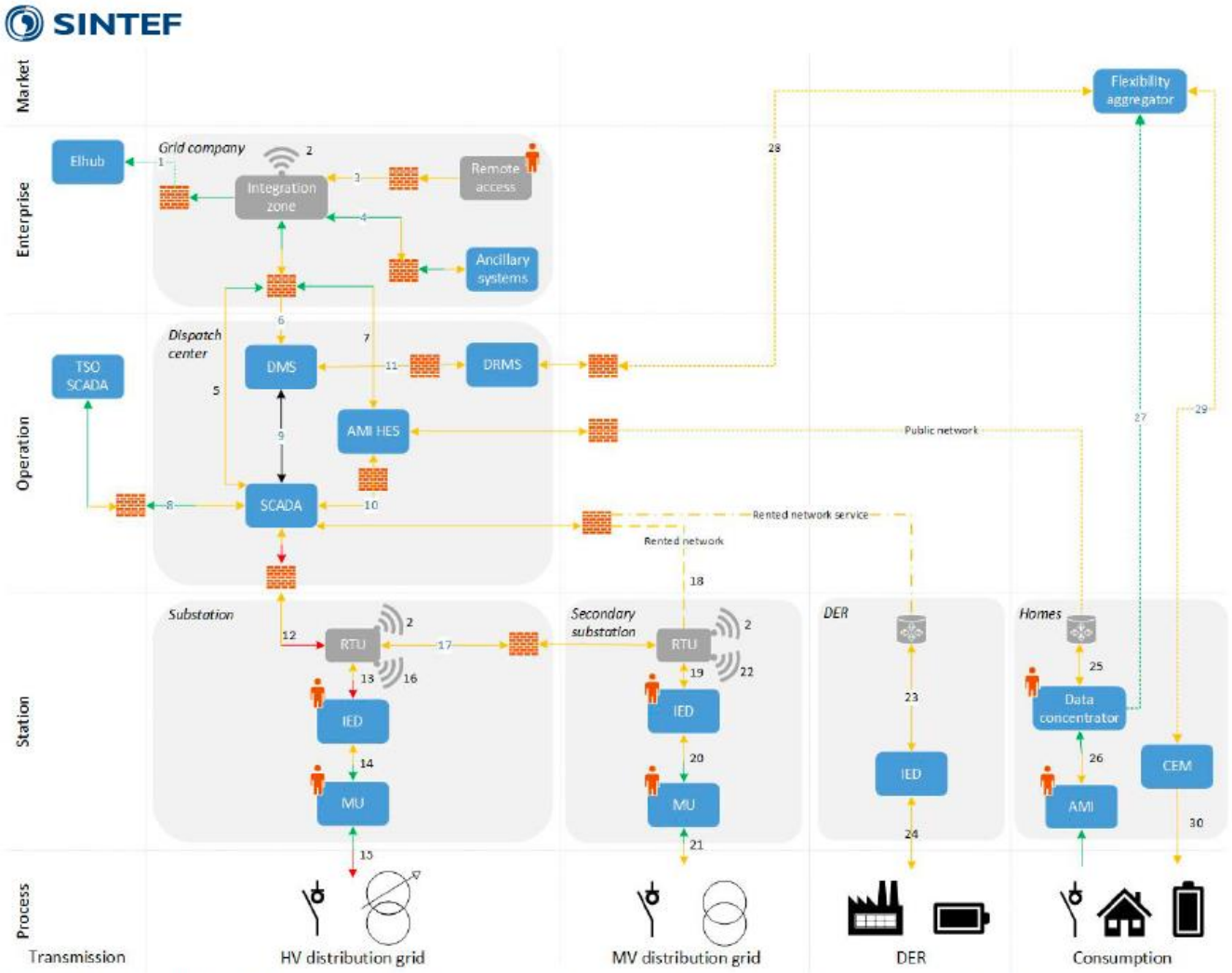
Prosjektnotat

Referansesystem for overordnet risikoanalyse av smarte distribusjonsnett

VERSJON
1.0

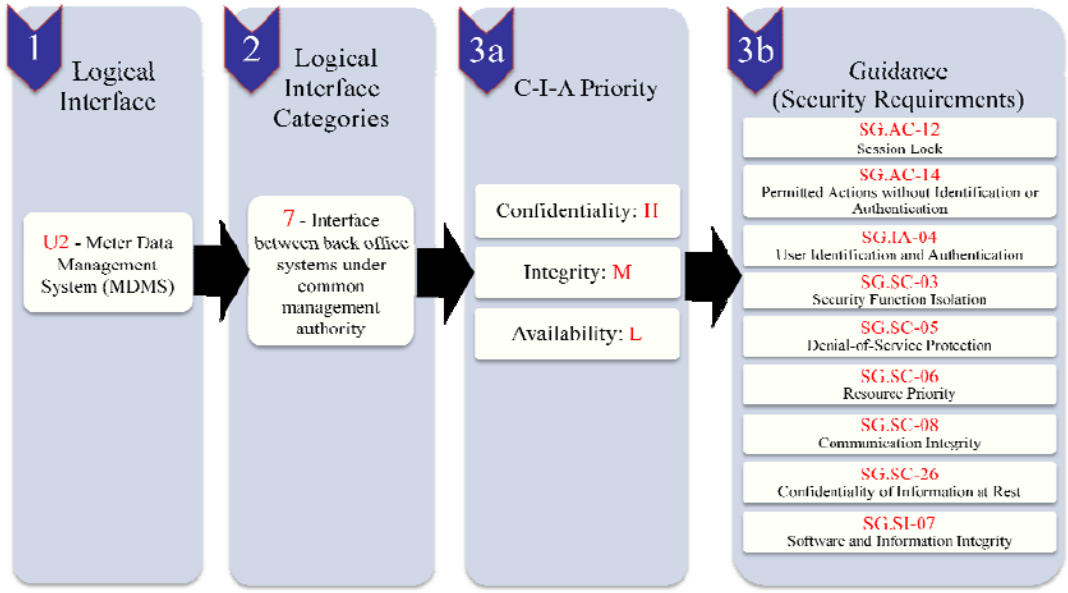
DATO
2020-11-24

FORFATTER(E)
Jørn Foros



Figur 3: Forslag til forenklet generisk referansesystem for overordnet risikoanalyse av smarte distribusjonsnett

Standarder og rammeverk: NIST IR7628



NISTIR 7628 Revision 1

Guidelines for Smart Grid Cybersecurity

