Fælles sprog på elnettet

Hvorfor er det vigtigt med samme sprog, når elnettet i fremtiden bliver mere decentral og mere mangfoldig?

Claus Amtrup Andersen

Direktør i EURISCO

Medlem af S-557 samt TC57 WG15 (Datasikkerhed) og WG17 (DER)

EURISCO
RESEARCH & DEVELOPMENT

EURISCO ApS

softwareudvikling for energisystemer

- ✓ Dansk virksomhed etableret i 1994
- ✓ Specialister indenfor standardiseret datakommunikation
- ✓ Læs mere om hvad vi kan tilbyde på **www.eurisco.dk**

S-557 (TC57 Dansk National komite)

IEC TC57 WG17 (Distributed Energy Resources)

Project leder for TR61850-90-8 (TC57 WG17) now JWG11

IEC TC57 WG15 (Security)

S-454 (EV Dansk National komite)

IEC TC69 WG4 (EV Power supplies and chargers)

IEC/ISO JWG V2G Communication Interface (TF leader)

CEN/CENELEC

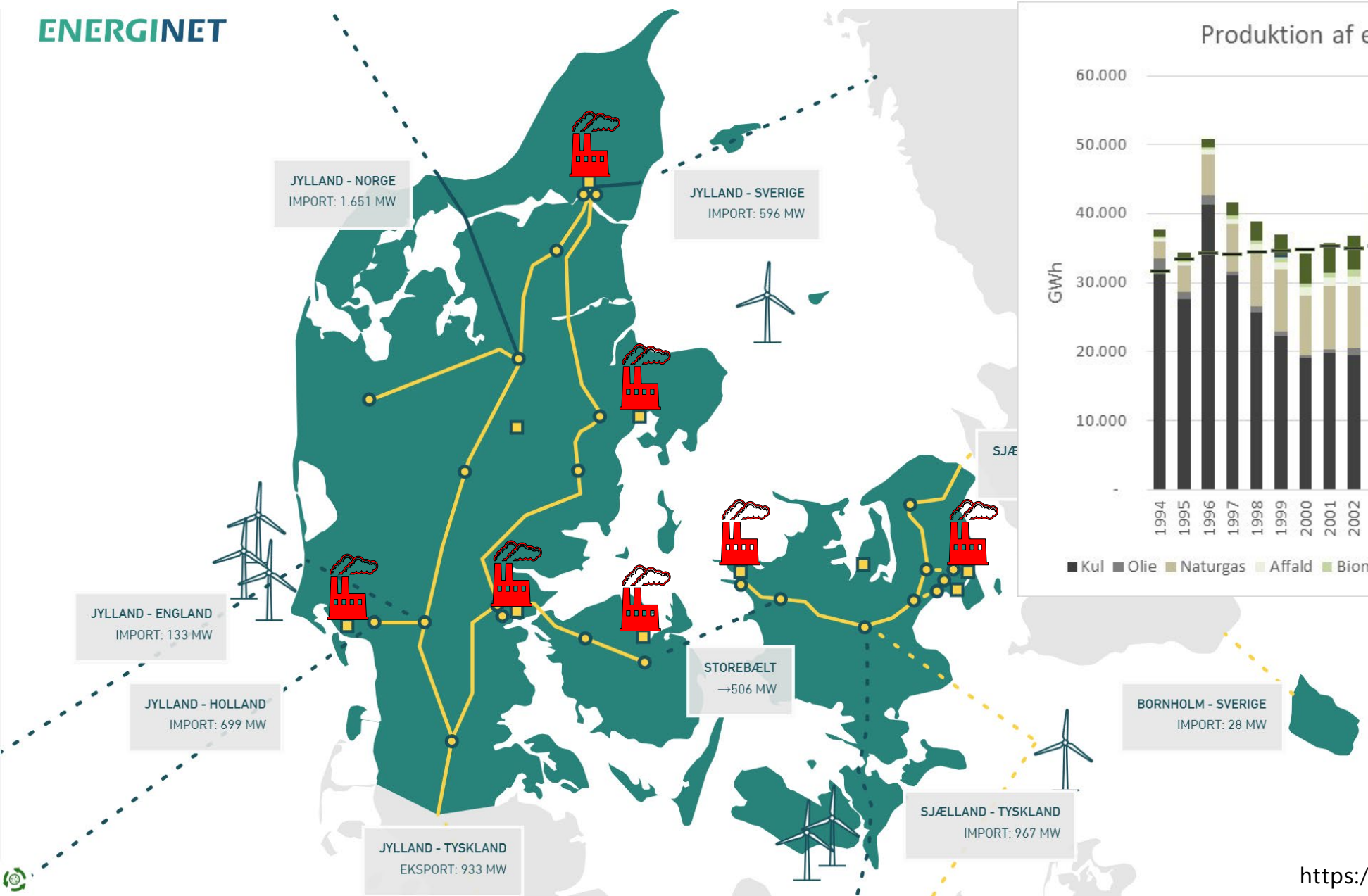
Project leader for CEN/CENELEC EV Focus Group for 'EV Communication'

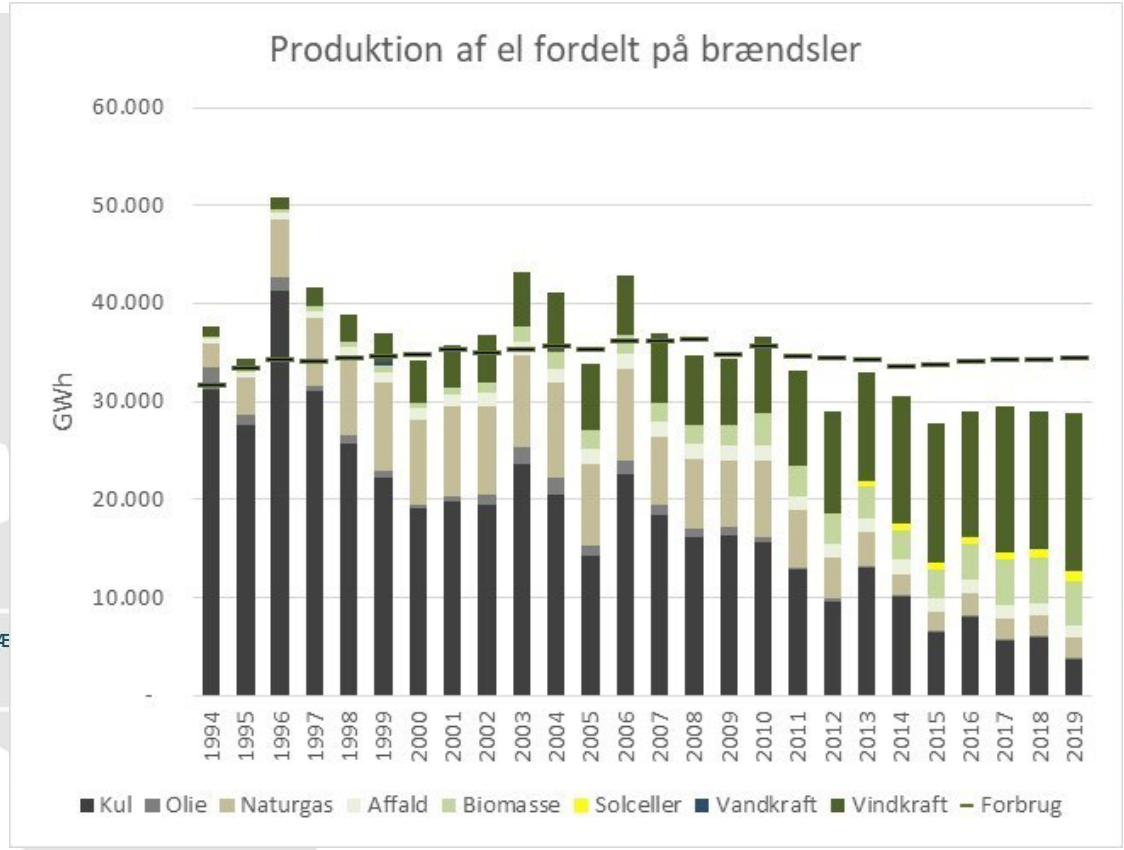
Raporteur between M468 and M490 (**SG-CG steering group member**)

