Dit BMS er sikkert godt nok men er det sikkert nok?

RAMBØLL

Bright ideas.
Sustainable change.

Public

OT sikkerhed
Agenda

- Intro
- Fælles system forståelse
- ”Ladeporten”
- Demo – sådan finder du ”ladeporten”
- Step 1 - kortlagt installation
- Step 2 - ”lavt hængende” handlinger
- Step 3 - Generelle fokus punkter

Christian K. Nielsen

Senior OT Security specialist

Market – Rambøll Energy

Location - Copenhagen

Background

Kombination af teknisk ekspertise og kommunikationsevner.
Fokuseret på IT/OT-kommunikation med kompetencer inden for teknisk problemløsning, systemdesign og sikkerhedsstandarder såsom IEC62443, NIST og NIS2.

Særlig erfaring med risikovurdering og logisk tænkning i komplekse SCADA-systemer.
Nøglekompetencer omfatter OT-cybersikkerhed, dyb teknisk forståelse af IT/OT-kommunikation, kendskab til OSI-modellen samt evnen til at forklare komplekse problemstillinger på en enkel og forståelig måde.

Functional experience

2024 –
Rambøll Energy
Senior OT Security specialist

- OT Security lead – EPC
- Risk assessment workshop
- Standard compliance

2008 – 2024
ABB A/S
Senior Cyber Security technical Lead

+Sanovo
+Fjernvarme Fyn
+Tipatek
+Konsulent

- Network design, supervision
- Firewall configuration
- IEC62443 design
- NIS2
- Risk assessment workshop

Sector experience

Olie / Gas /Skib - Offshore

- **Modbus RTU/TCP**
- **Profibus**
- **Fiber optik**

Onshore

- **Fjernvarme**
- **Affald**
- **Pharma**
- **Industri**

Træning

- **Hirschmann(NDE1,2)**
- **Cisco (ICND1,2)**
- **Palo Alto + Checkpoint**
- **GICSP**
- **IEC62443**

Drivkraft

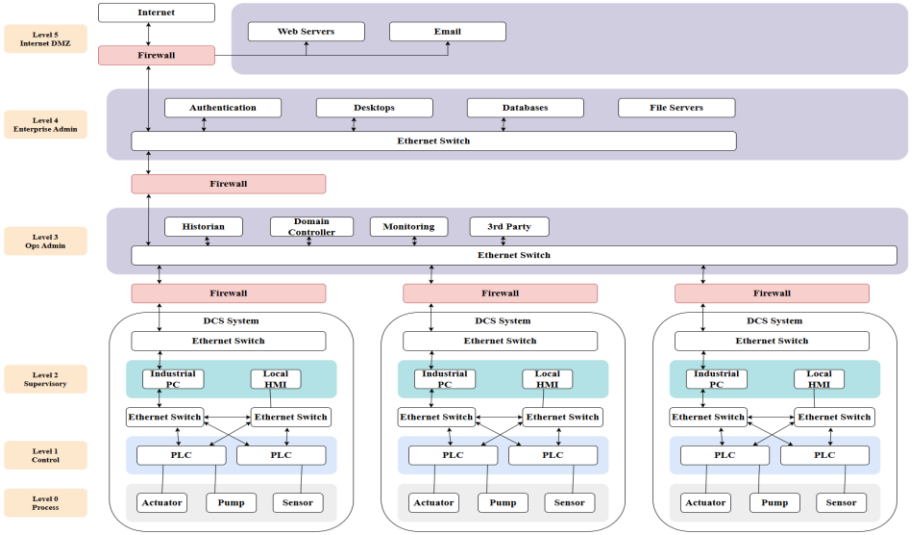
- Teknisk udfordring
- Se løsninger
- Nedbryd kompleksitet
- …Keep it simple

