SINTEF

Cyber Security Considerations for Self-healing Smart Grid Networks

Martin Gilje Jaatun

(Yaw-toon)

Martin.G.Jaatun@sintef.no

@seniorfrosk

FLEXnett

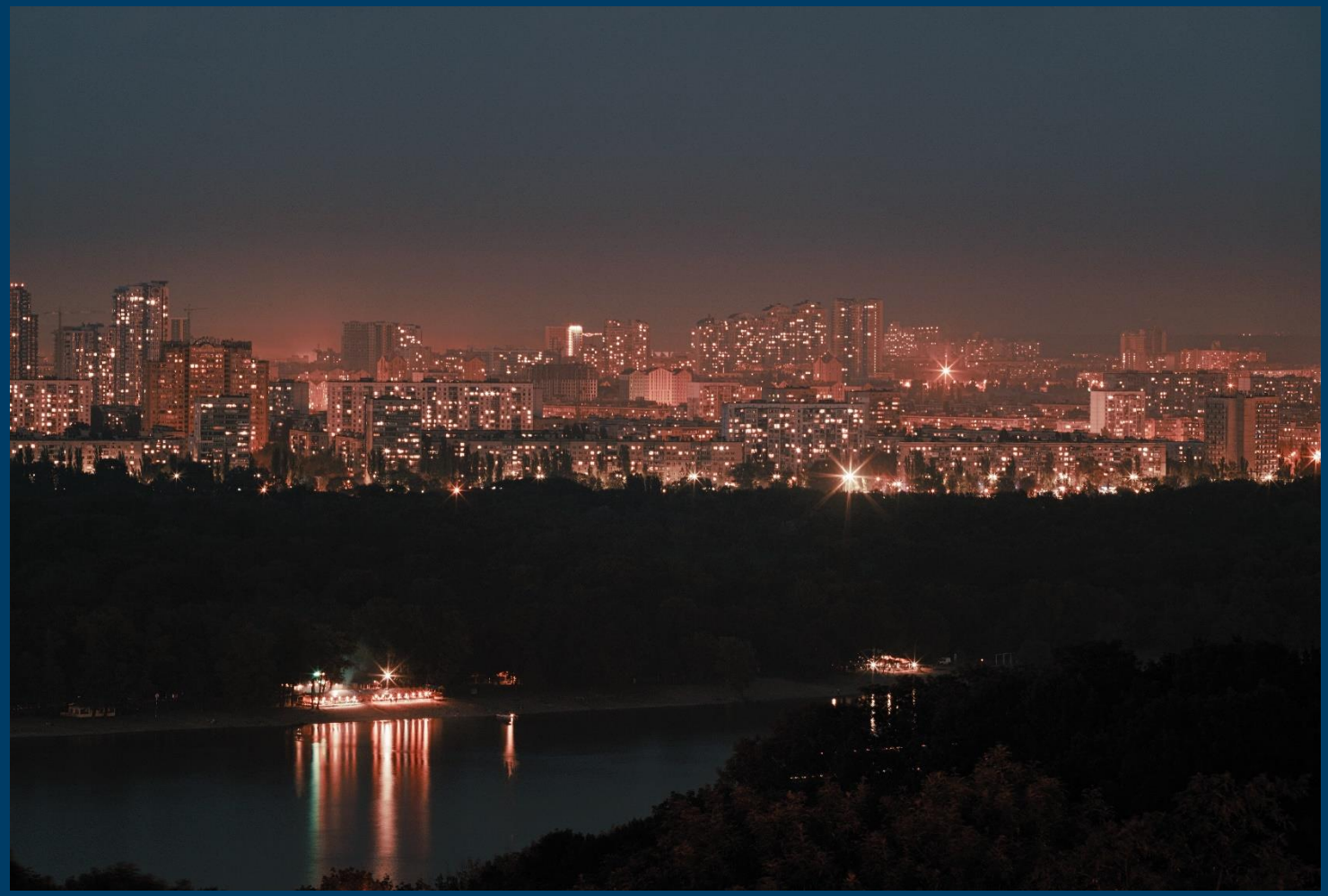
No, actually, it was just a couple of years ago

December 23, 2015

http://www.bbc.com/news/world-europe-26387353

It was the day before Christmas Eve:

We go from this…



…to this

2015: Ukraine – what happened?

