Sikkerhed i El-målere

Sommerhack – 2020

Thomas Ljungberg Kristensen, thomas@welcomesecurity.net

Thomas Ljungberg Kristensen

96 Aarhus Universitet, Datalog

03 Systematic, Systems Engineer

07 Danske Bank, Developer

12 Kamstrup, Systems Engineer

14 FortConsult, Senior Security Consultant

15 WelcomeSecurity, Security Advisor

19 OWASP, Co-chapter Lead - Aarhus

19 Deloitte, Senior Manager, Cyber

20 Norlys, IT security architect

Dette er mine holdning og repræsenterer ikke nogle af de virksomheder, som jeg har været eller er ansat ved!

DISCLAIMER

Hvorfor “smarte” el-måler

og er de smarte?

Hvorfor?

Præcis, korrekt og rimelig afregning

Bruger-involvering

Ny markedsmodeller

En nødvendighed for decentral strømproduktion

og så er det en EU regel 

Kamstrup, Echelon, Landis og Gyr

Hvad er smart?

OMNIPOWER® i korte træk

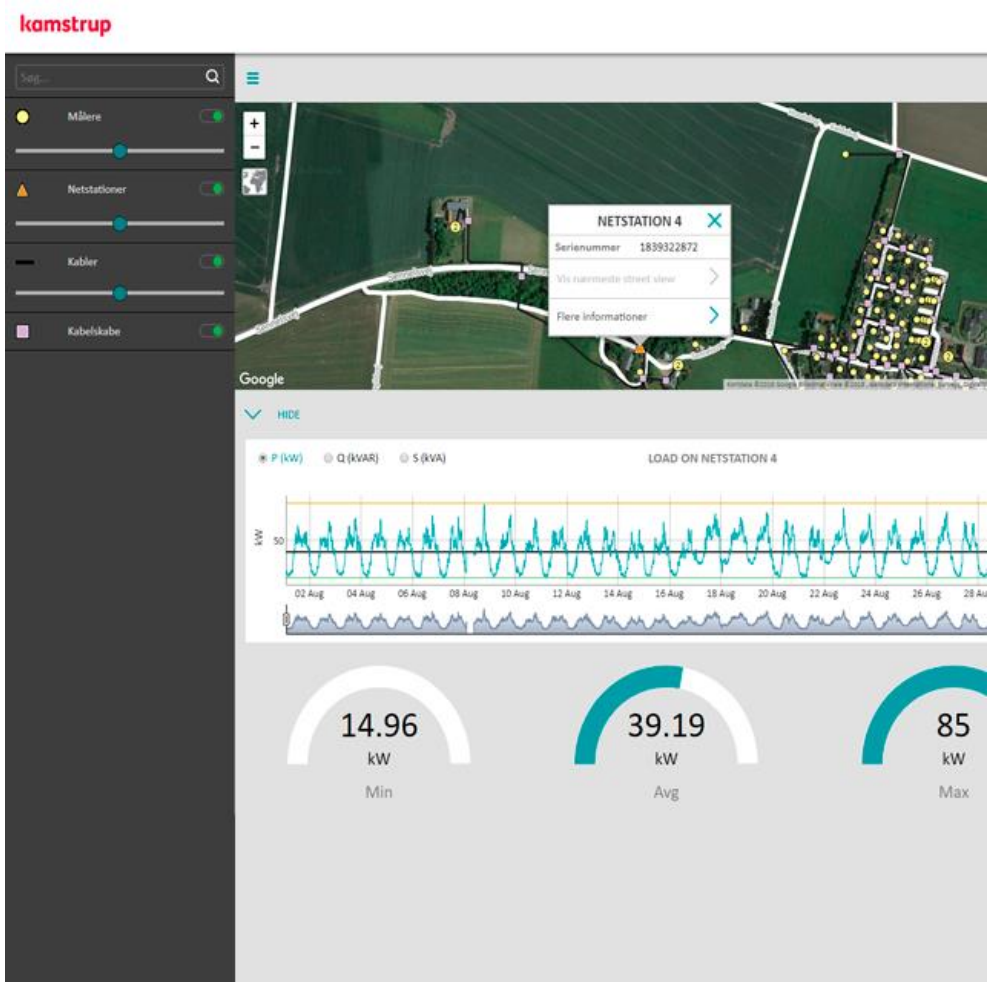
Målertype	OMNIPOWER® Enfaset	OMNIPOWER® Trefaset	OMNIPOWER® DIN-skinnemåler
			