Volume 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements

The Smart Grid Interoperability Panel – Smart Grid Cybersecurity Committee

http://dx.doi.org/10.6028/NIST.IR.7628r1

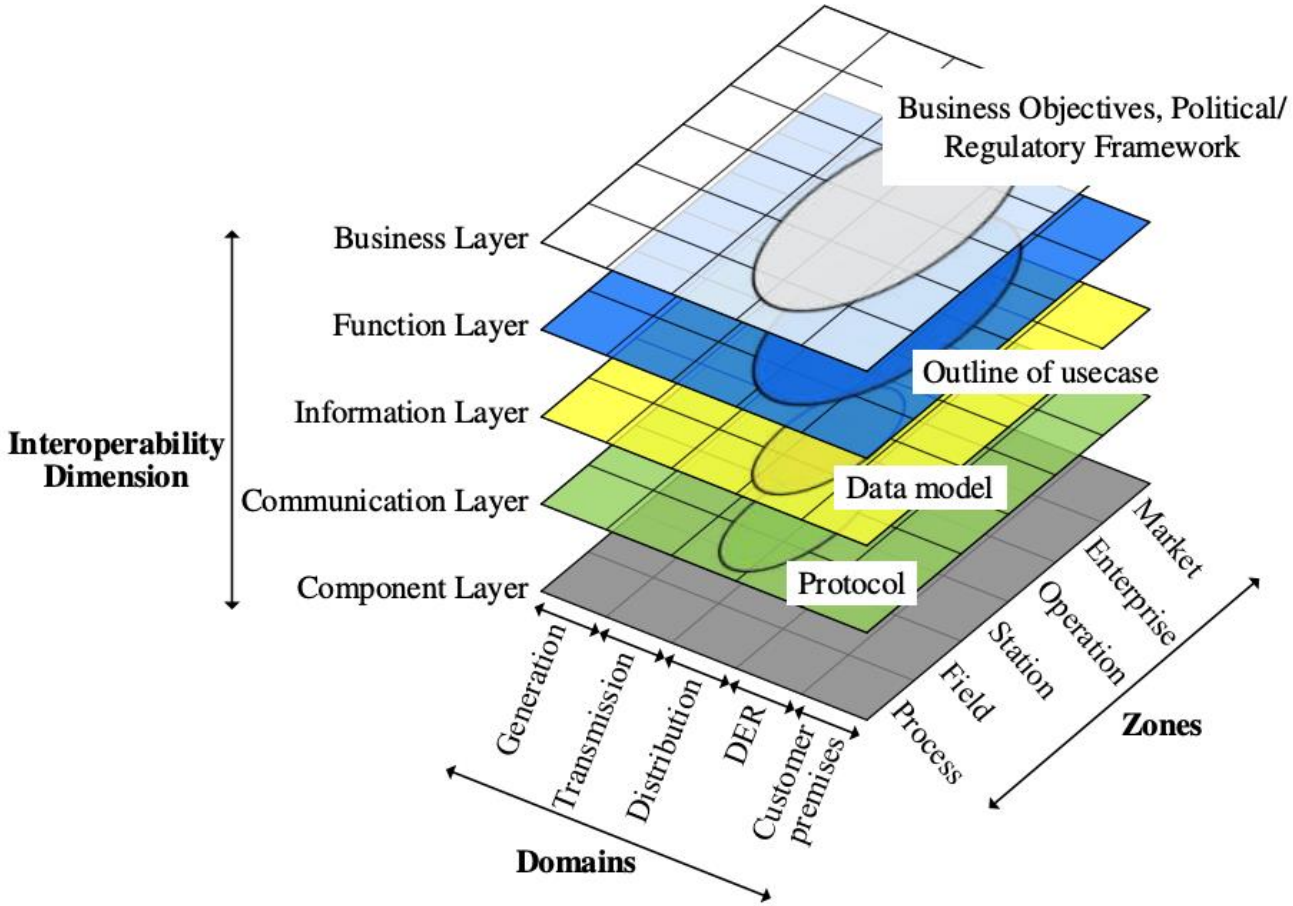
A. C. . -F. Chan and J. Zhou, "On smart grid cybersecurity standardization: Issues of designing with NISTIR 7628," in IEEE Communications Magazine, vol. 51, no. 1, pp. 58-65, January 2013, doi: 10.1109/MCOM.2013.6400439.