http://www.bbc.com/news/world-europe-26387353

- BLACKENERGY 3 malware used to gain access to corporate networks of Ukrainian DSOs
- Used Distribution Management System (DMS) to disconnect substations from the grid
- RTUs "bricked" by malicious updates
- "KillDisk" functionality wiped Windows HMIs

https://dragos.com/blog/crashoverride/CrashOverride-01.pdf

Impact

- Without access to SCADA infrastructure, ability to automatic control was lost for up to a year in places
- 225 000+ customers were left without power for 6 hours and more
  - Not necessarily fun in December…
- Restoration only possible through manual efforts

2016: Ukraine – it's deja-vu all over again

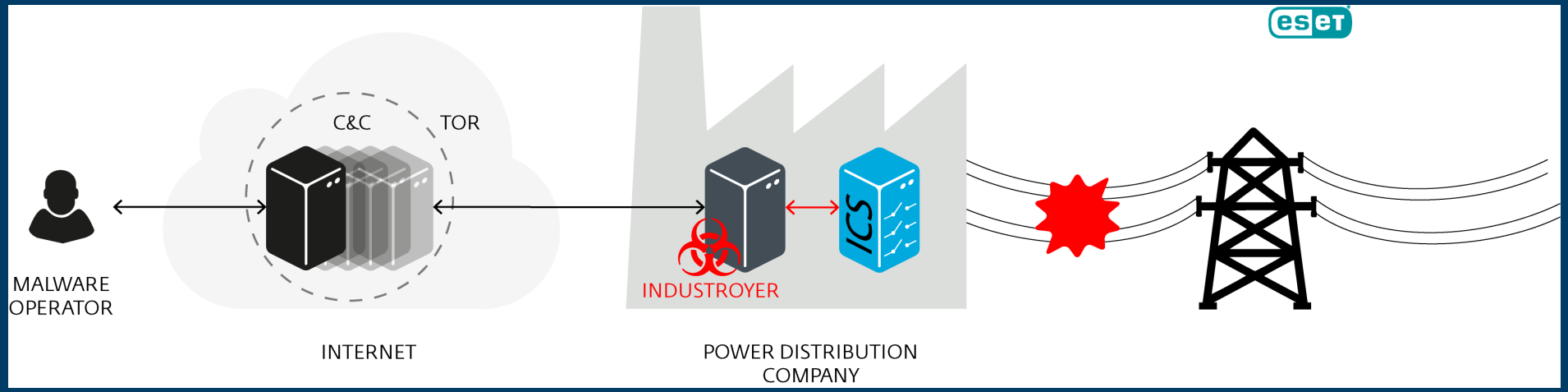
- Affected Pivnichna transmission substation in Kiev
- Blackout for 1 hour in parts of Kiev from just before midnight December 17
- "Similar to previous year"…
- …but new malware?
- Proof-of-concept?

And the malware keeps on coming...

Crashoverride

INDUSTROYER

- IEC 60870-5-101
- IEC 60870-5-104
- IEC 61850
- OLE for Process Control Data Access (OPC DA)