Fælles system forståelse

- En bygning

Source: https://itp.nyu.edu/networks/building-management-systems-an-overview/

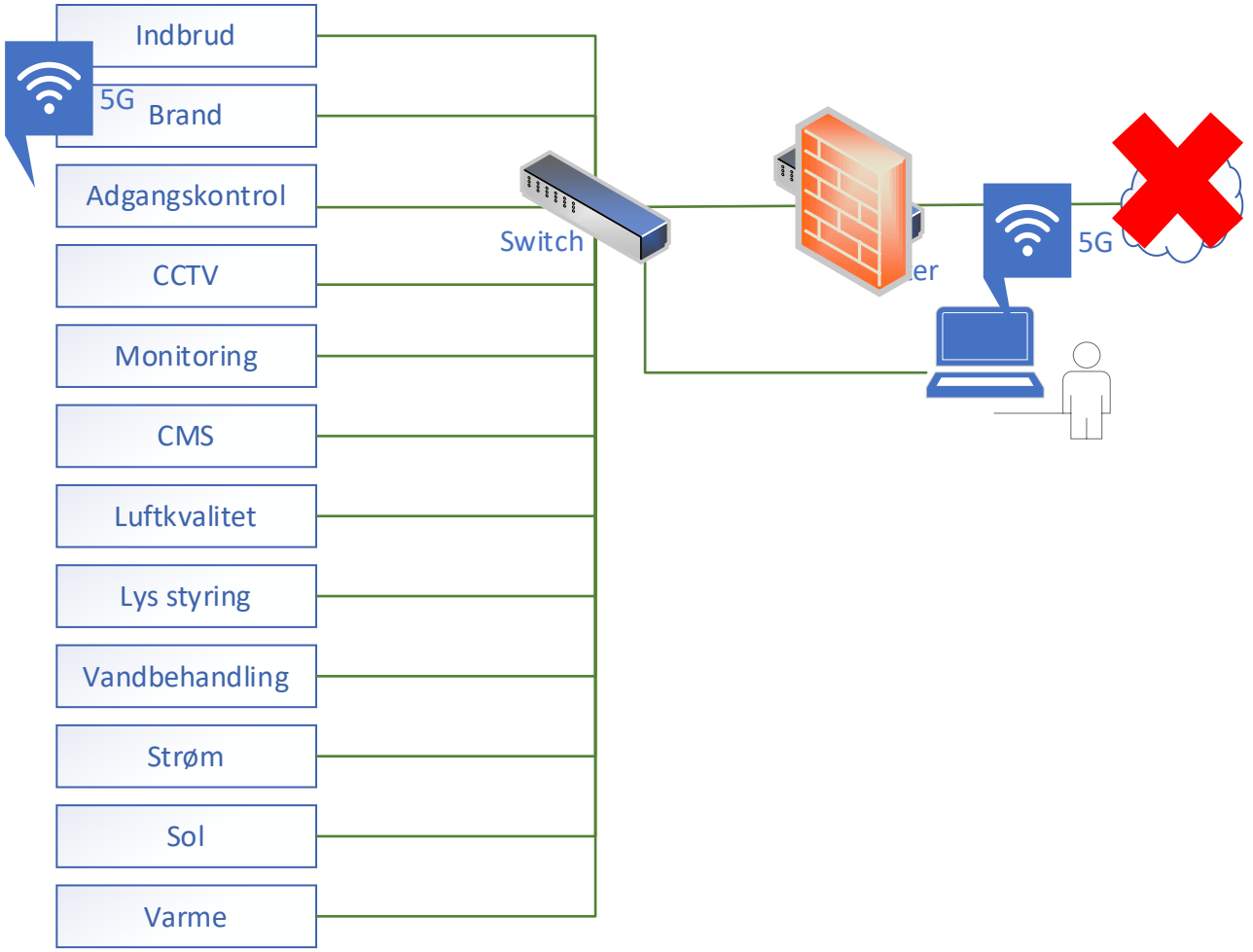
- Topologi



Source: https://www.agilicus.com/white-papers/piercing-the-purdue-model-zero-trust-in-operational-technology/