Sum: 48 grensesnitt med 22 logiske kategorier på tvers av 7 smartgriddomener

NIST National Institute of Standards and Technology U.S. Department of Commerce

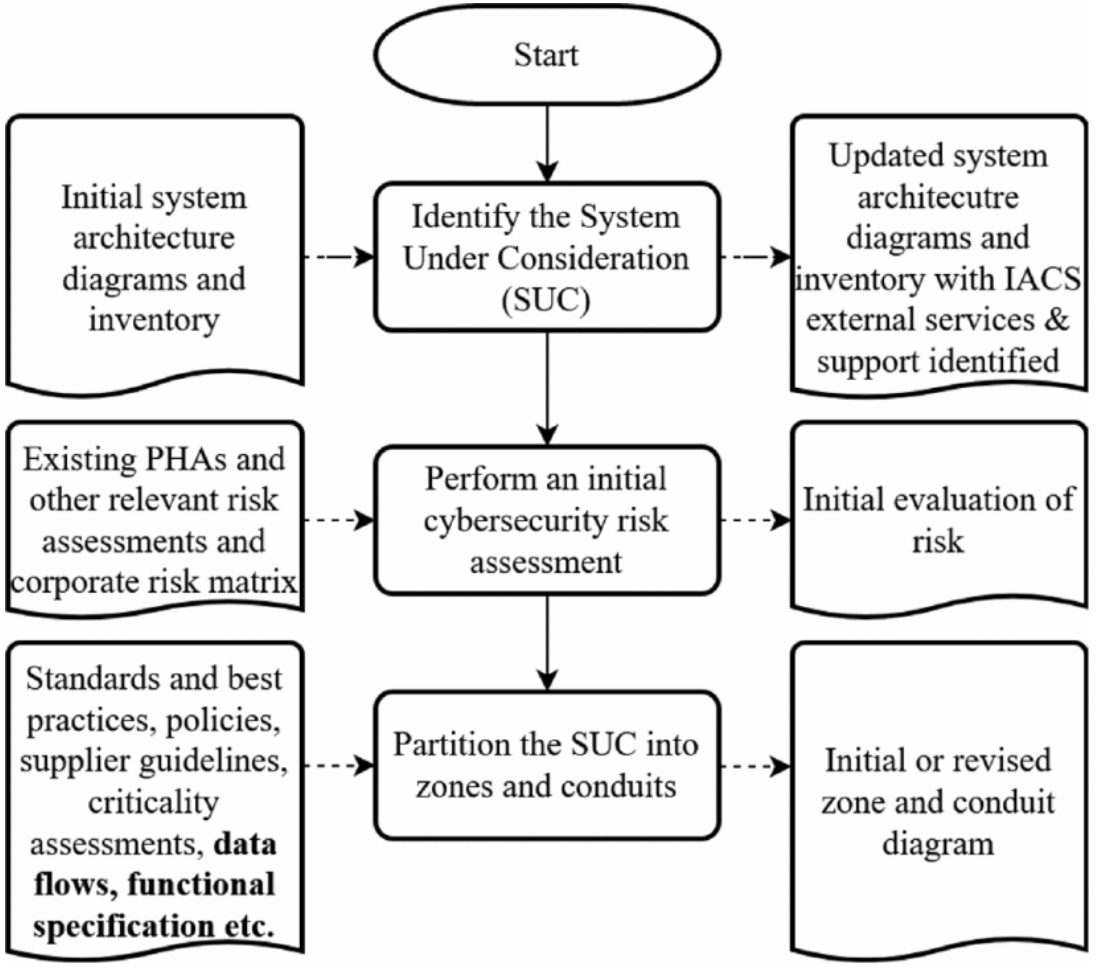
Standarder og rammeverk: SGAM

- Smart Grid Architecture Model



Standarder og rammeverk: IEC 62443

- «OT-versjonen» av ISO 27000-serien



M. Kern et al., "An Architecture-based Modeling Approach Using Data Flows for Zone Concepts in Industry 4.0," 2020 IEEE International Symposium on Systems Engineering (ISSE), Vienna, Austria, 2020, pp. 1-8, doi: 10.1109/ISSE49799.2020.9272013.

Standarder og rammeverk: MITRE ATT&CK ICS

ICS Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for ICS.