Chairman for the 'EM-AhG-SmartCharge' under CEN/CENELEC

EURISCO
RESEARCH & DEVELOPMENT

Tidligere var produktionen primært '**central**'





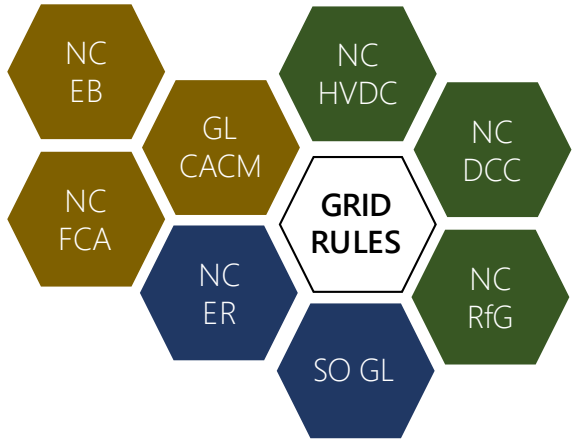
https://energinet.dk/energisystemet-lige-nu/

Sikker datakommunikation for kritisk infrastruktur

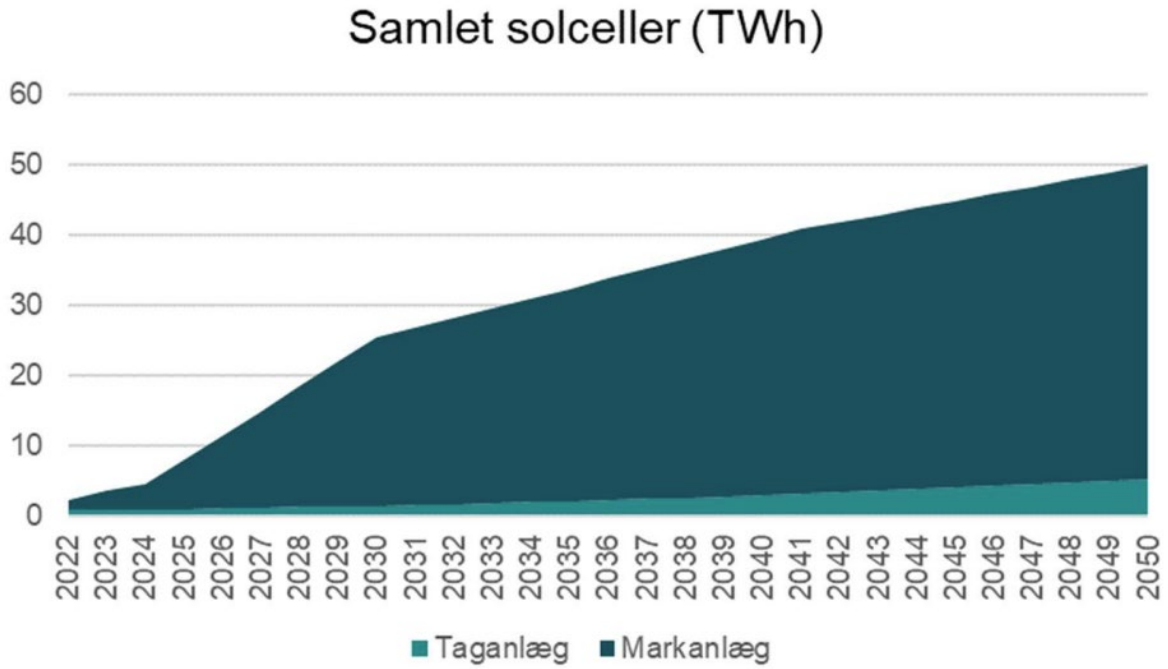
Operatører af nettilsluttede energianlæg har brug for datakommunikation som er:

- Sikker
- Standardiseret
- Stabilt, hurtigt og effektivt.