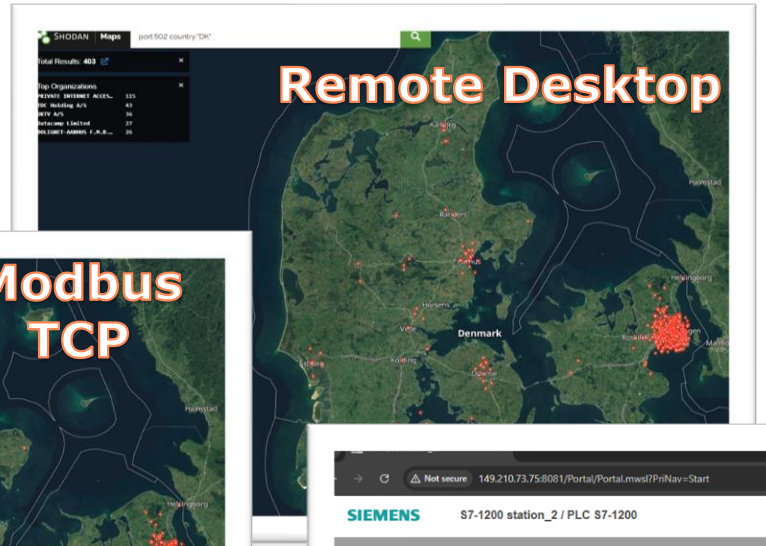
- Systemer i bygning
  - Sikkerhed
    - Indbrud
    - Overvågning
    - Adgangskontrol
    - CCTV
  - Bygning
    - Brandalarm
    - CMS(Construction Monitor)
    - HVAC
    - Luftkvalitet måling
    - Vandbehandling
  - Energi
    - Strøm
    - Sol
    - Varme
    - Lys

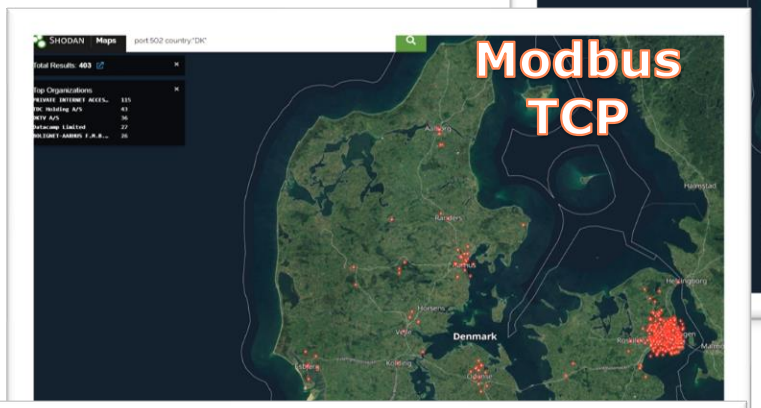
Ladeporten

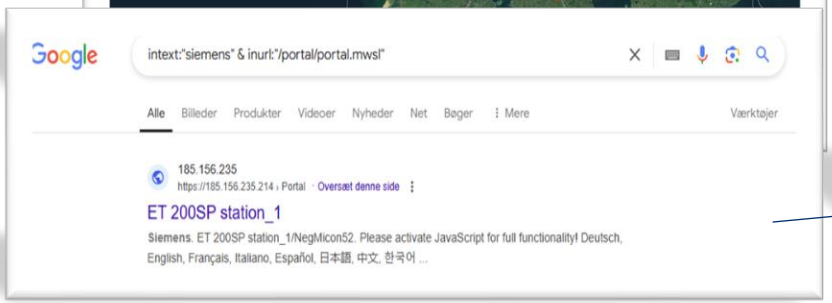


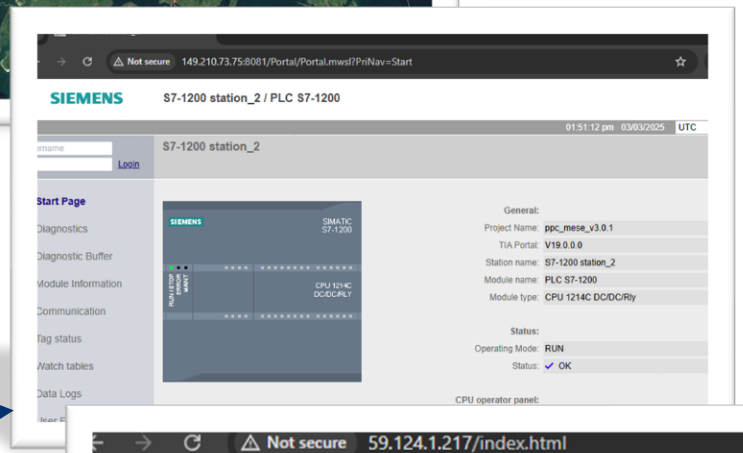
1. Ingen sikkerhed, systemejer er klar over det = alt virker
2. IT sikkerhed / lovgivning kræver firewall = intet virker
3. nogen montere 5G, systemejer **tror** alt er godt= alt virker