Tilslutning	Direkte	Direkte	
Måleværdier	A+, A-, R+, R-, aktiv, reaktiv og tilsyneladende effekt – i alt og pr. fase. Middel RMS-spænding og RMS-strøm pr. fase, frekvens, effektfaktor og total harmonis		

Diverse	Energiregistre	Strømregistre
RTC med kvalitetsinfo	Aktiv positiv energi A+	Maks.-effekt P+maks.
Timetæller	Aktiv negativ energi A-	Maks.-effekt P+maks. RTC
Debiteringsstoptæller	Reaktiv positiv energi R+	Maks.-effekt P+maks. Tarif 1
Effekttærskeltæller (A+)	Reaktiv negativ energi R-	Maks.-effekt P+maks. Tarif 1 RTC
Pulsindgang	Tilsyneladende positiv energi E+	Maks.-effekt P+maks. Tarif 2
	Tilsyneladende negativ energi E-	Maks.-effekt P+maks. Tarif 2 RTC
	Aktiv positiv energi A+ Tarif 1	Akkumuleret maks.-effekt P+maks.
	Aktiv positiv energi A+ Tarif 2	Akkumuleret maks.-effekt P+maks. Tarif 1
	Aktiv positiv energi A+ Tarif 3	Akkumuleret maks.-effekt P+maks. Tarif 2
	Aktiv positiv energi A+ Tarif 4	Maks.-effekt Q+maks.
	Reaktiv positiv energi R+ Tarif 1	Maks.-effekt Q+maks. RTC
	Reaktiv positiv energi R+ Tarif 2	Maks.-effekt Q+maks. Tarif 1
	Reaktiv positiv energi R+ Tarif 3	Maks.-effekt Q+maks. Tarif 1 RTC
	Reaktiv positiv energi R+ Tarif 4	Maks.-effekt Q+maks. Tarif 2
		Maks.-effekt Q+maks. Tarif 2 RTC
		Akkumuleret maks.-effekt Q+maks.
		Maks.-effekt S+maks.
		Maks.-effekt S+maks. RTC
		Maks.-effekt S+maks.
		Maks.-effekt S+maks. RTC

Datalogger
Bryder
Tariffer

og meget mere

Hvad er smart?



Kilde: https://www.kamstrup.com/da-dk/elloesninger/dataanalyse-til-el

Smart Grid Reference Architecture

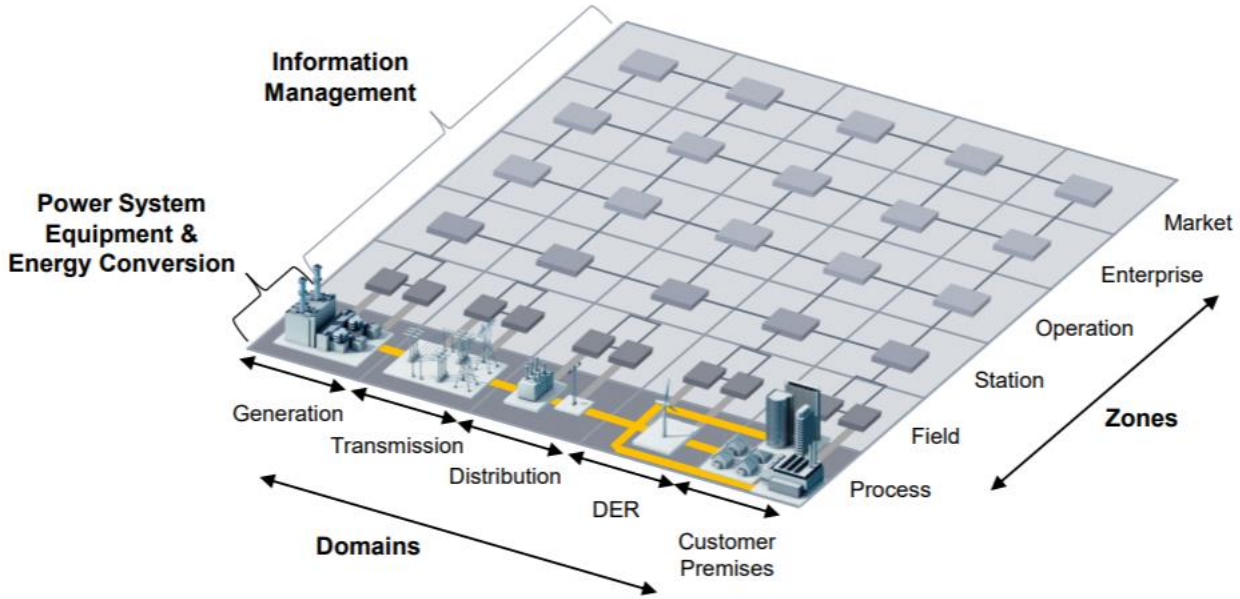


Figure 7: Smart Grid plane - domains and hierarchical zones

Kilde:https://ec.europa.eu/energy/sites/ener/files/documents/xpert_group1_reference_architecture.pdf