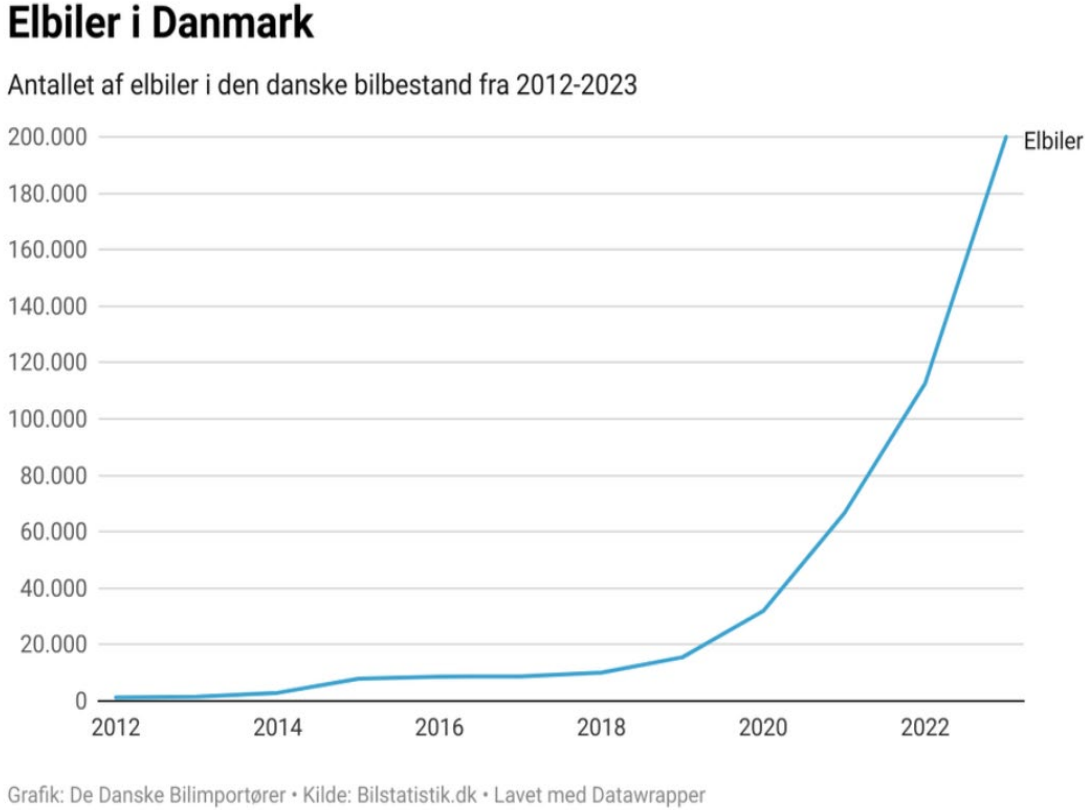
New European Grid Codes



I dag og fremover er produktionen mere '**decentral**'

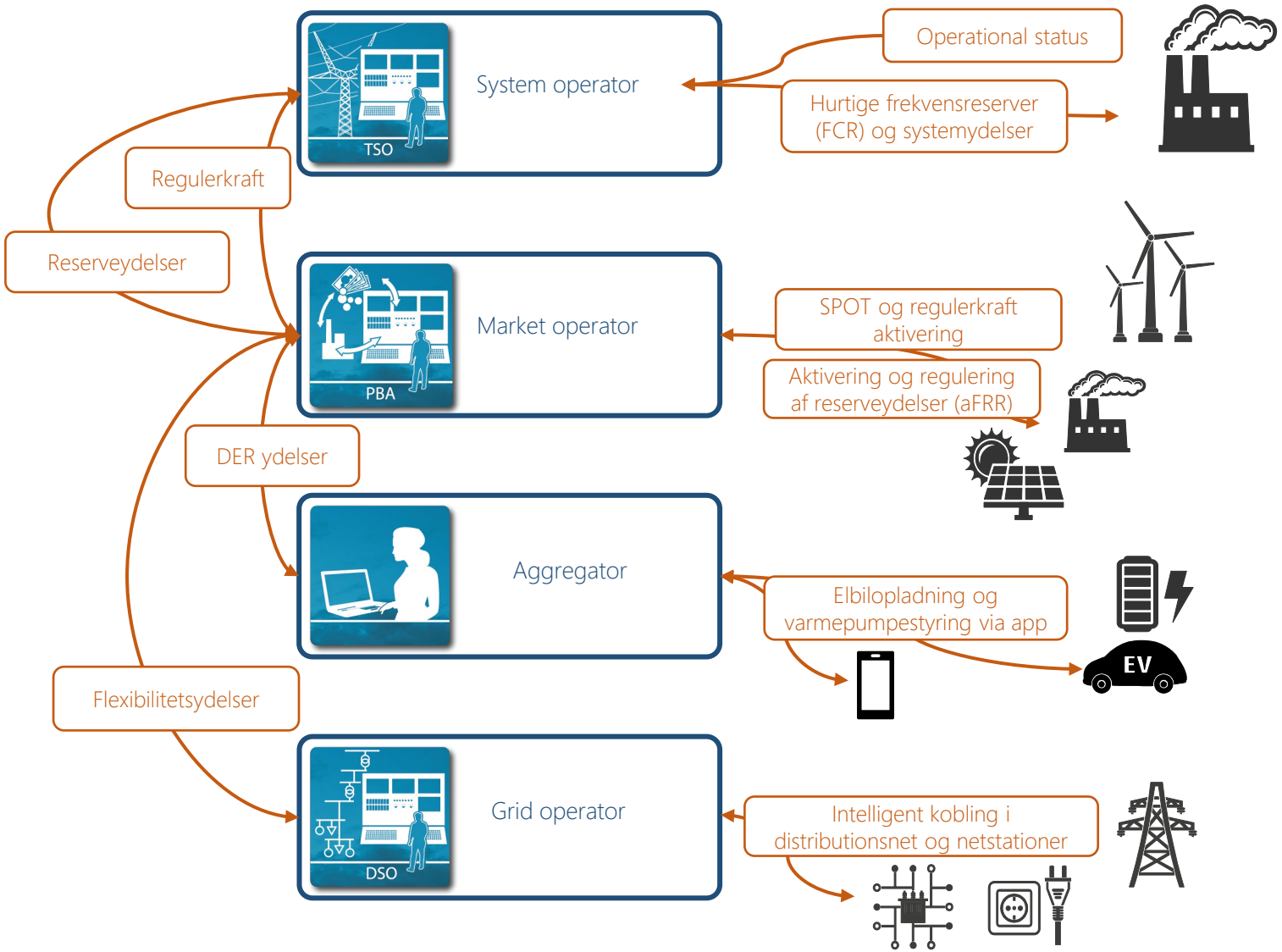


https://ens.dk/sites/ens.dk/files/Hoeringer/af22_-_baggrundsnotat_-_solceller.pdf