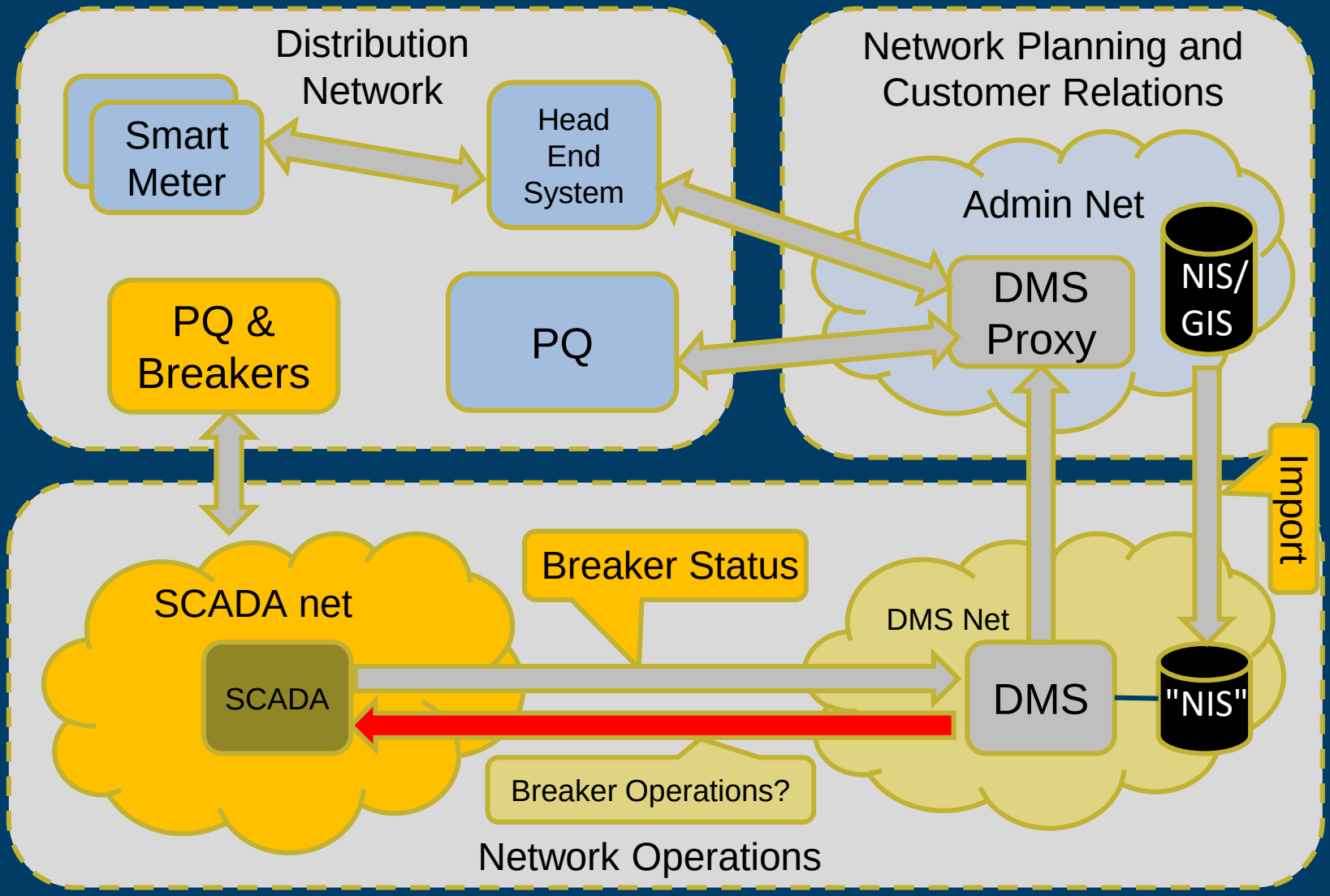


https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/

SINTEF

@seniorfrosk

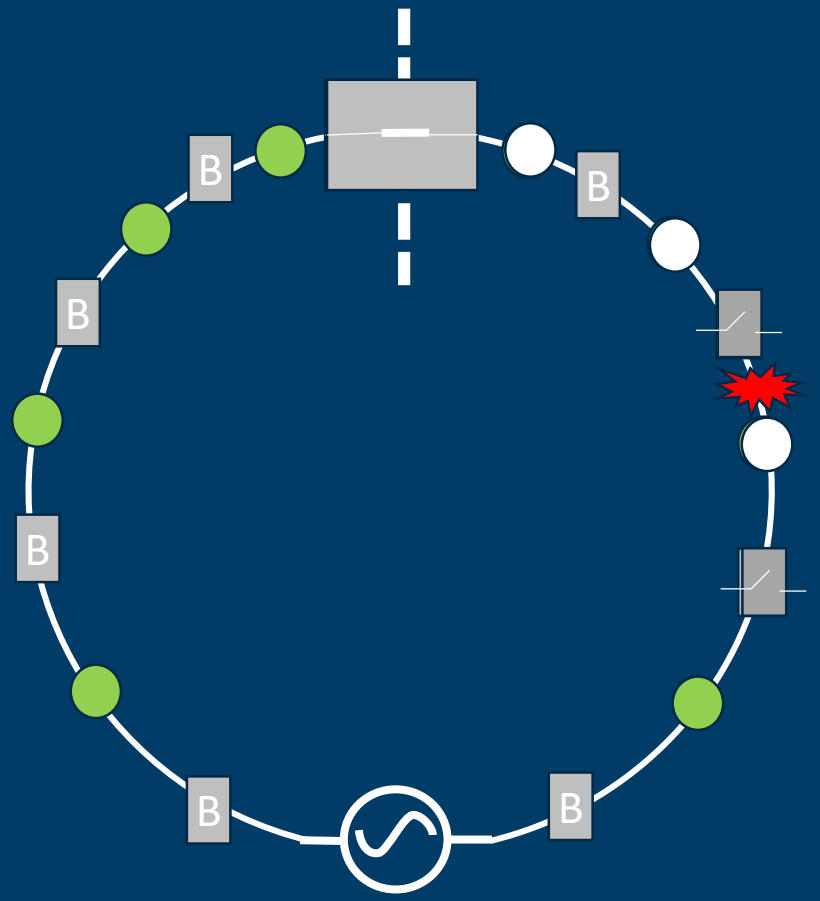