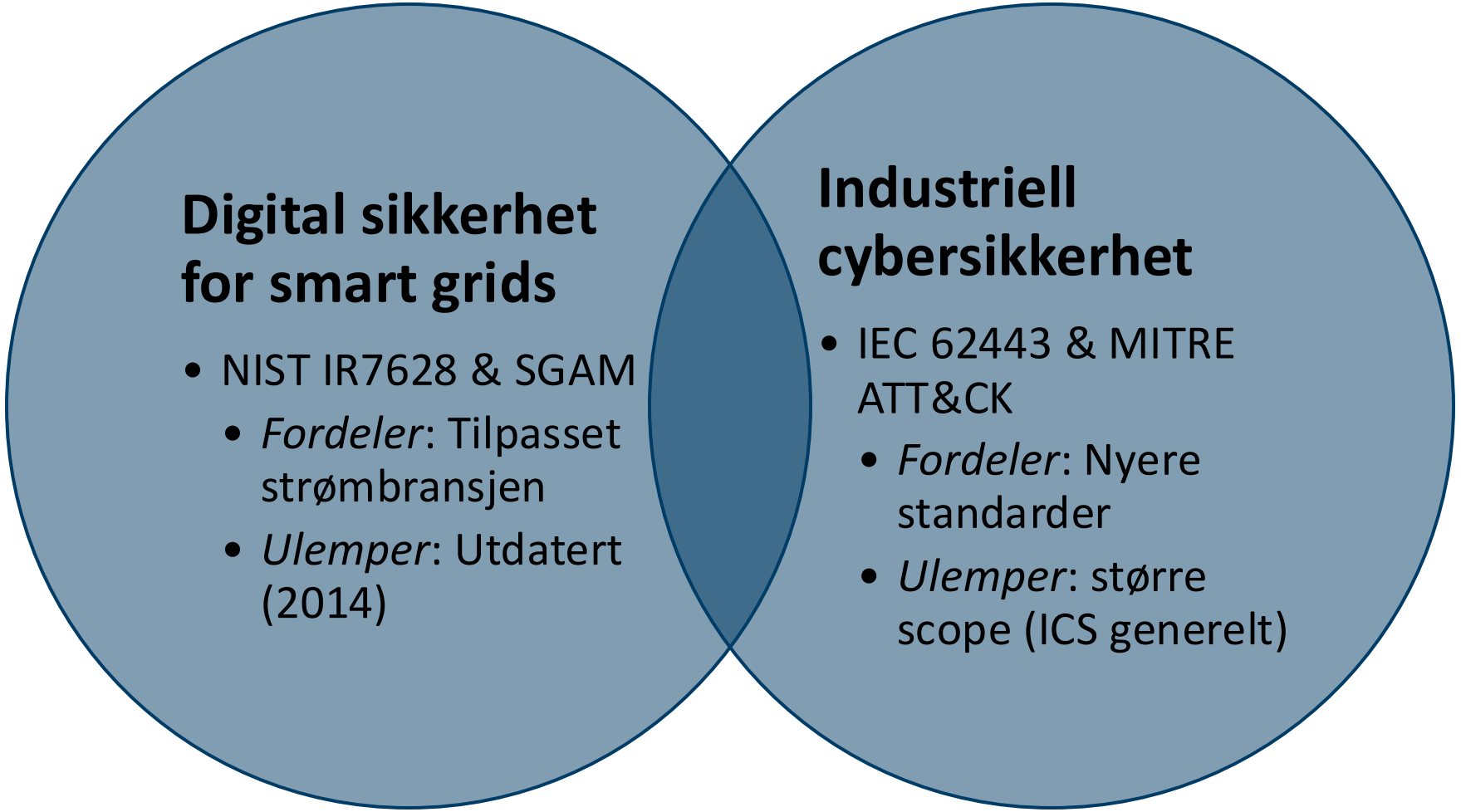
View on the ATT&CK® Navigator

Version Permalink

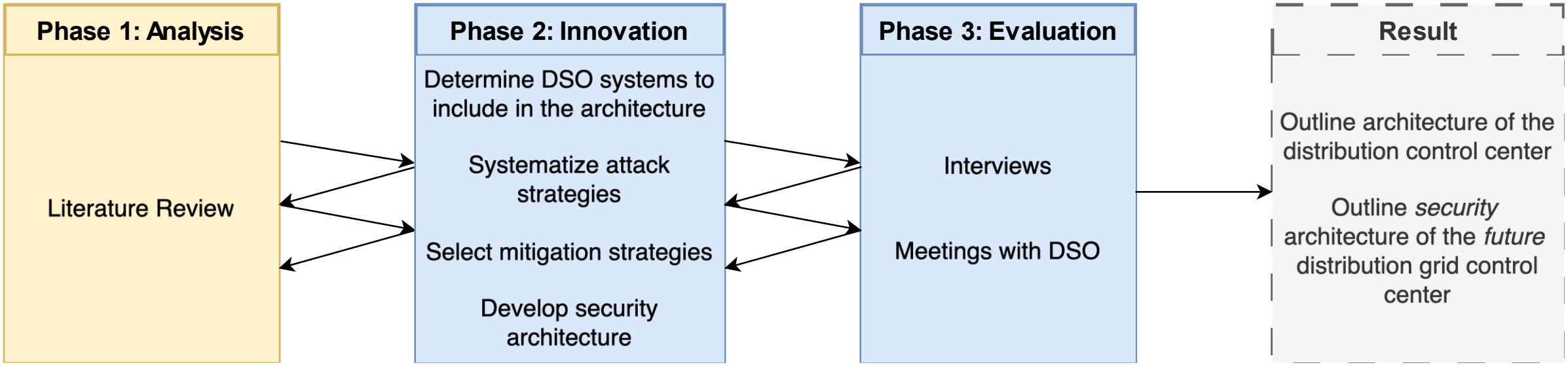
Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
12 techniques	10 techniques	6 techniques	2 techniques	7 techniques	5 techniques	7 techniques	11 techniques	3 techniques	14 techniques	5 techniques	12 techniques
Drive-by Compromise	Autorun Image	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Change Operating Mode	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Command-Line Interface	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Execution through API	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Graphical User Interface	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Hooking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image		Change Credential		Loss of Productivity and Revenue
Replication Through Removable Media	Modify Controller Tasking			System Binary Proxy Execution		Valid Accounts	Monitor Process State		Data Destruction		Loss of Protection
Rogue Master	Native API						Point & Tag Identification		Denial of Service		Loss of Safety
Spearphishing Attachment	Scripting						Program Upload		Device Restart/Shutdown		Loss of View
Supply Chain Compromise	User Execution						Screen Capture		Manipulate I/O Image		Manipulation of Control
Transient Cyber Asset							Wireless Sniffing		Modify Alarm Settings		Manipulation of View
Wireless Compromise									Rootkit		Theft of Operational Information
									Service Stop		
									System Firmware		