...og **forbruget** mere flexibelt

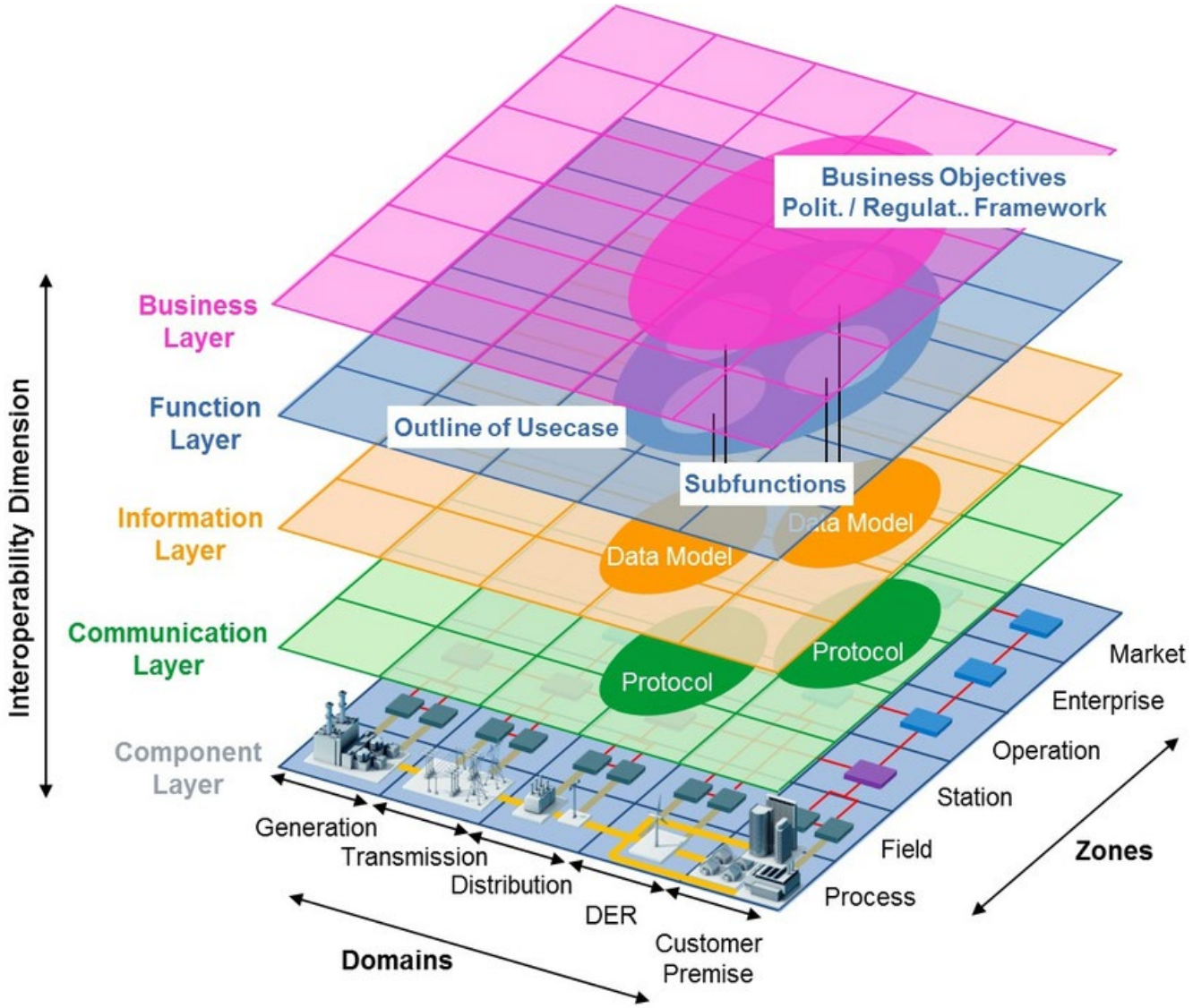
Datakommunikation til DER (Distributed Energy Resources)



Den klassiske datakommunikation mellem nutidens energianlæg er designet til et el-system, som var centralstyret med forudsigelige forbrugsmønstre, samt med en produktion, som kunne reguleres efter et til tider øget behov.

Denne forudsigelige og stabile produktion hører dog fortiden til, hvorfor der nu er et endnu større behov for en fælles datakommunikation på elnettet i takt med, at fremtidens elproduktion øges, decentraliseres og diversificeres.

SGAM (Smart Grid Architecture Model)



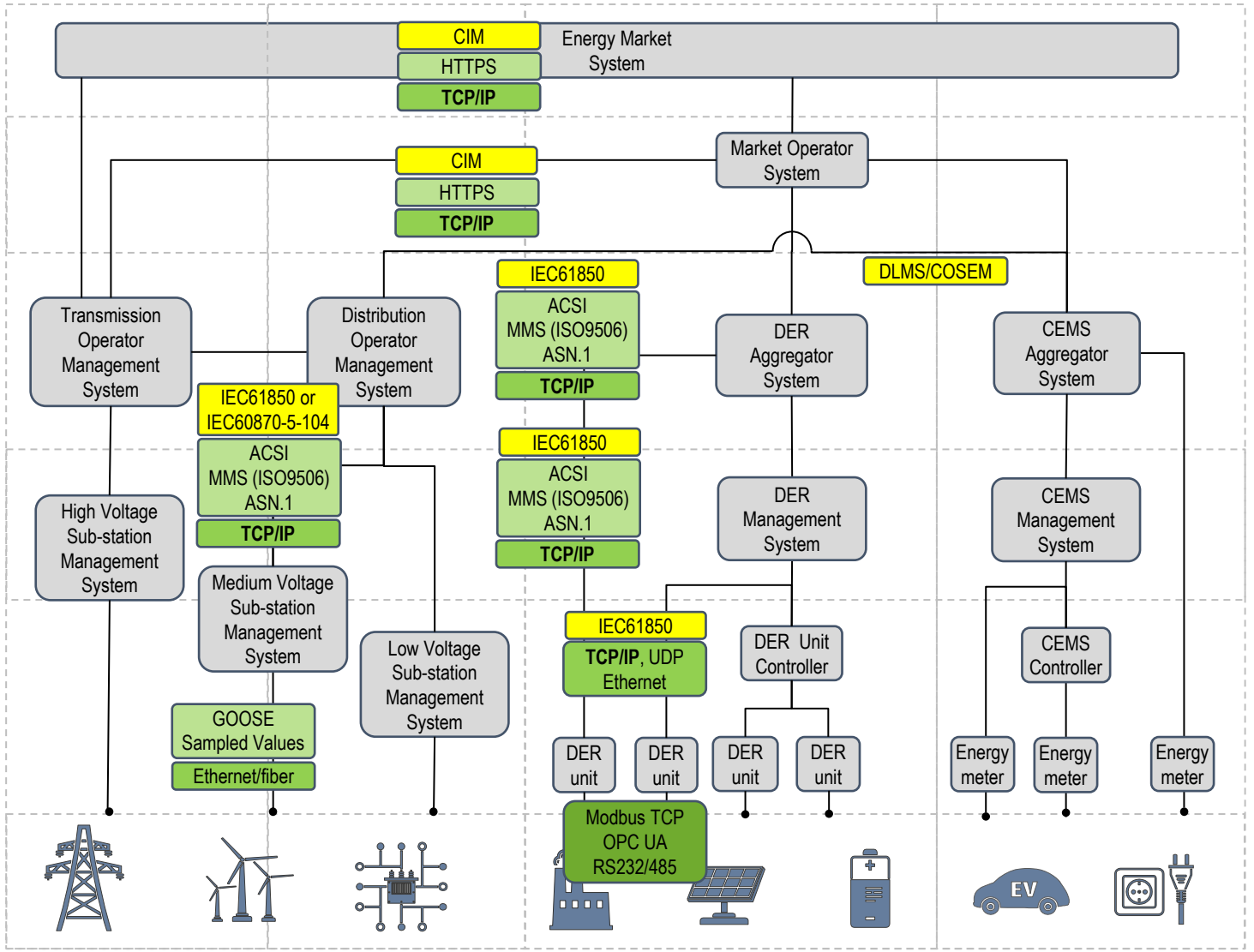
For at sikre interoperabilitet imellem internationale standarder, benyttes en model kaldet SGAM

SGAM modellen arbejder med et under-liggende komponentniveau, som afspejler den fysiske verden med domæner og zoner.