On with the show…



SINTEF

@seniorfrosk

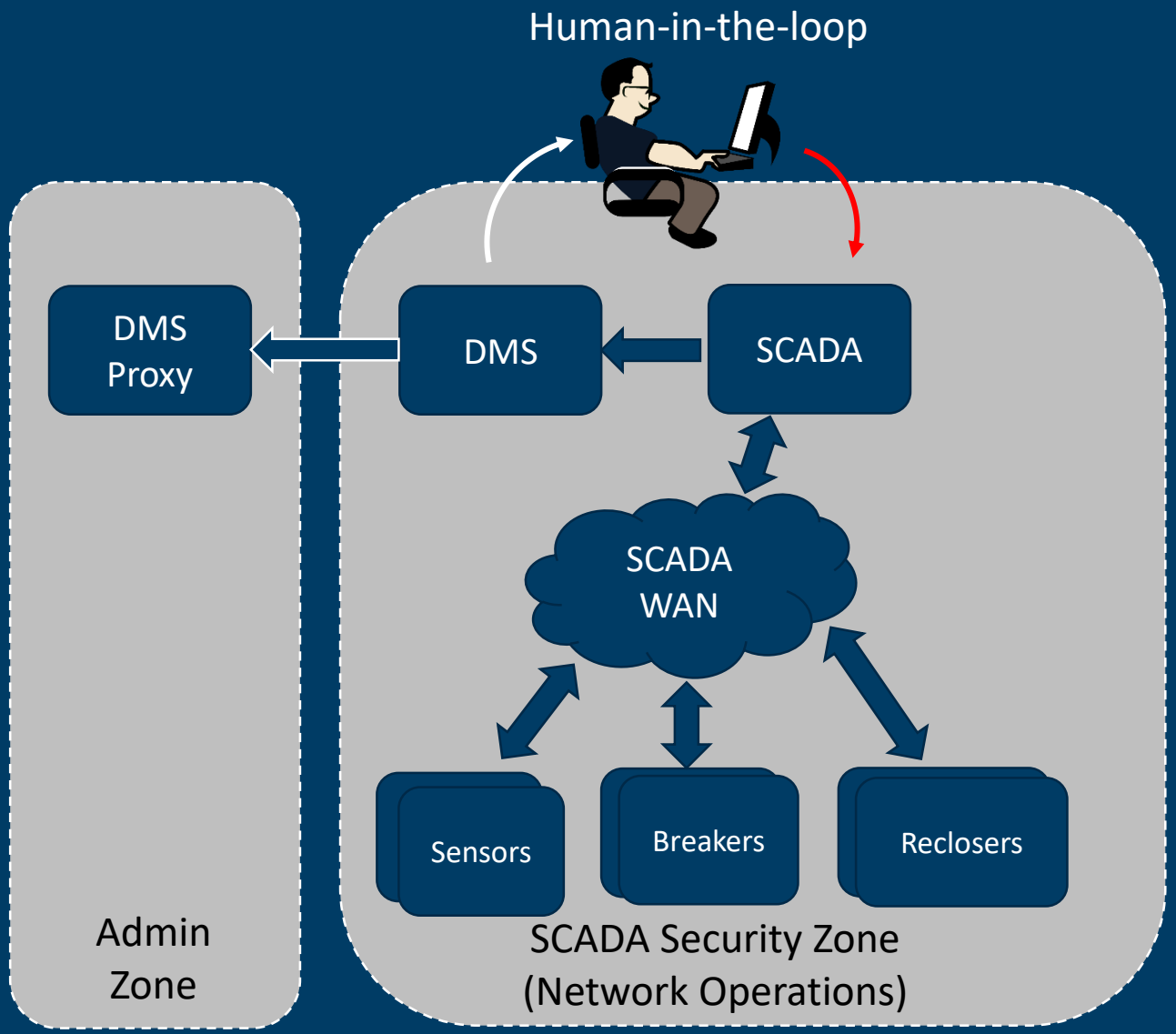
A flash introduction to self-healing (Fault Location, Isolation and System Restoration)