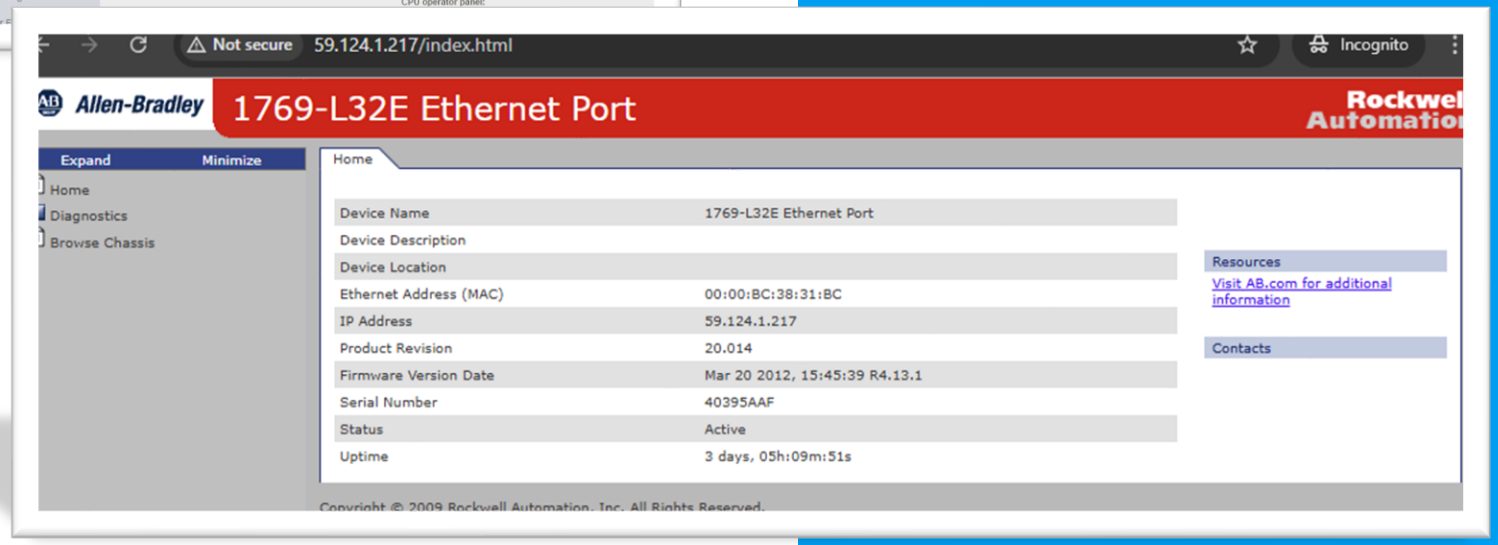
DEMO











Følgende udføres:

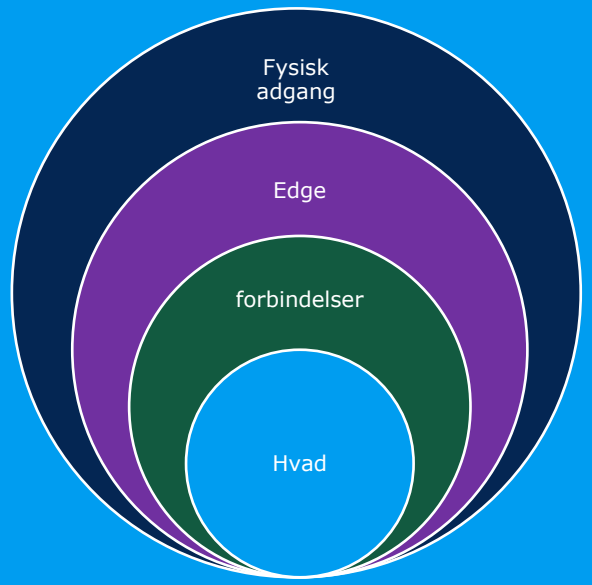
- Opslag af kendt protokol
  - Link: iana.org – Modbus / bacnet /rdp /
- Shodan.io søgning
  - Link: shodan.io - port:___ country:"DK"
- Exploit Database søgning / Google Hacking
  - Link: exploit-db.com
- Google søgning
  - Link: google.com

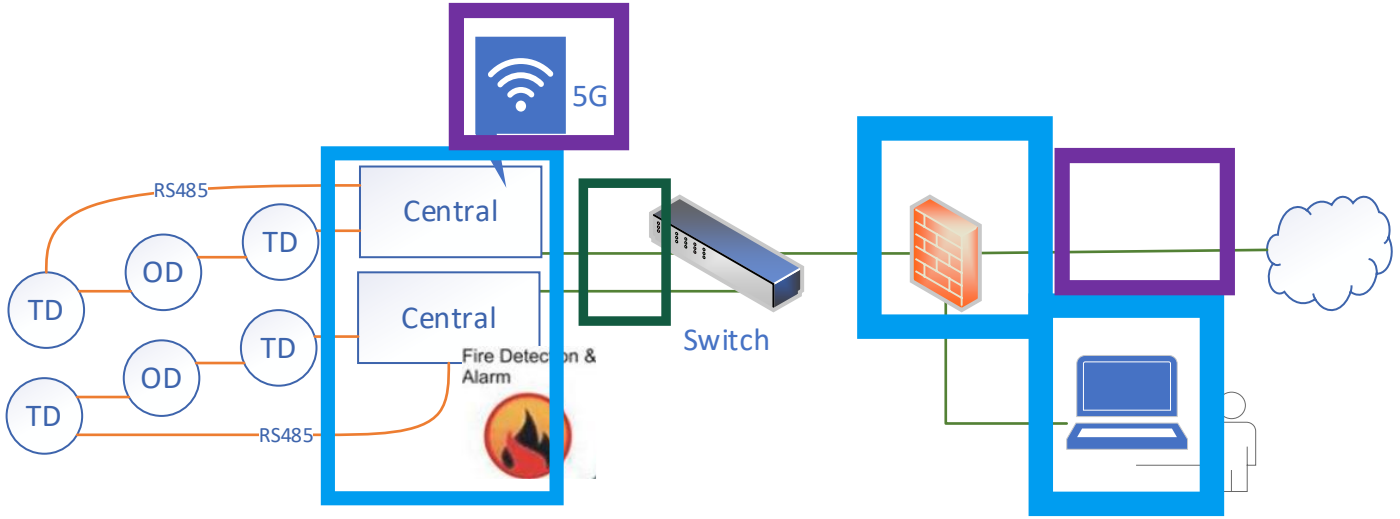
Step 1

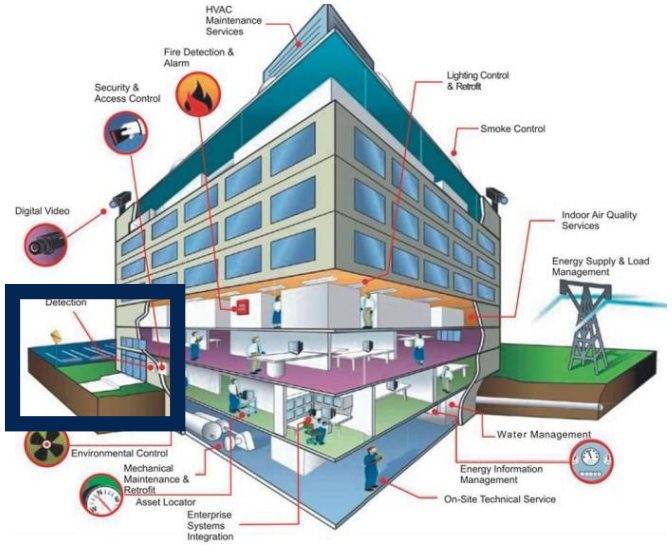
Få kortlagt installation – Her og nu

- Opstart en asset/inventar liste

- Security onion - Simplificeret
  - Hvad er installeret
  - Forbindelser (Patch kabler)
  - Undersøg hvor er "Edge" på system
  - Fysisk adgang