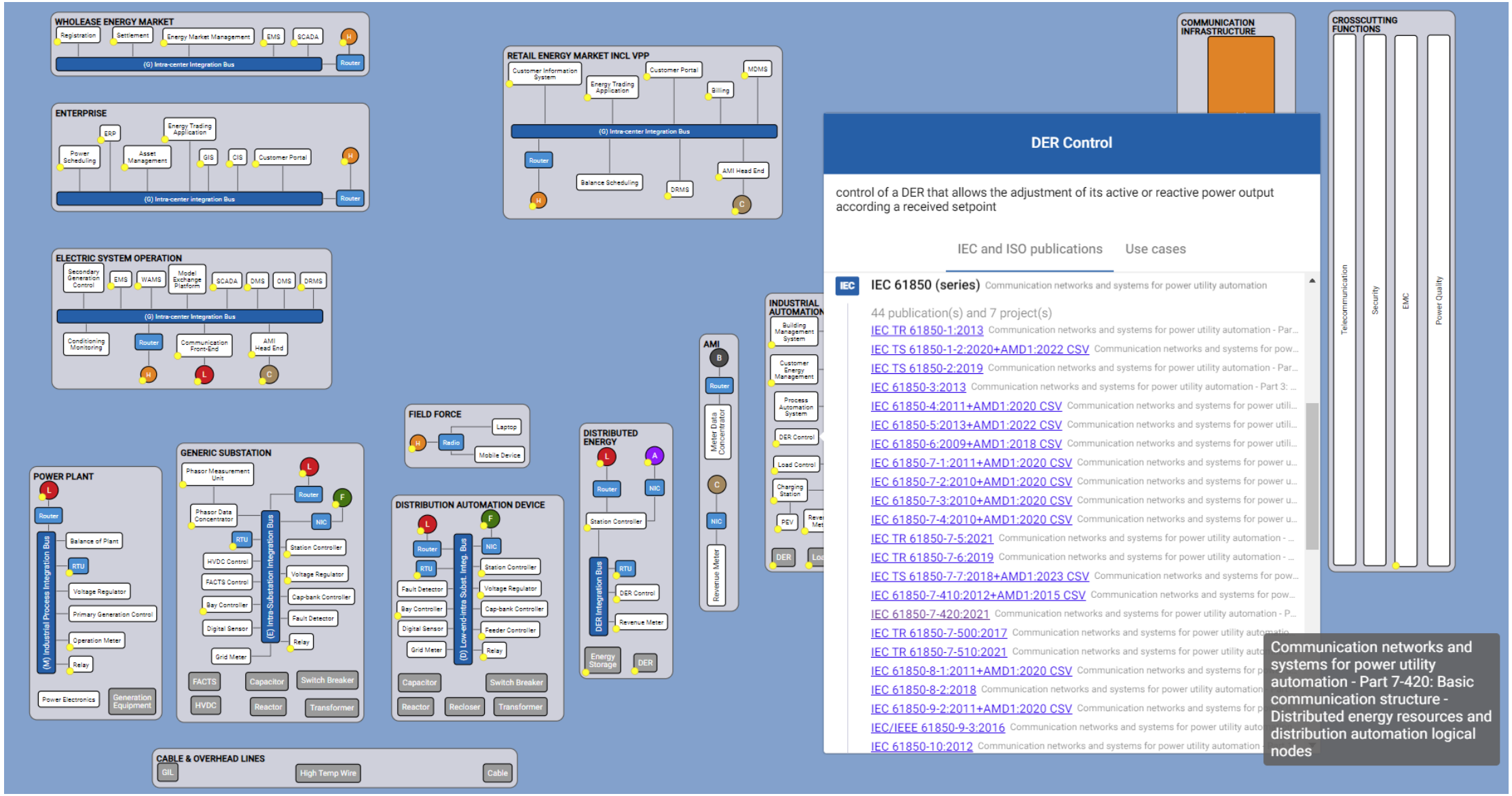
Oven på de fysiske komponenter, mappes så 4 niveauer, bestående af:

- Kommunikationsteknologier
- Informationsmodeller
- Funktioner (tekniske use-cases)
- Forretning (ikke tekniske use-cases)

SGAM communication / information layer



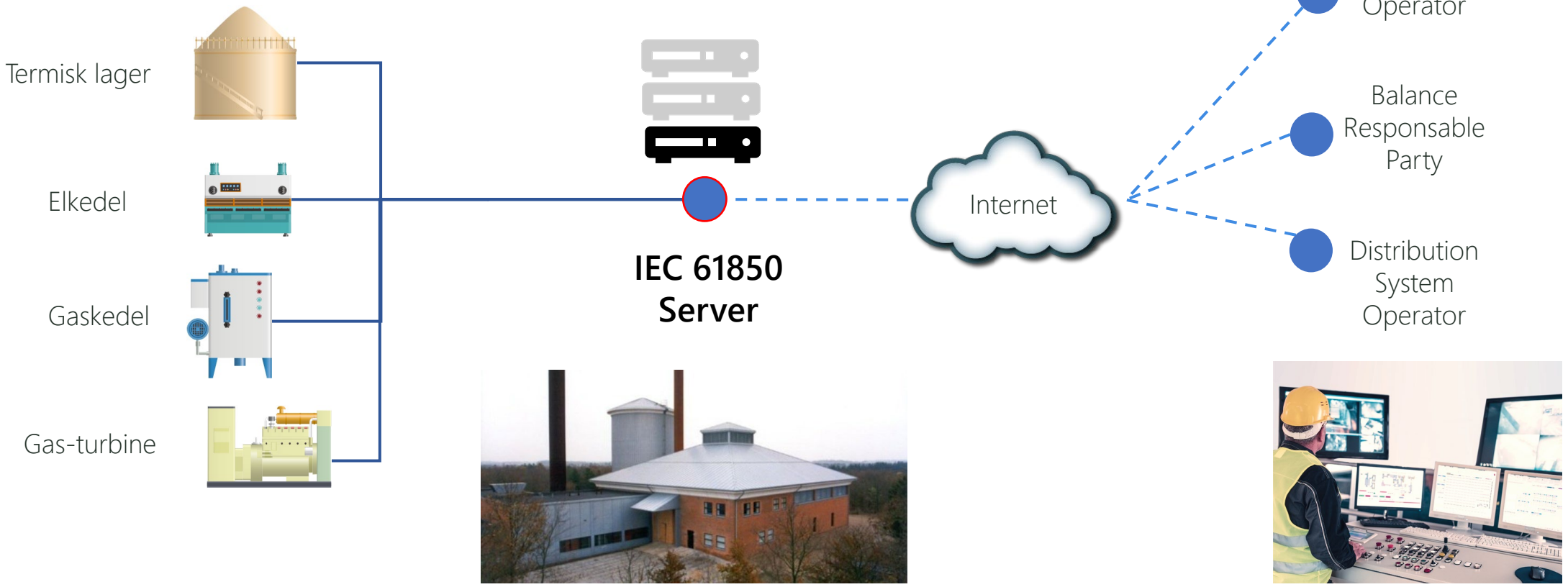
International IEC standards for DER (Distributed Energy Resources)



https://mapping.iec.ch/#/maps/1

Hvorfor benytte IEC 61850 datakommunikation?