SINTEF

@seniorfrosk

Today – a human in the loop

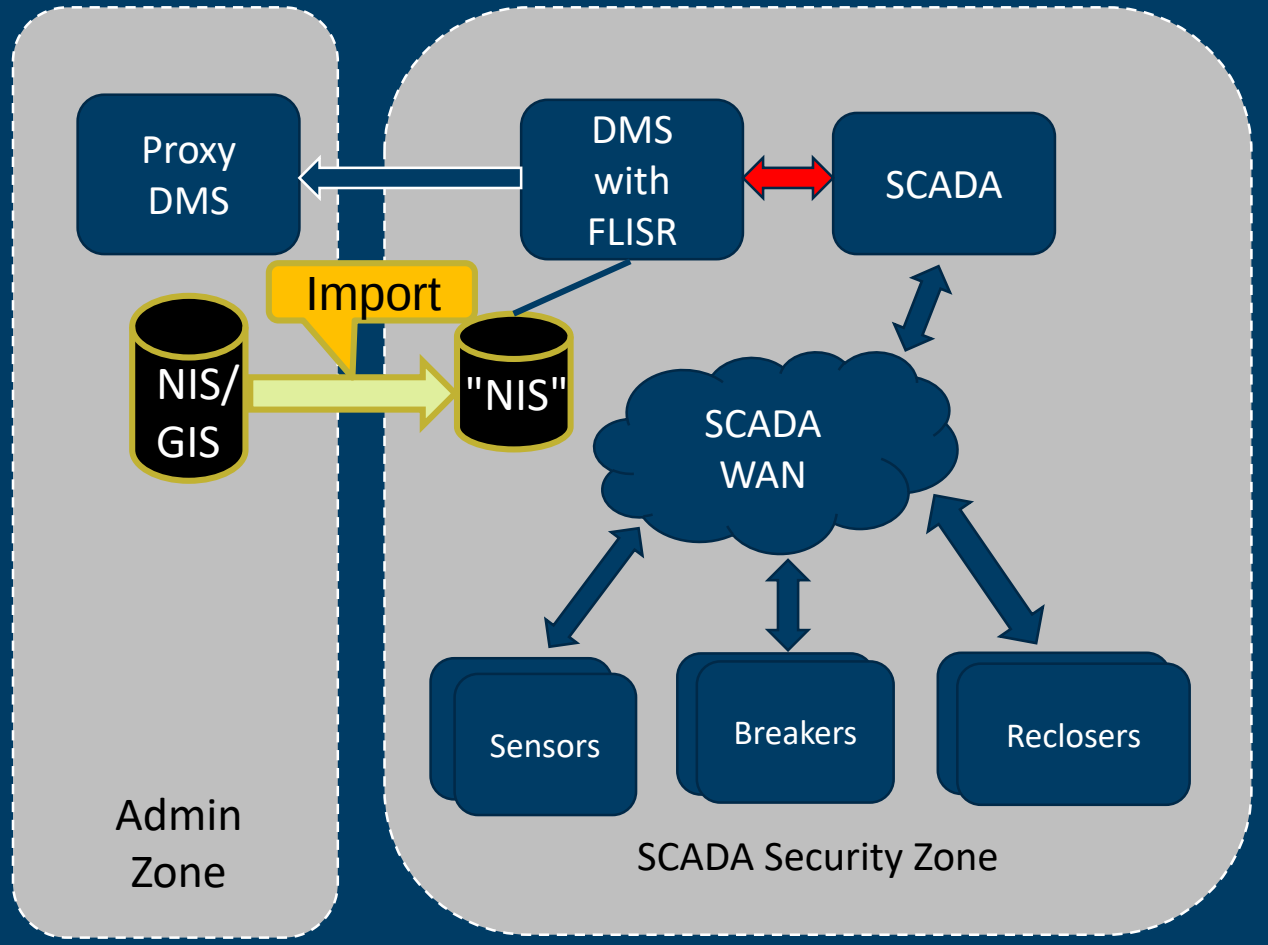


SINTEF

@seniorfrosk

Sentralised FLISR

- DMS must be able to actively manipulate SCADA
- If DMS is compromised , SCADA is also compromised
- Daily import of NIS/GIS *may* represent critical vulnerability
- Reduced need for manual reconfiguration in case of topology changes



SINTEF

@seniorfrosk

The goal is secure decentralised FLISR

- To achieve this we need new security mechanisms implemented in the SCADA network
- Some things we can do today…
  - SCADA IDS with machine learning
  - Whitelisting
  - Rate-limiting of changes
- …but we need mechanisms that are more integrated and holistic, not ad hoc and piecemeal

Questions?

Technology for a better society

https://infosec.sintef.no

http://cineldi.no

Martin.G.Jaatun@sintef.no

@seniorfrosk