- Taktikker = “hvorfor”
- Teknikker = “hvordan”
- Tiltaksstrategier

Oppsummering: standarder og rammeverk

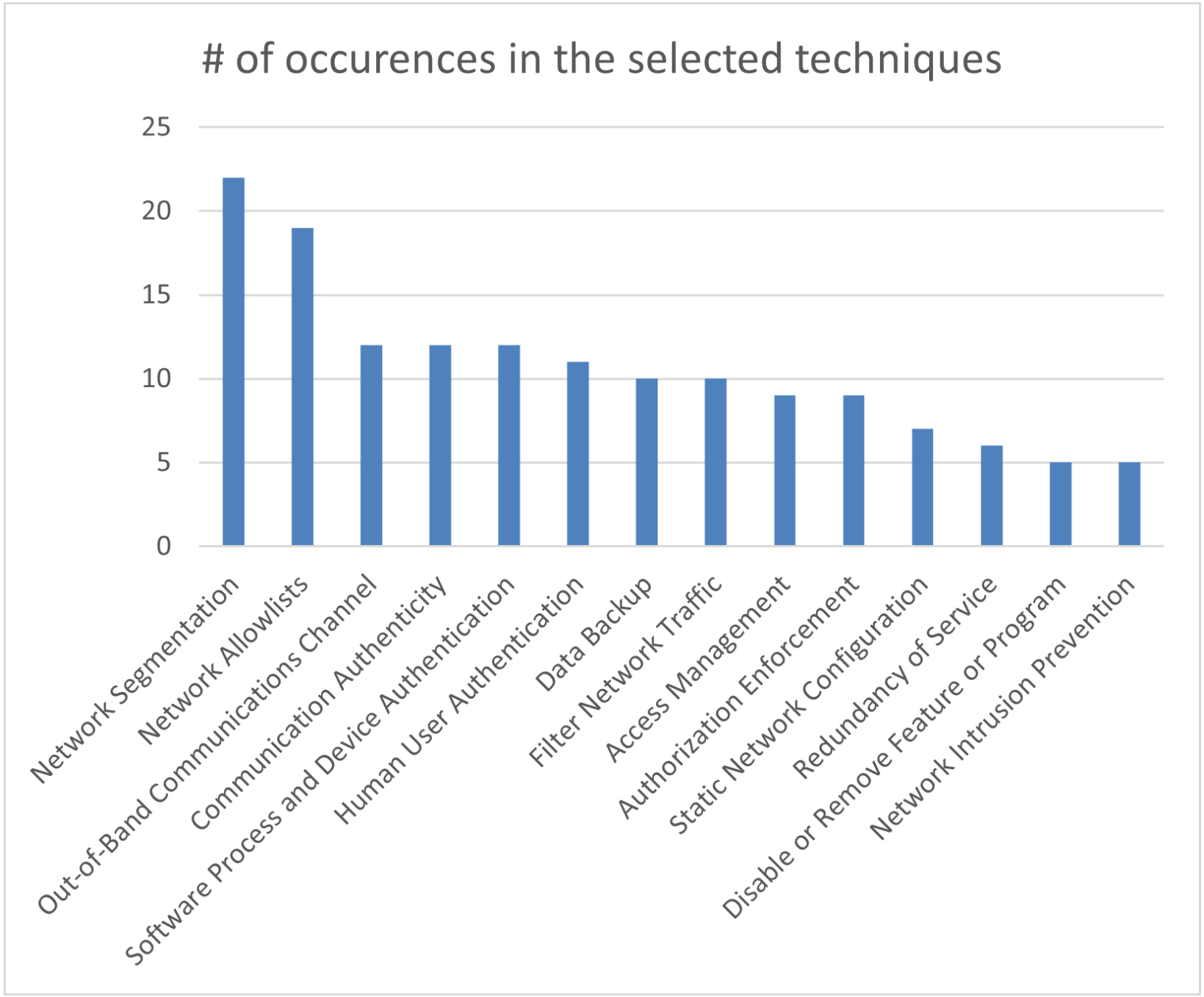


Hvordan har vi gjort det?