Smart Grid Reference Architecture

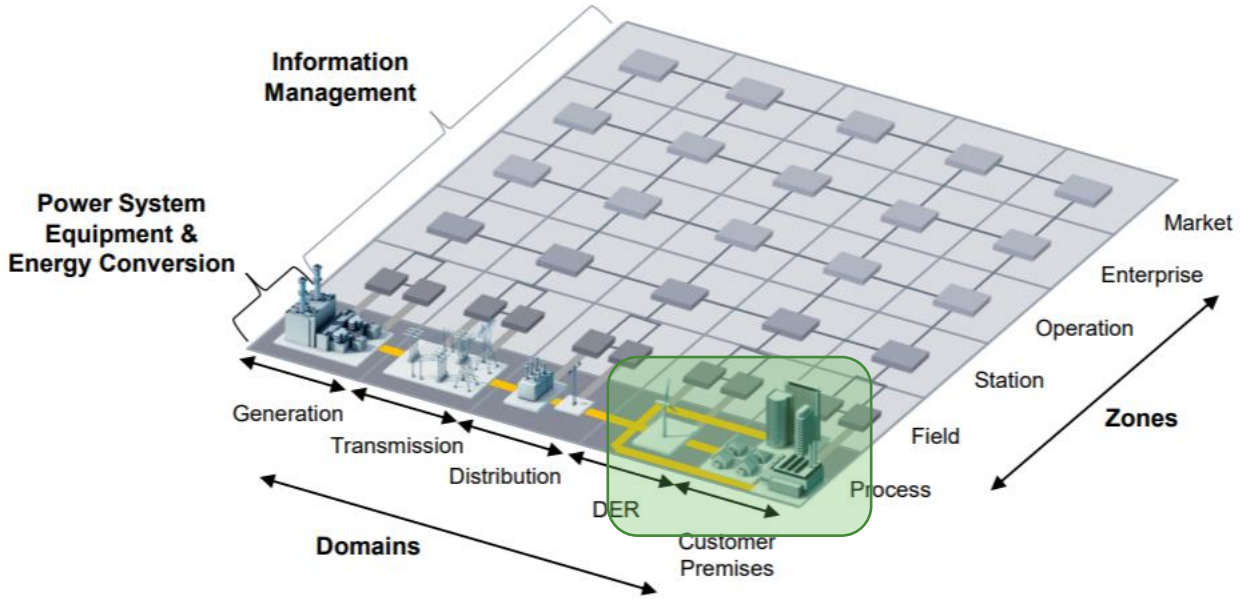


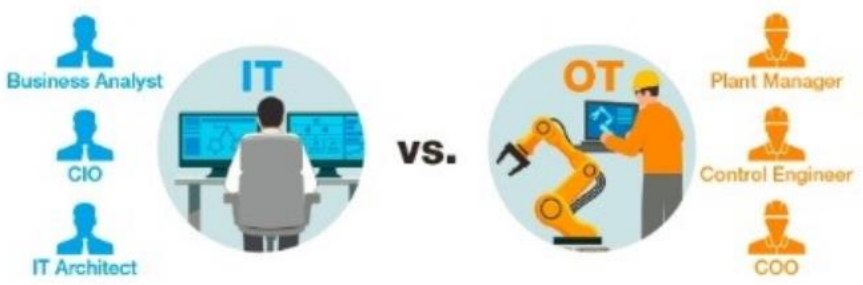
Figure 7: Smart Grid plane - domains and hierarchical zones

Kilde:https://ec.europa.eu/energy/sites/ener/files/documents/xpert_group1_reference_architecture.pdf

OT eller IT eller …

Gør det en forskel?

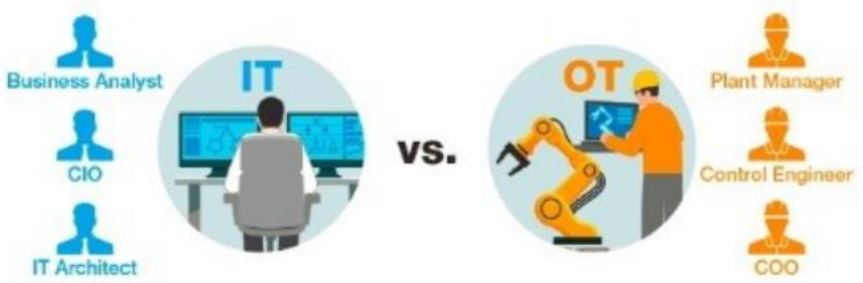
OT, IT eller noget helt andet?