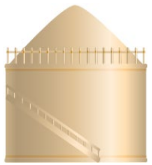
- Event driven (outbound) server eller polling fra klient
- Data hentes ved 'kilden'
- Delt adgang mellem flere aktører – anlægget ejer datagateway (IEC 61850 server)



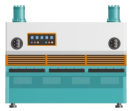
IEC 61850 standard for navngivning af signaler

Unique international identifier for det specifikke anlæg > f.eks.: **Ribe Fjernvarme (...4Y)**

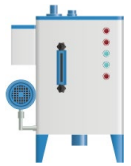
EIC45W00...4Y_HD2EB1/MMXU1.TotW.mag.f



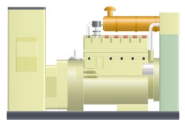
Termisk lager	EIC45W0000000000004Y_AF/MHET1.HeatOut.mag.f}: EIC45W0000000000004Y_HD1CP1/DCTS1.ThmCapTot.mag.f}: EIC45W0000000000004Y_HD1CP1/DCTS1.ThmIn.mag.f}: EIC45W0000000000004Y_HD1CP1/DCTS1.ThmOut.mag.f}:



Elkedel	EIC45W0000000000004Y_HD2EB1/DCTS1.ThmOut.mag.f}: EIC45W0000000000004Y_HD2EB1/DRCC1.OutWSet.setMag.f}: EIC45W0000000000004Y_HD2EB1/DRCS1.CsmpRsvDn.mag.f}: EIC45W0000000000004Y_HD2EB1/DRCS1.CsmpRsvUp.mag.f}: EIC45W0000000000004Y_HD2EB1/DRCT1.MaxWLim.setMag.f}: EIC45W0000000000004Y_HD2EB1/DRCT1.MinWLim.setMag.f}: EIC45W0000000000004Y_HD2EB1/MMXU1.TotW.mag.f}:



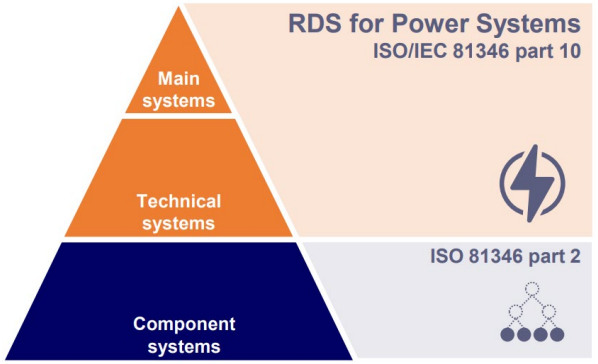
Gaskedel	EIC45W0000000000004Y_HD3EM1/DCTS1.ThmOut.mag.f}: EIC45W0000000000004Y_HD4EM1/DCTS1.ThmOut.mag.f}:



Gas-turbine	EIC45W0000000000004Y_HG1GA1/DRCC1.OutWSet.setMag.f}: EIC45W0000000000004Y_HG1GA1/DRCT1.MaxWLim.setMag.f}: EIC45W0000000000004Y_HG1GA1/DRCT1.MinWLim.setMag.f}: EIC45W0000000000004Y_HG1GA1GA/MMXU1.TotW.mag.f}: EIC45W0000000000004Y_HG1GA2/DRCC1.OutWSet.setMag.f}: EIC45W0000000000004Y_HG1GA2/DRCT1.MaxWLim.setMag.f}: EIC45W0000000000004Y_HG1GA2/DRCT1.MinWLim.setMag.f}: EIC45W0000000000004Y_HG1GA2GA/MMXU1.TotW.mag.f}: EIC45W0000000000004Y_HG1GA3/DRCC1.OutWSet.setMag.f}: EIC45W0000000000004Y_HG1GA3/DRCT1.MaxWLim.setMag.f}: EIC45W0000000000004Y_HG1GA3/DRCT1.MinWLim.setMag.f}: EIC45W0000000000004Y_HG1GA3GA/MMXU1.TotW.mag.f}: EIC45W0000000000004Y_HG1GA4/DRCC1.OutWSet.setMag.f}: EIC45W0000000000004Y_HG1GA4/DRCT1.MaxWLim.setMag.f}: EIC45W0000000000004Y_HG1GA4/DRCT1.MinWLim.setMag.f}: EIC45W0000000000004Y_HG1GA4GA/MMXU1.TotW.mag.f}: EIC45W0000000000004Y_HG1GA5/DRCC1.OutWSet.setMag.f}: EIC45W0000000000004Y_HG1GA5/DRCT1.MaxWLim.setMag.f}:

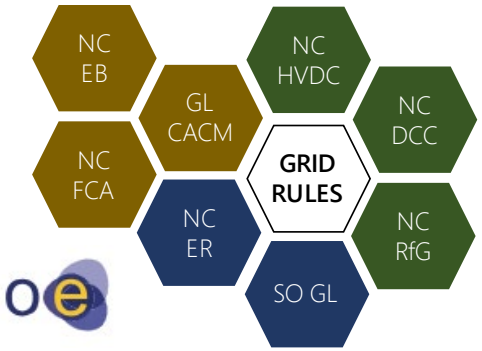
Sektor specifik Reference Designator System (RDS) som defineret i IEC 81346
> **Heat Supply System**
> **Electrical Boiler**

IEC61850-7-420 navngivning
Measurement (MMXU)
Total Real Power (TotW)
Mag.f (analog float value)

