

OT-Networks

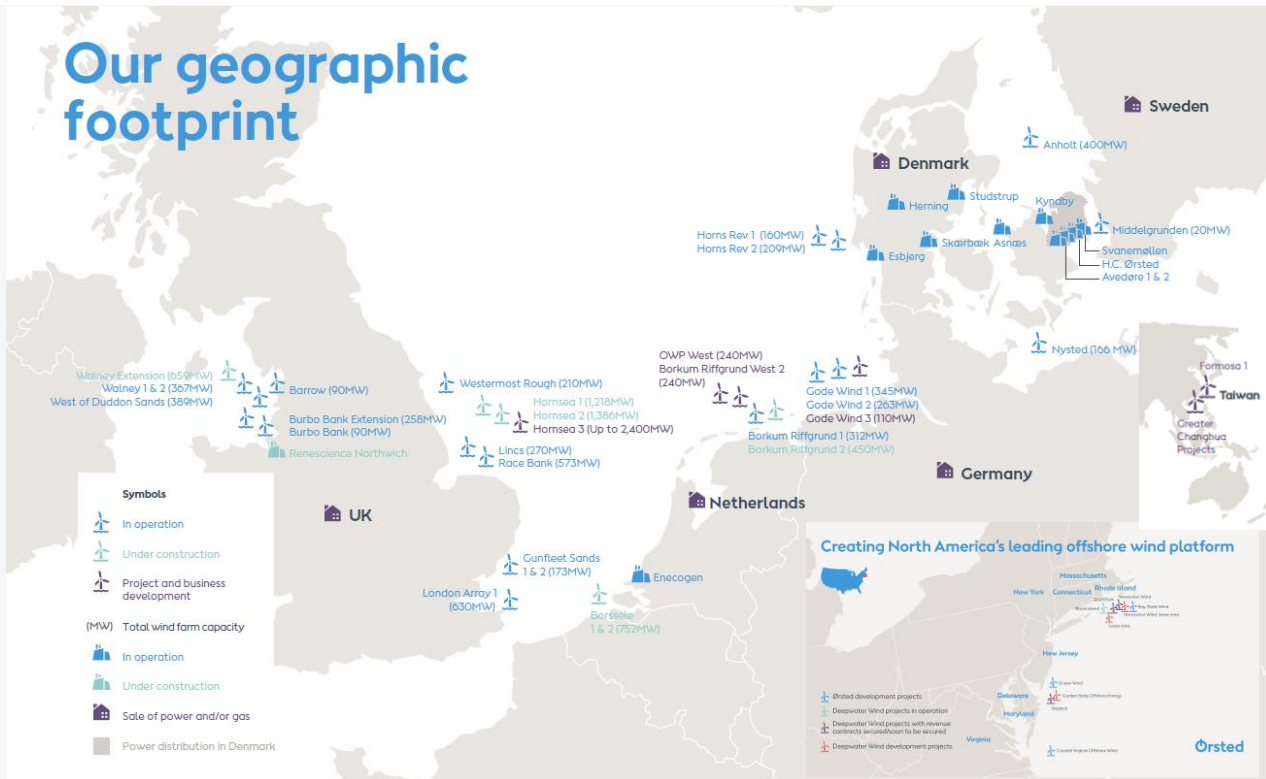
How is Ørsted working with architecture and security. What are the functional requirements to the networks seen from the system side