Business Priority	Confidentiality	Availability
Major Focus	Data integrity	Zero downtime for control processes
Protection Targets	Windows computers, servers	Legacy industrial devices (PLC, HMI, meters)
Environmental Conditions	Air-conditioned	Harsh environments (extreme temperatures, vibrations, shocks)

Kilde: http://event.moxa.com/newsletter/connection/2019/08/feat_02.html

OT, IT eller noget helt andet?

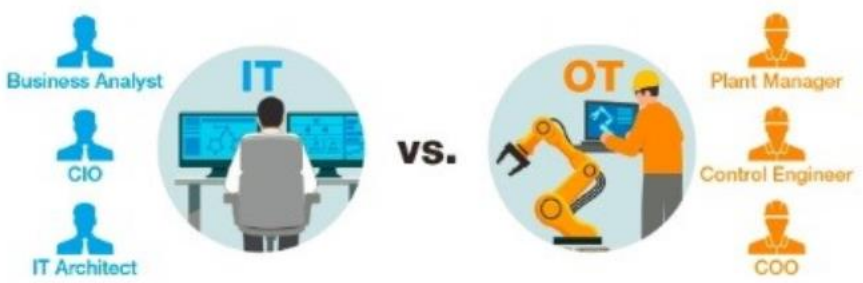


Business Priority	Confidentiality	Availability
Major Focus	Data integrity	Zero downtime for control processes
Protection Targets	Windows computers, servers	Legacy industrial devices (PLC, HMI, meters)
Environmental Conditions	Air-conditioned	Harsh environments (extreme temperatures, vibrations, shocks)

Af de større dele, ja
– men ikke af de enkle

Kilde: http://event.moxa.com/newsletter/connection/2019/08/feat_02.html

OT, IT eller noget helt andet?



Business Priority	Confidentiality	Availability
Major Focus	Data integrity	Zero downtime for control processes
Protection Targets	Windows computers, servers	Legacy industrial devices (PLC, HMI, meters)
Environmental Conditions	Air-conditioned	Harsh environments (extreme temperatures, vibrations, shocks)

Af de større dele, ja
– men ikke af de enkle

Ikke rigtigt
– men sikkerhedsmæssigt et mareridt

Kilde: http://event.moxa.com/newsletter/connection/2019/08/feat_02.html

The Ten Immutable Laws of Security (Version 2.0)

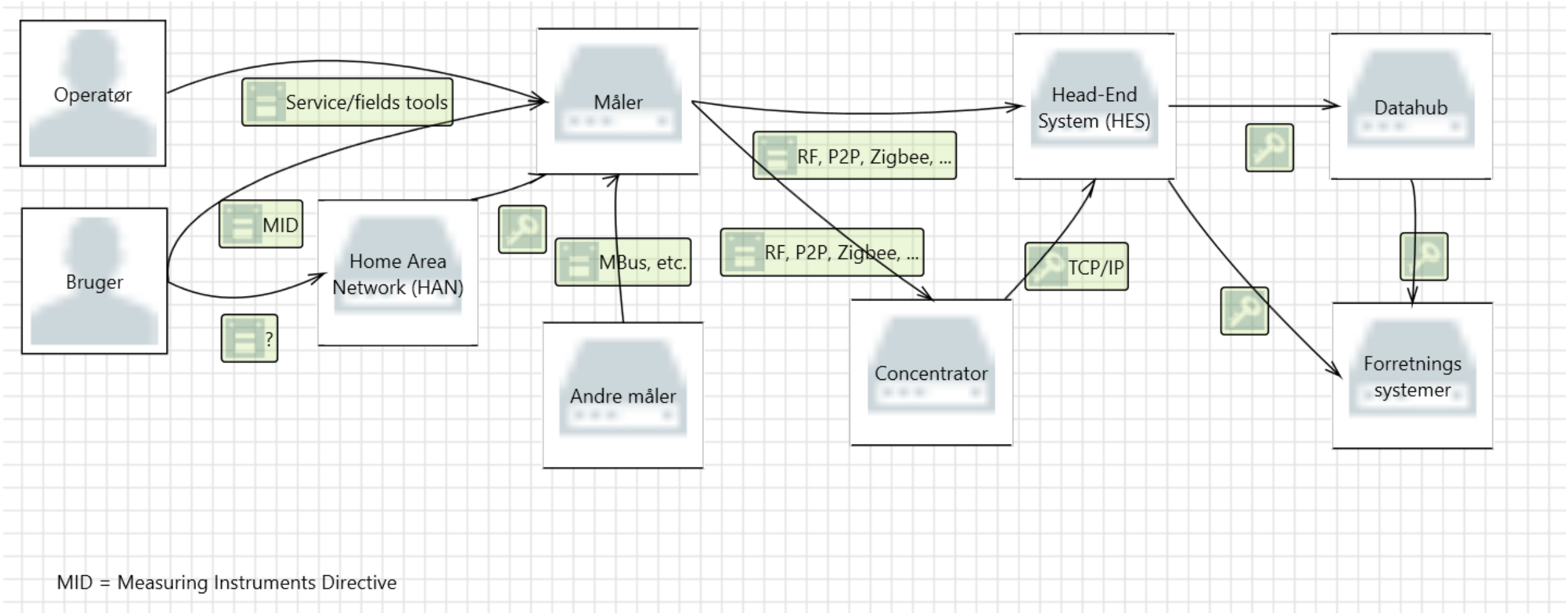
> Law #1: If a bad guy can persuade you to run his program on your computer, it's not solely your computer anymore.
> Law #2: If a bad guy can alter the operating system on your computer, it's not your computer anymore.
> Law #3: If a bad guy has unrestricted physical access to your computer, it's not your computer anymore.
> Law #4: If you allow a bad guy to run active content in your website, it's not your website any more.
> Law #5: Weak passwords trump strong security.
> Law #6: A computer is only as secure as the administrator is trustworthy.
> Law #7: Encrypted data is only as secure as its decryption key.
> Law #8: An out-of-date antimalware scanner is only marginally better than no scanner at all.
> Law #9: Absolute anonymity isn't practically achievable, online or offline.
> Law #10: Technology is not a panacea.