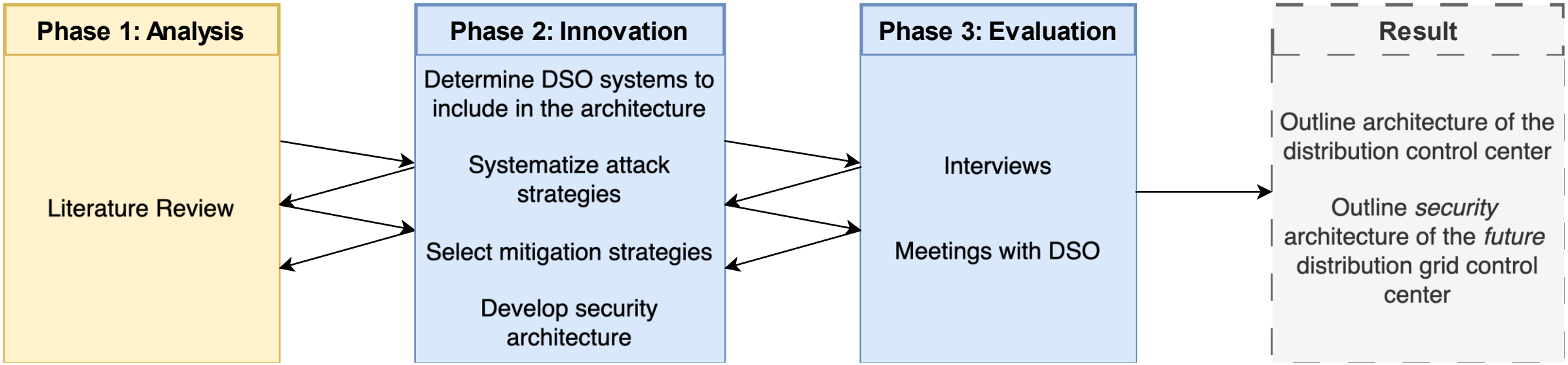


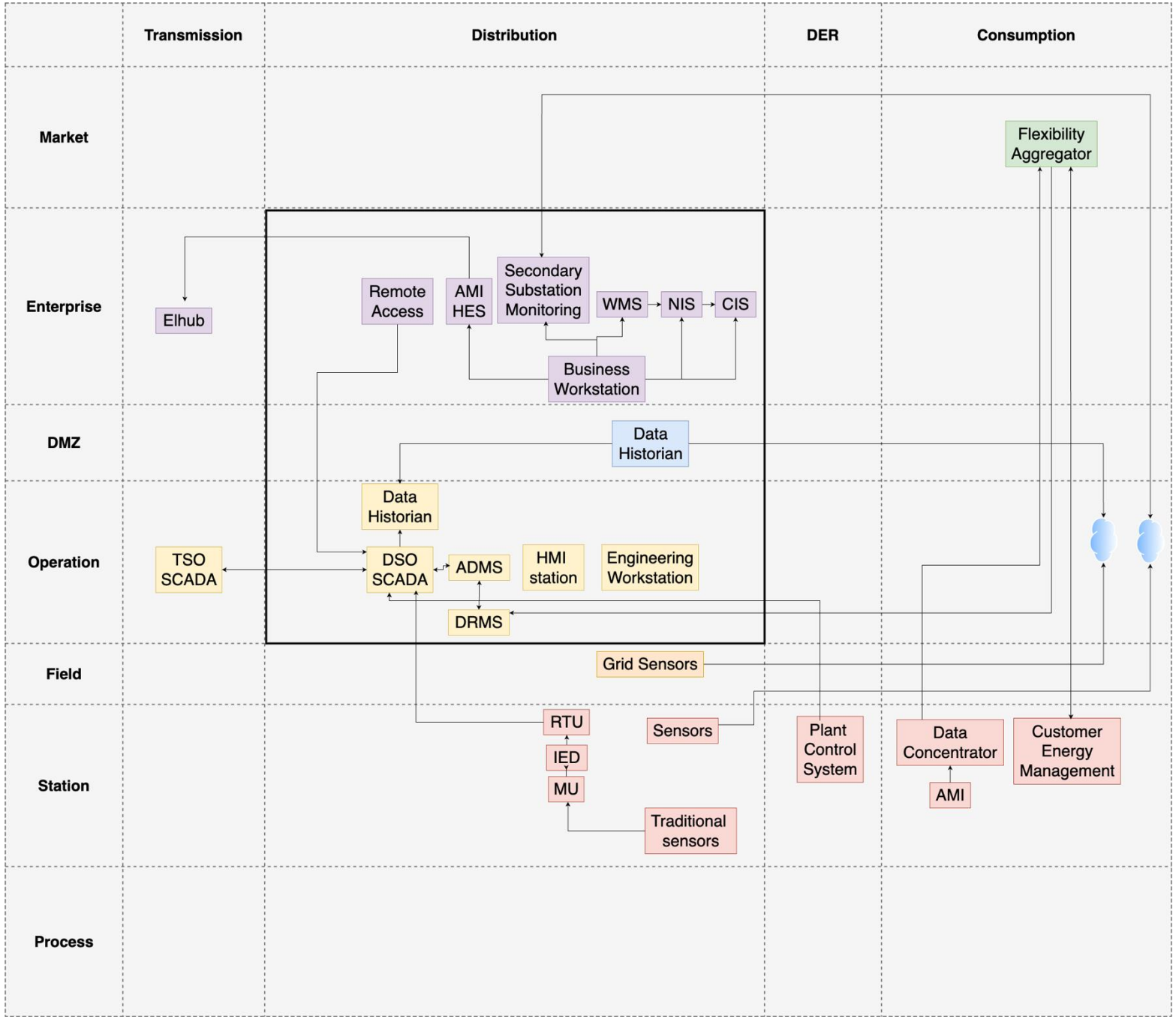
Inkludering- og ekskluderingskriterier

Inkluder teknikk/motiltak dersom det handler om...	Ekskluder teknikk/mottiltak dersom det handler om...
Nettverkstopologi	Sosial manipuleringsangrep
Plassering av systemet	Brukerrettigheter på sluttbrukernivå
API konfigurasjon som har innvirkning på arkitekturen	Sluttbrukerbeskyttelse og riktig konfigurasjon
Konfigurasjon av sikkerhetselementer	
Konfigurasjon av nettverksselementer	
Fjernstyring	
Plassering av data historian	


# of occurences in the selected techniques
25
20
15
10
5
0
Network Segmentation
Network Allowlists
Out-of-Band Communications Channel
Communication Authenticity
Software Process and Device Authentication