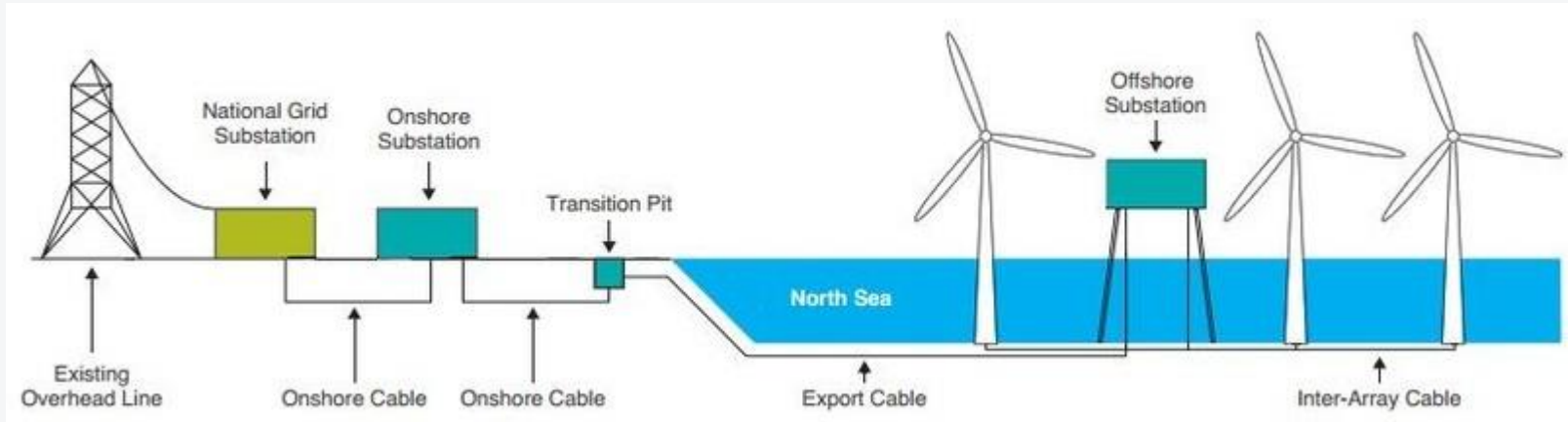
Mads Thorsted Nielsen
Manager SCADA Communication