Kilde: https://docs.microsoft.com/da-dk/archive/blogs/rhalbheer/ten-immutable-laws-of-security-version-2-0

Sikkerhed i EI-målere

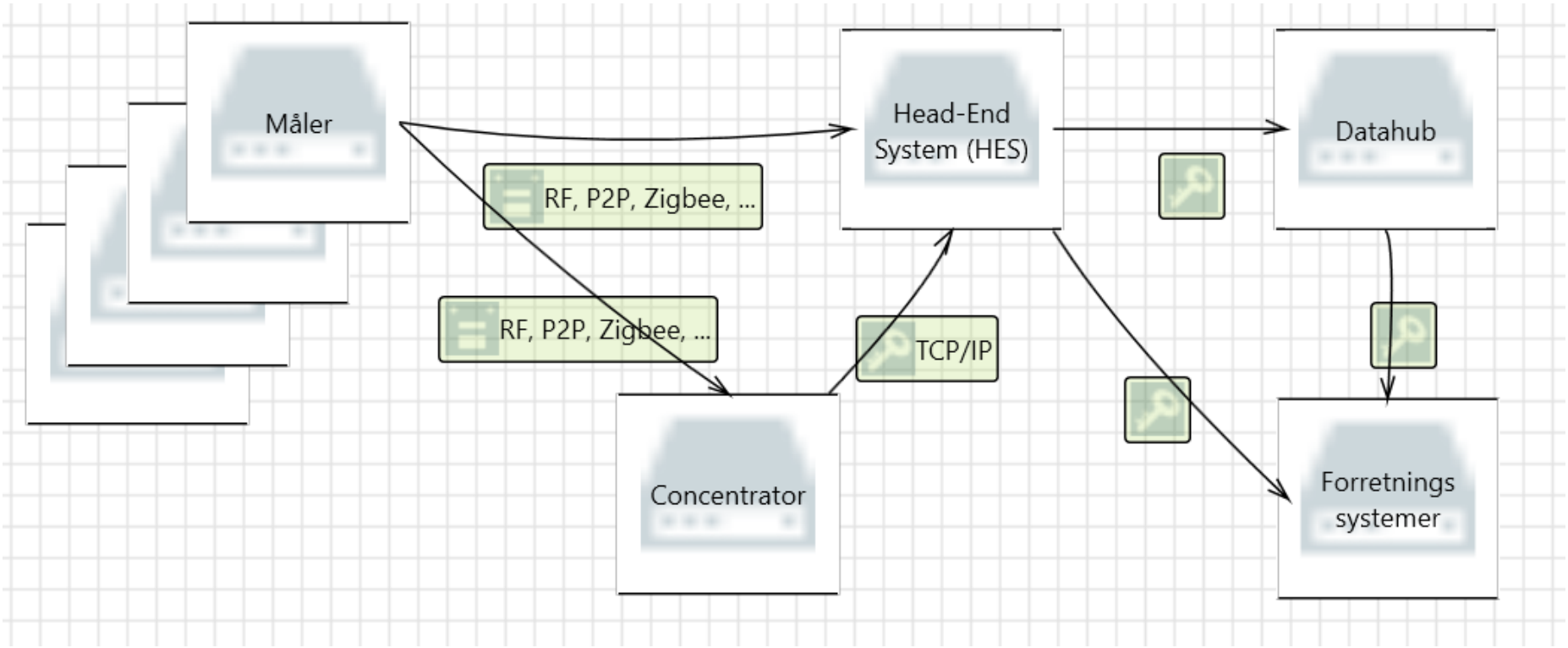
Interaktivt ;-)