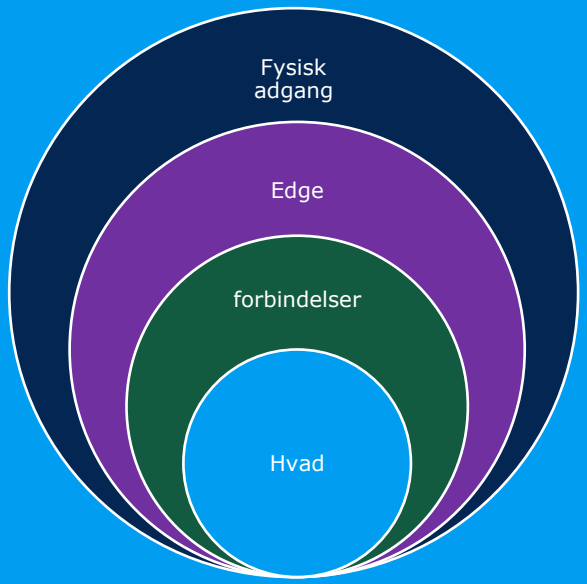


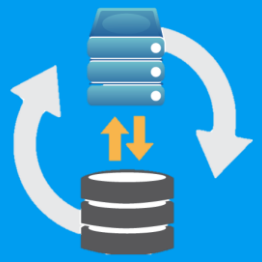


Step 2

Udfør alle ”lavt hængende” handlinger

- Fysisk adgang
  - Fjern kile i dør
  - Lås på teknikskabe / kabinetter
  - Monter RJ45 / USB port låse
- Logisk adgang
  - Opdater ALLE default brugernavne / passwords
  - Luk alle overflødige porte
  - Stop ikke benyttede services på netværk
  - Fjern patch kabler der ikke er i brug
  - Luk remote adgange der ikke er i brug





RACI Chart

Task/Role	Role 1	Role 2	Role 3
Task 1	R	R	I
Task 2	A	C	C
Task 3	A	I	I

R = Responsible
A = Accountable
C = Consulted
I = Informed

Step 3

Generelle fokus punkter

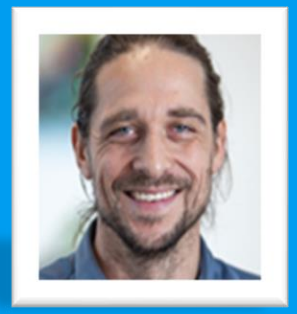
- Inventar liste med relevant information
- Backup / Restore setup
  - Hvor er, hvordan indlæser og virker backuppen?
- Disaster / Recovery – kom tilbage i kontrol, evt. kun nøddrift
  - Hvem gør hvad, hvorfor og hvordan? RACI Chart
- Patch management, hvordan, hvorfor og hvad?
- Awareness – øg fokus ved øvelser, tænkte scener mv.

- Input til samlet risiko vurdering (IEC62443-3-2)
- Inddrag ledelsen
- Stil krav til leverandør

Overvej:

- Dataretning sikker > usikker
- Hvad er monteret, hvor er det monteret
- Opdater procedure, NÅR det rammer er de gode
- Del erfaringer/templates i jeres netværk

Rune L. Lauritzen
rull@ramboll.com
M +45 5161 2182



Thomas R. Frederiksen
trfn@ramboll.com
M +45 5161 2919

Christian K. Nielsen
cknl@ramboll.com
M +45 6036 1727

Bright
ideas.
Sustainable
change.

RAMBØLL