30 Oct 2018

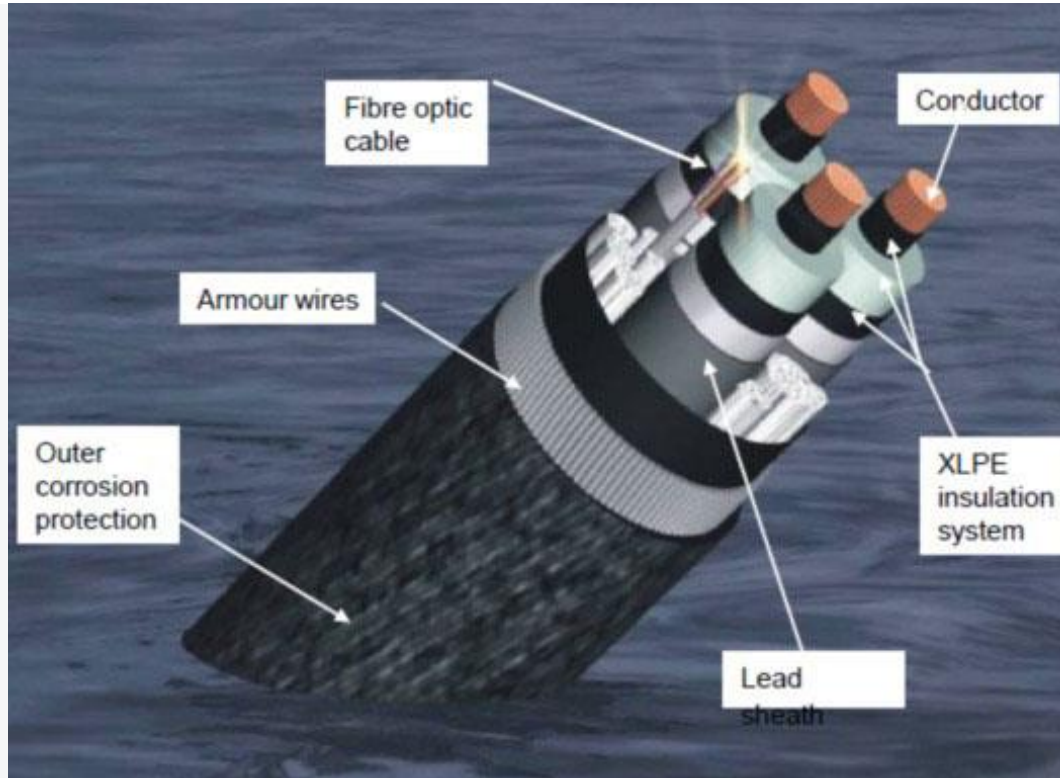
Our geographic footprint



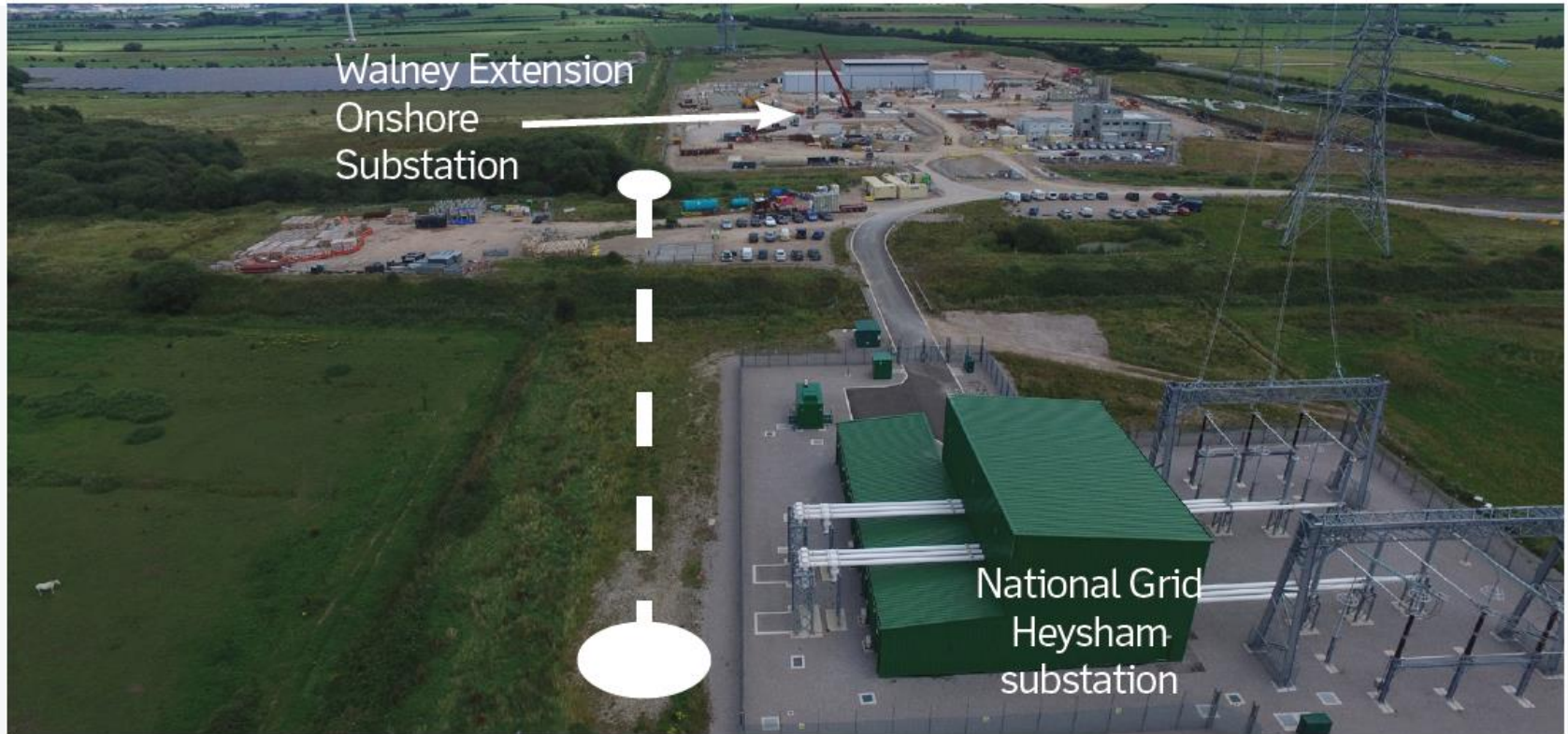
An offshore windfarm



Export cable



Walney Extension 659 MW – Onshore Substation (Heysham, Lancashire, UK)



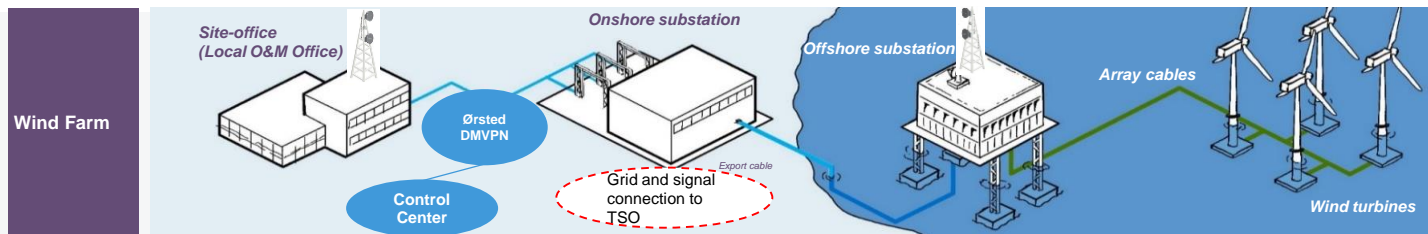
Walney Extension 659 MW: Z04 Offshore Substation (Irish Sea, UK)