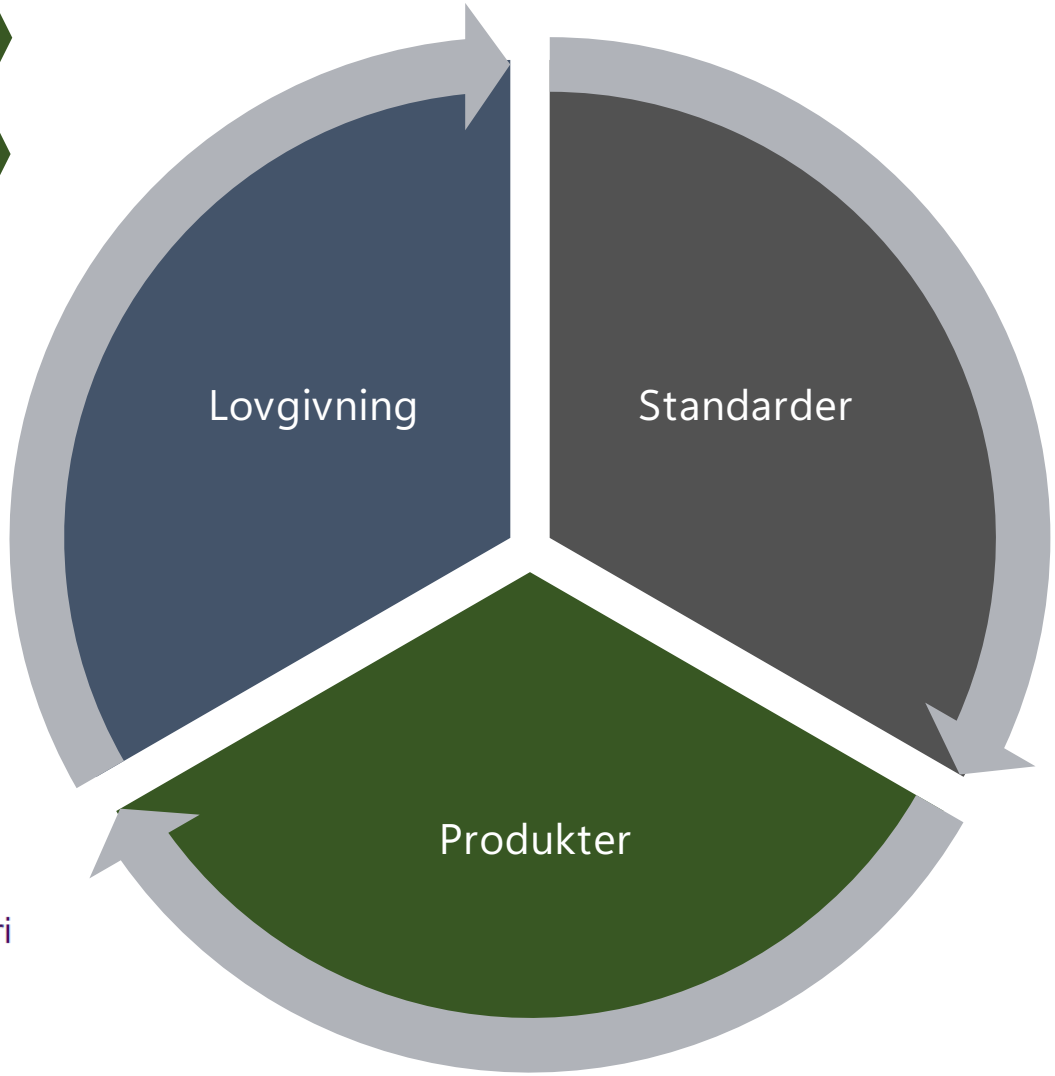


https://www.81346.com/81346-10

Det samlede system for S-557



entsoe

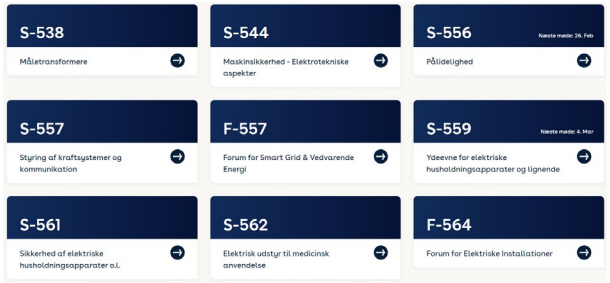


CEN CENELEC

IEC International Electrotechnical Commission

ISO Standards

DS DANSK STANDARD



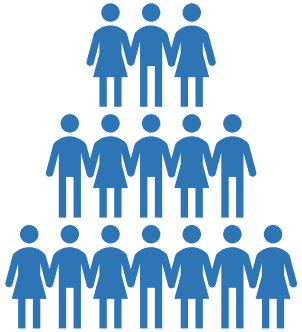
Energistyrelsen

ENERGINET

GREEN POWER DENMARK

DANSK FJERNVARME

Dansk Industri



Cybersikkerhed

Få et overblik over hvad der findes af angrebsmuligheder indenfor Industrielle Control Systemer

MITRE | ATT&CK® Matrices Tactics Techniques Defenses CTI Resources Benefactors Blog Search

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	9 techniques	6 techniques	2 techniques	6 techniques	5 techniques	7 techniques	11 techniques	3 techniques	14 techniques	5 techniques	12 techniques
Drive-by Compromise	Change Operating Mode	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	Command-Line Interface	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	Execution through API	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	Graphical User Interface	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	Hooking	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image		Change Credential		Loss of Productivity and Revenue
Replication Through Removable Media	Native API					Valid Accounts	Monitor Process State		Data Destruction		Loss of Protection
Rogue Master	Scripting						Point & Tag Identification		Denial of Service		Loss of Safety
Spearphishing Attachment	User Execution						Program Upload		Device Restart/Shutdown		Loss of View
Supply Chain Compromise							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		

T0885

Commonly Used Port

Adversaries may communicate over a commonly used port to bypass firewalls or network detection systems and to blend in with normal network activity, to avoid more detailed inspection. They may use the protocol associated with the port, or a completely different protocol. They may use commonly open ports, such as the examples provided below.

- TCP:80 (HTTP)
- TCP:443 (HTTPS)
- TCP/UDP:53 (DNS)
- TCP:1024-4999 (OPC on XP/Win2k3)
- TCP:49152-65535 (OPC on Vista and later)
- TCP:23 (TELNET)
- UDP:161 (SNMP)
- TCP:502 (MODBUS)
- TCP:102 (S7comm/ISO-TSAP)
- TCP:20000 (DNP3)
- TCP:44818 (Ethernet/IP)

ID: T0885
Sub-techniques: No sub-techniques
Tactic: Command and Control
Platforms: None
Contributors: Matan Dobrushin - Otorio
Version: 1.1
Created: 21 May 2020
Last Modified: 13 October 2023