Human User Authentication
Data Backup
Filter Network Traffic
Access Management
Authorization Enforcement
Static Network Configuration
Redundancy of Service
Disable or Remove Feature or Program
Network Intrusion Prevention

Hvordan har vi gjort det?

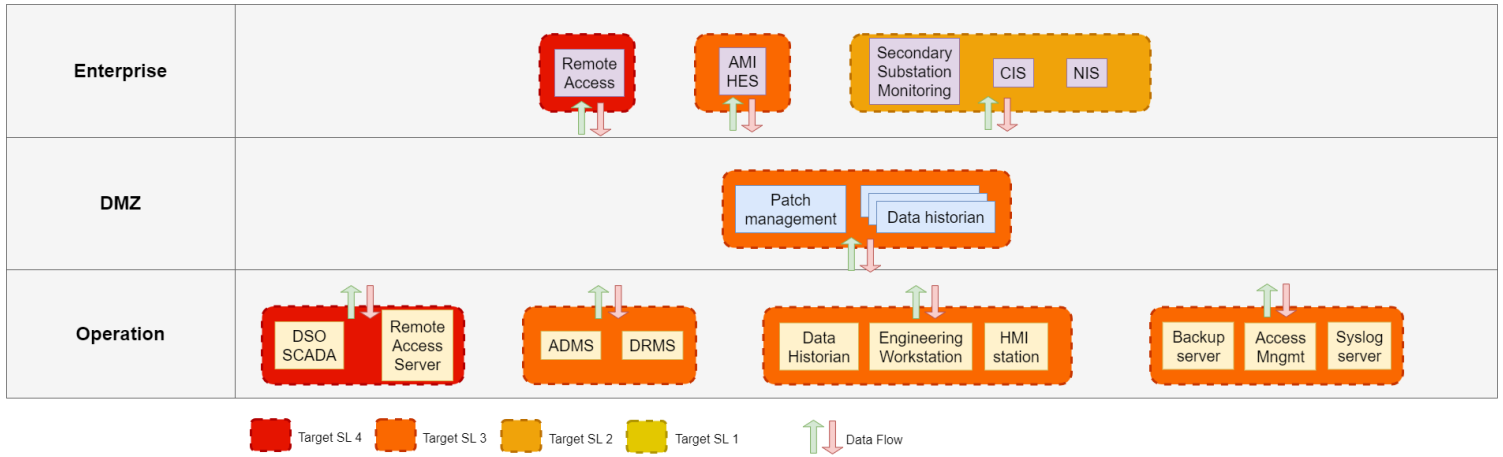



Transmission
Distribution
DER
Consumption
Market
Enterprise
DMZ
Operation
Field
Station
Process
Flexibility Aggregator
Elhub
Remote Access
AMI HES
Secondary Substation Monitoring
WMS
NIS
CIS
Business Workstation
Data Historian
Data Historian
TSO SCADA
DSO SCADA
ADMS
HMI station
Engineering Workstation
DRMS
Grid Sensors
RTU
IED
MU
Sensors
Traditional sensors
Plant Control System
Data Concentrator
AMI
Customer Energy Management