Enkel måler

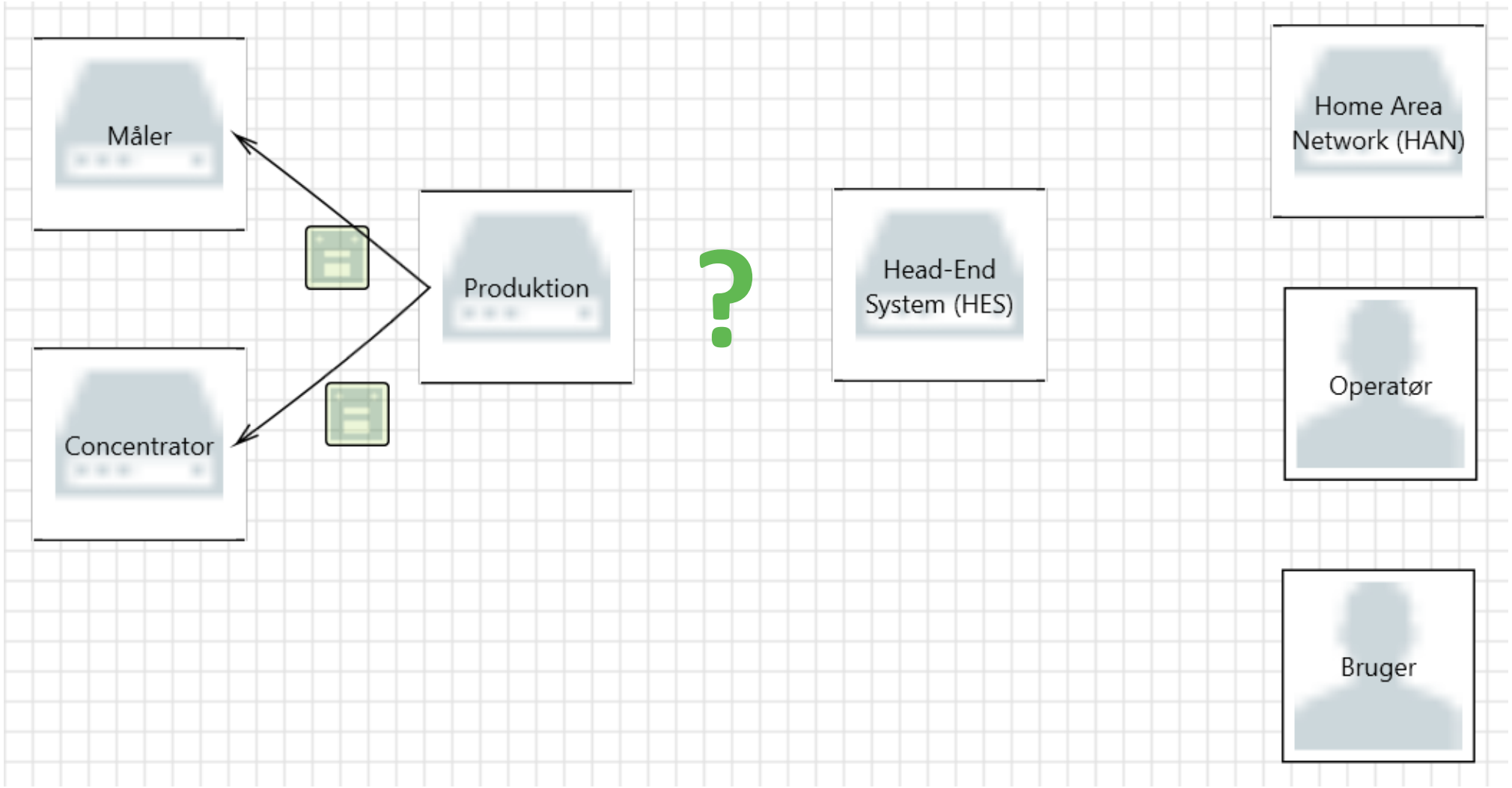


MID = Measuring Instruments Directive

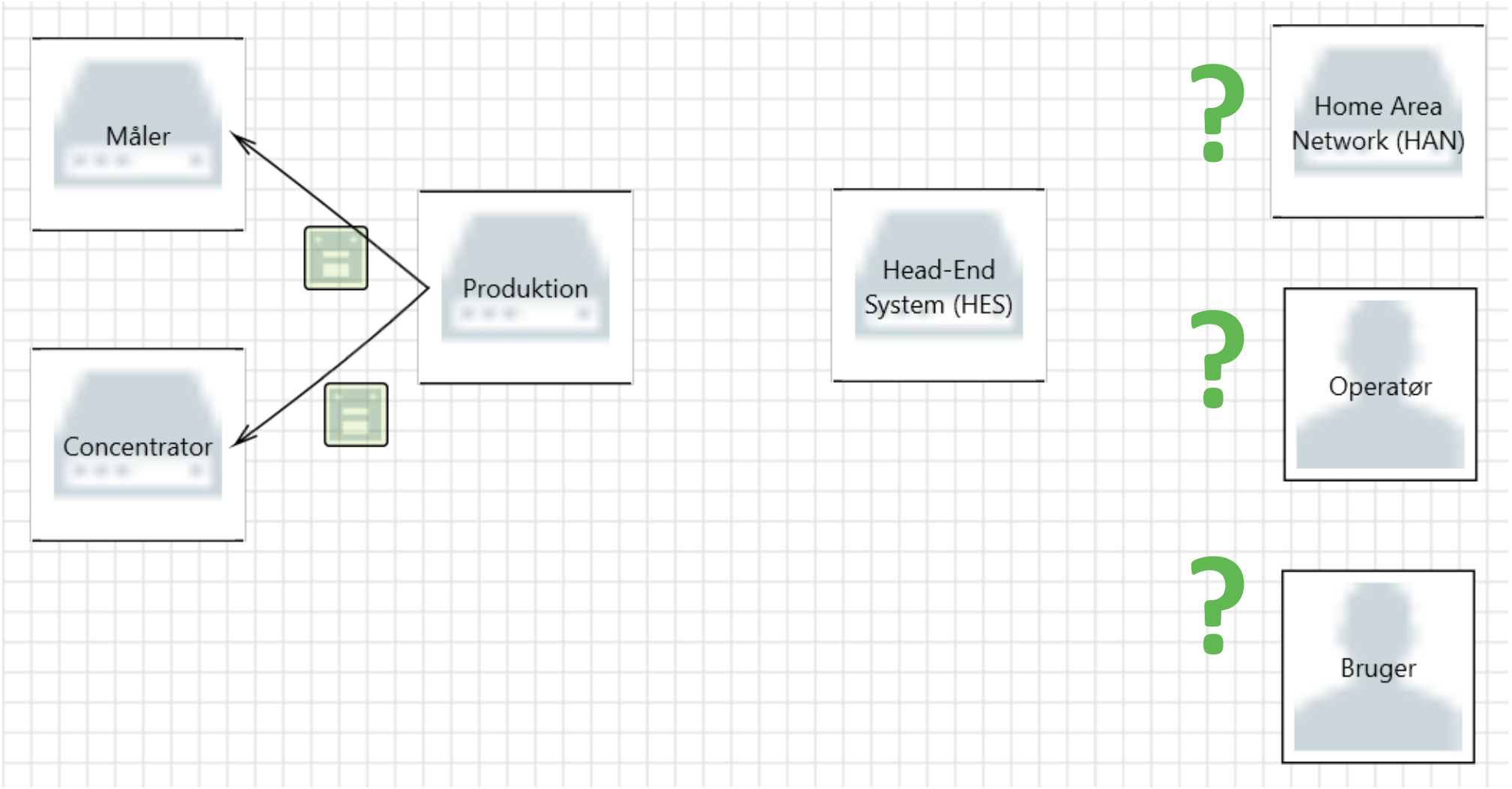
Flere målere



Nøgledistribution – ”Provisioning”



Nøgledistribution – ”Provisioning”



Hvad gør andre….

Emil hackede et af Danmarks største energiselskaber – så ansatte de ham

Emil Gurevitch hackede SEAS-NVE og fik job i Silicon Valley. Som sikkerhedsingeniør arbejder han med at forhindre hackerangreb som det verdensomspændende WannaCry-angreb, der i weekenden har ramt mere end 230.000 computere i 150 lande.