Version Permalink

Procedure Examples

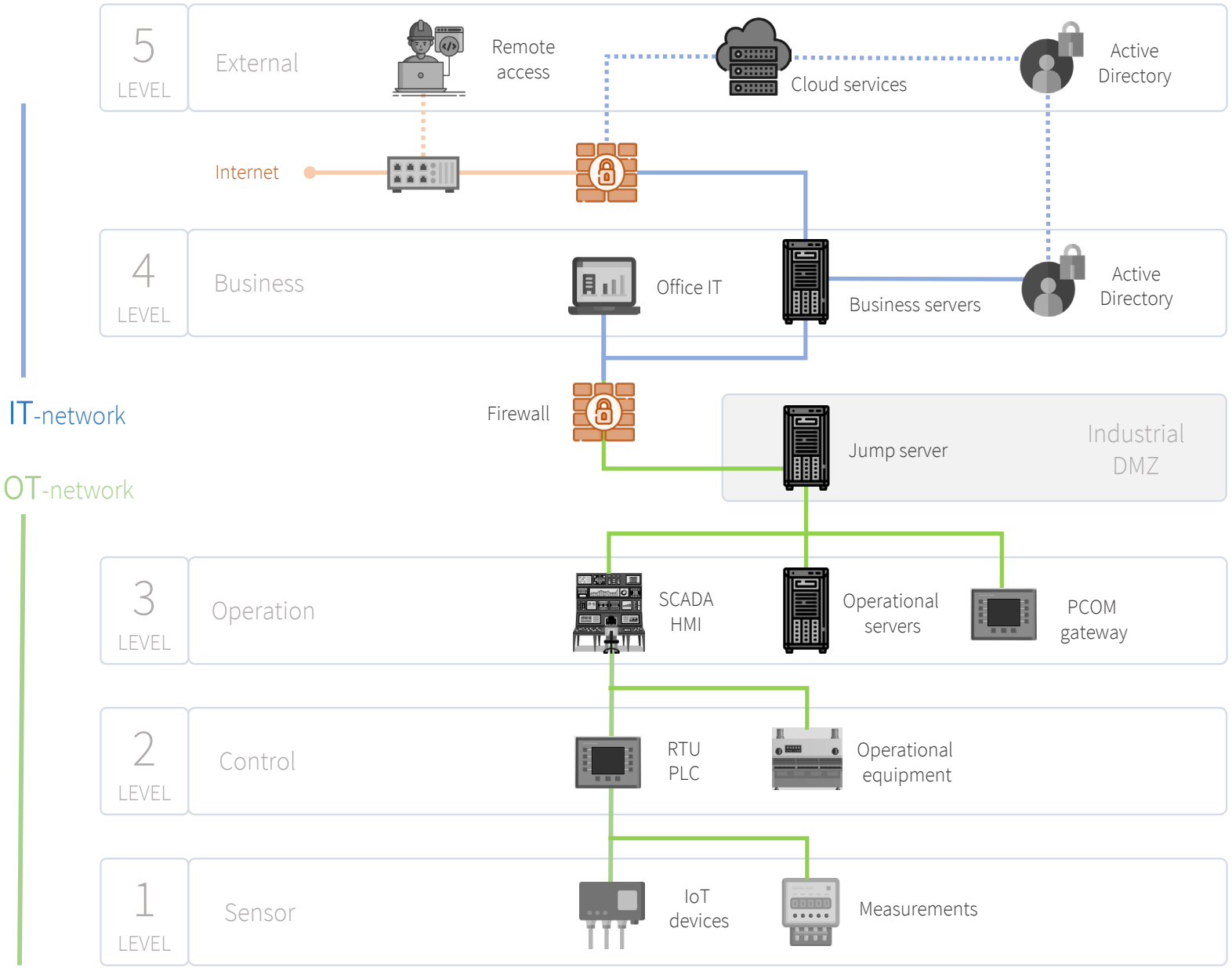
Prøv f.eks. at læse mere om Sandworm angrebet på Ukraines elsystem i 2015

ID	Name	Description
C0028	2015 Ukraine Electric Power Attack	During the 2015 Ukraine Electric Power Attack, Sandworm Team used port 443 to communicate with their C2 servers. [1]
S0603	Stuxnet	Stuxnet attempts to contact command and control servers on port 80 to send basic information about the computer it has compromised. [2]
S1009	Triton	Triton uses TriStations default UDP port, 1502, to communicate with devices. [3]

Targeted Assets

ID	Asset
A0008	Application Server
A0007	Control Server
A0009	Data Gateway

https://attack.mitre.org/matrices/ics/



IT/OT-sikkerhed

Purdue-modellen benyttes gerne når der indenfor IT/OT arbejdes med sikring af netværk.

Segmentering mellem IT og OT er væsentlig når man har at gøre med kritisk infrastruktur.

DER er typisk i OT segmentet og idet der er tale om energianlæg som kommunikere via internettet, stilles der særlige krav til:

Autentificering (hvem kommunikeres der med)
Kryptering (af både transport og data)
Auditering (logning af data og validering)
Genopretning (backup/restore)

Vigtige sikkerhedsstandarder:

X.509, X-510 (certificate)

IEC 62443-4-1, 4-2 (requirements)

IEC 62351-3, -4, -8, -9

(E2E encryption, RBAC, key management)

IEC61850 (Client)

Transport layer:
TLS 1.2 (IEC 62351-3)

Application layer:
E2E security (IEC 62351-4)

Internet

VPN/SSH: Customer specific

FlexGrid
a simple solution to a complex problem

POWER PLAN

Hvordan bruger vi standarderne?

Internet router

Firewall (IT)

IEC61850 (Server)
RBAC (IEC 62351-8)

DMZ

Ethernet 1

IEC 61850
Secure MMS

CERTIFIED DATA GATEWAY
Server

Ethernet 2

Modbus TCP
OPC UA

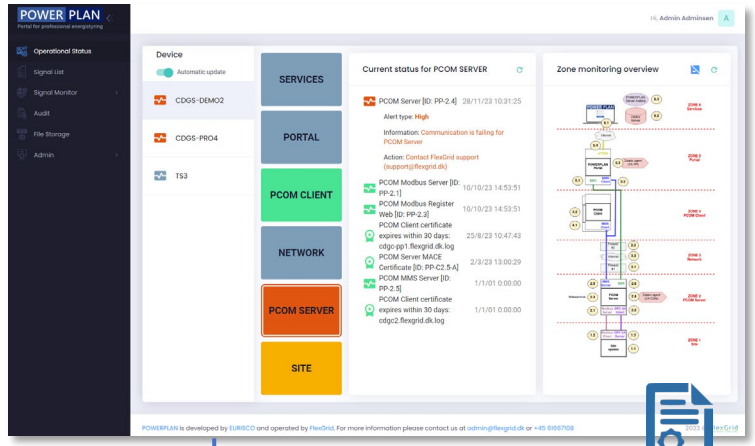
Firewall (OT)

Kraftvarmeværk

Protection relay

PLC/RTU Controllers

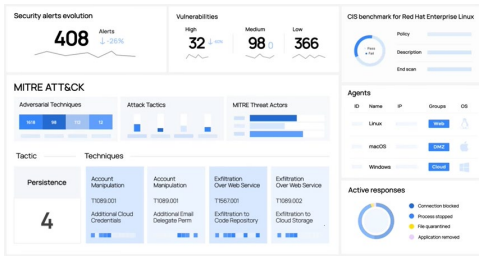
SCADA



Security information and event management

CIS Controls (IEC 62443)

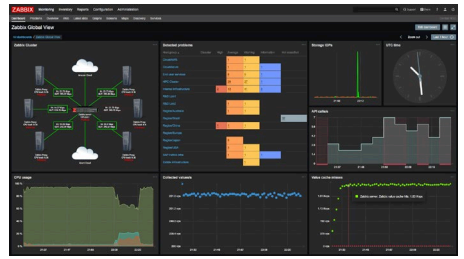
wazuh.



Certificate handling SSL/TLS/MACE (X.509)

Key Management (IEC 62351-9)

ZABBIX



EURISCO
RESEARCH & DEVELOPMENT

Tak for opmærksomheden
Spørgsmål?

Claus Amtrup Andersen

Kan kontaktes på: caa@eurisco.dk

EURISCO
RESEARCH & DEVELOPMENT