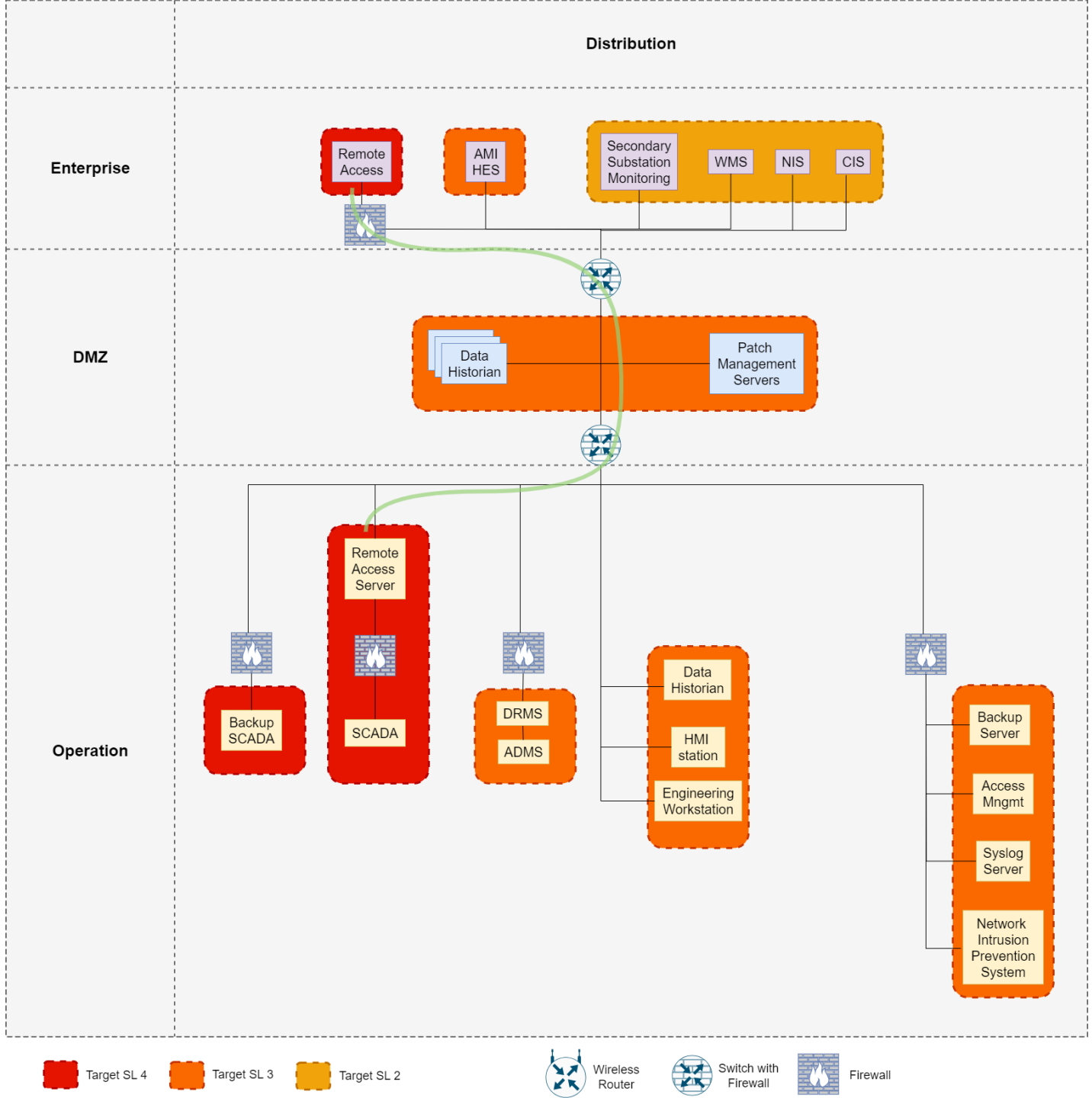
Antakelser

- Fokuset ligger kun på systemer tilkoblet driftssentralen.
- Kommunikasjonen mellom smartmålere og AMI HES er forenklet.
- Feltenheter, og microgrids er ikke en del av omfanget.
- Antallet historians er forenklet i figuren.
- Digitale tvillinger vil ha en tilsvarende plassering som ADMS og er derfor ekskludert.
- Nettverk IPS og IDS vil trolig finnes for industrielle nettverk i fremtiden.

Soner og kanaler fra IEC 62443



- Konkrete sikkerhetskrav
  - Skille IT og OT systemer
  - Skille kritiske systemer fra øvrige OT systemer
  - Separere fjernstyring
  - Skille trådløs og kablet kommunikasjon


Distribution
Enterprise
Remote Access
AMI HES
Secondary Substation Monitoring
WMS
NIS
CIS
DMZ
Data Historian
Patch Management Servers
Operation
Remote Access Server
Backup SCADA
SCADA
DRMS
ADMS
Data Historian
HMI station
Engineering Workstation
Backup Server
Access Mngmt
Syslog Server
Network Intrusion Prevention System
Target SL 4
Target SL 3
Target SL 2
Wireless Router
Switch with Firewall
Firewall

Implikasjoner av fremtidig teknologi I driftssentralen

- Realistisk sikkerhetsnivå i IEC 62443
- Hva slags ansvarsfordeling har skyløsninger i driftssentralen?
- Tilgangen til leverandører av sensorer og IoT enheter

Konklusjon

- Vi trenger en sikkerhetsarkitektur som sikrer driften av nettet.
- Men: vi trenger mer enn bare sikkerhetsarkitektur.

SINTEF

Teknologi for et bedre samfunn