Af Benjamin Dane
16. maj. 2017 | TEKNIK

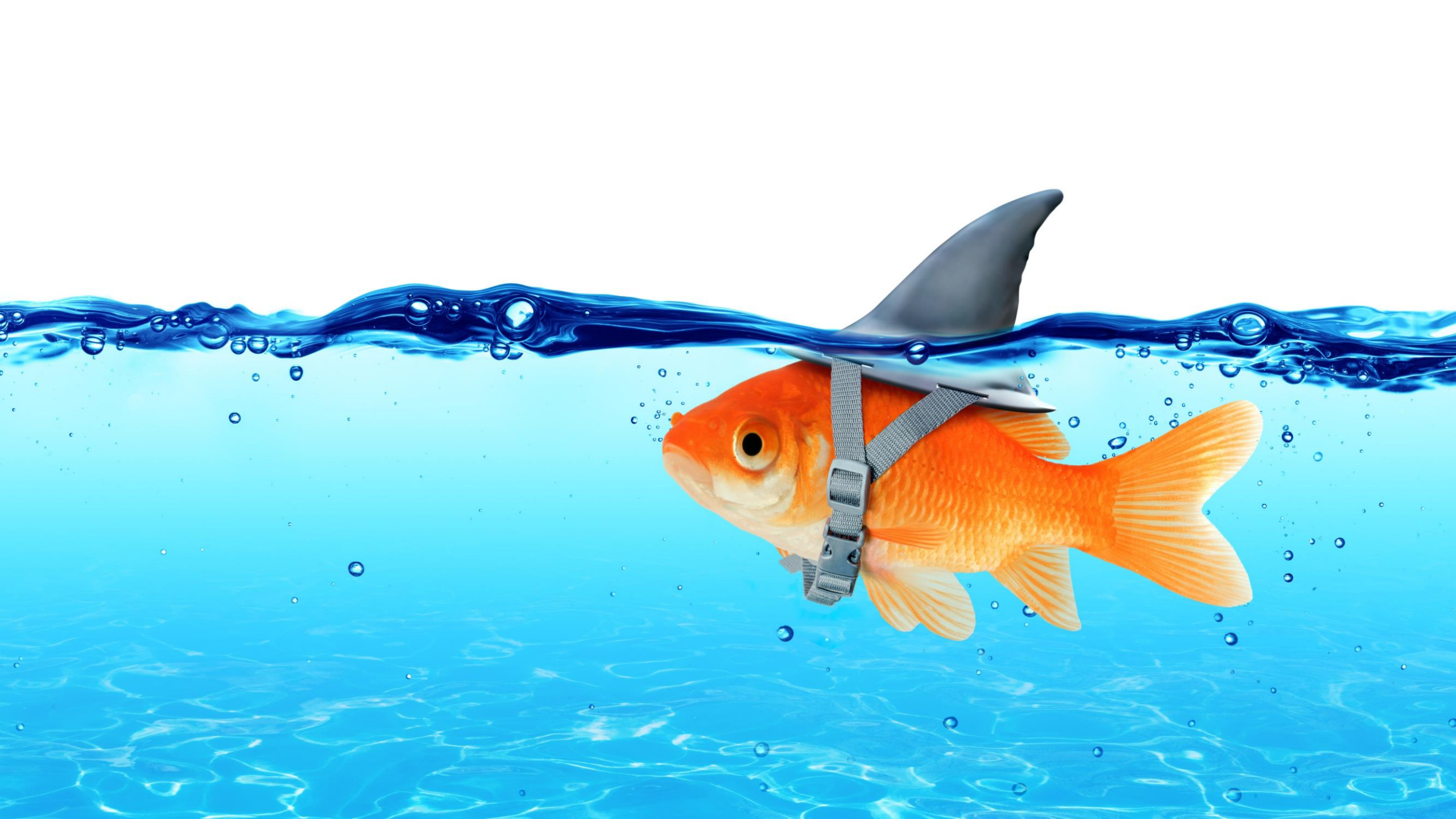
Kilde: https://www.euroman.dk/teknik/emil-hackede-et-af-danmarks-storste-energiselskaber--sa-ansatte-de-ham

Hvad gør andre….

Kamstrups el-målere har 20 nøgler til både kryptering og rollebaseret adgangsstyring

(Illustration: Jakob Møllerhøj)

Kilde: https://www.version2.dk/artikel/kamstrups-el-maalere-har-20-noegler-baade-kryptering-rollebaseret-adgangsstyring-1085035



WelcomeSecurity
Enabling value through IT security

TAK!

www.welcomesecurity.net

+45 2158 1410
thomas@welcomesecurity.net