Walney Extension: Wind Turbine Installation (Irish Sea, UK)



OT Systems in a Windfarm



Power Generation/Transmission Systems

Switchgear, Transformers

SCADA Systems

WTG SCADA, SCS SCADA

Safety & Security Systems

UPS, HVAC, CCTV, FAS, Helicopter Operation Systems

Network & Communication Systems

Backbone Network (Wired & Wireless), Radio Communication (VHF AM/FM, TETRA)

Measurement Systems

Wind Measurement (LIDAR), Wave Buoys

IT is dynamic

IT: Data is king

IT: Confidentiality is priority #1

IT: Patch Tuesdays

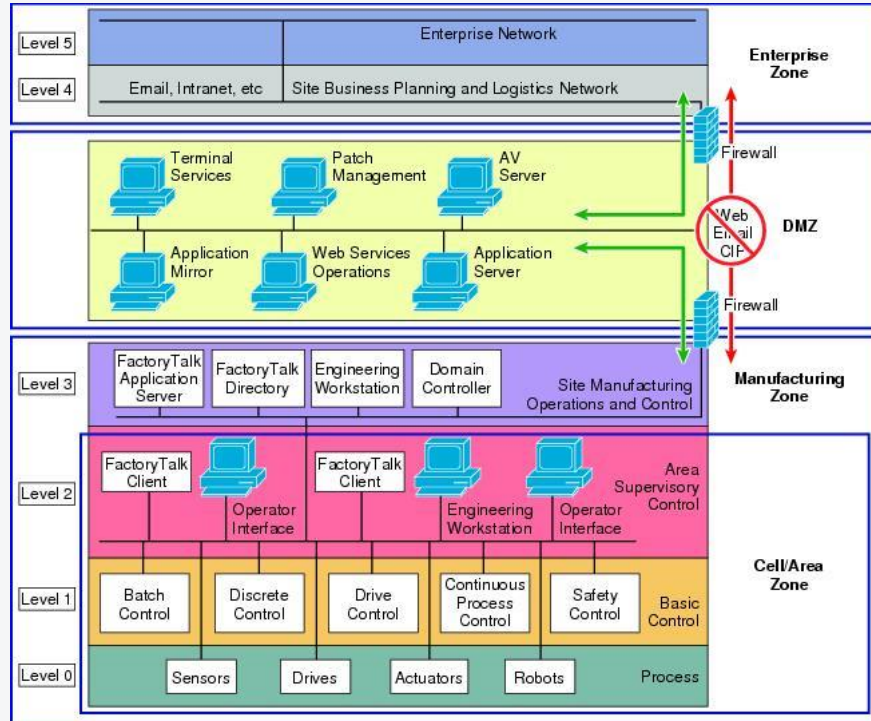
OT is deterministic

OT: Process is king

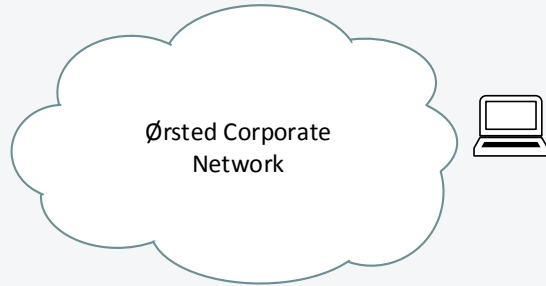
OT: Control is priority #1

OT: Patch...decade?

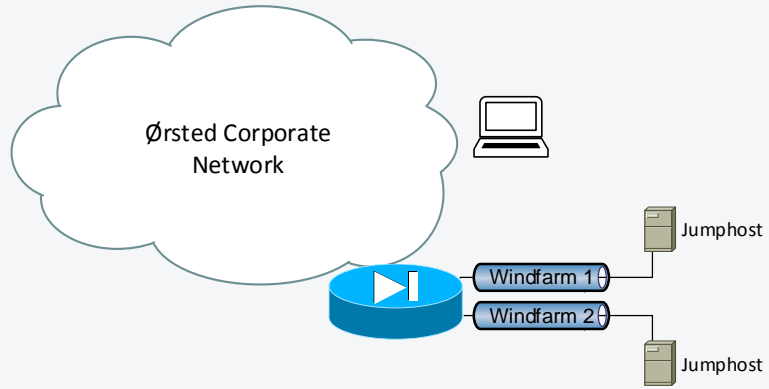
The architectural design

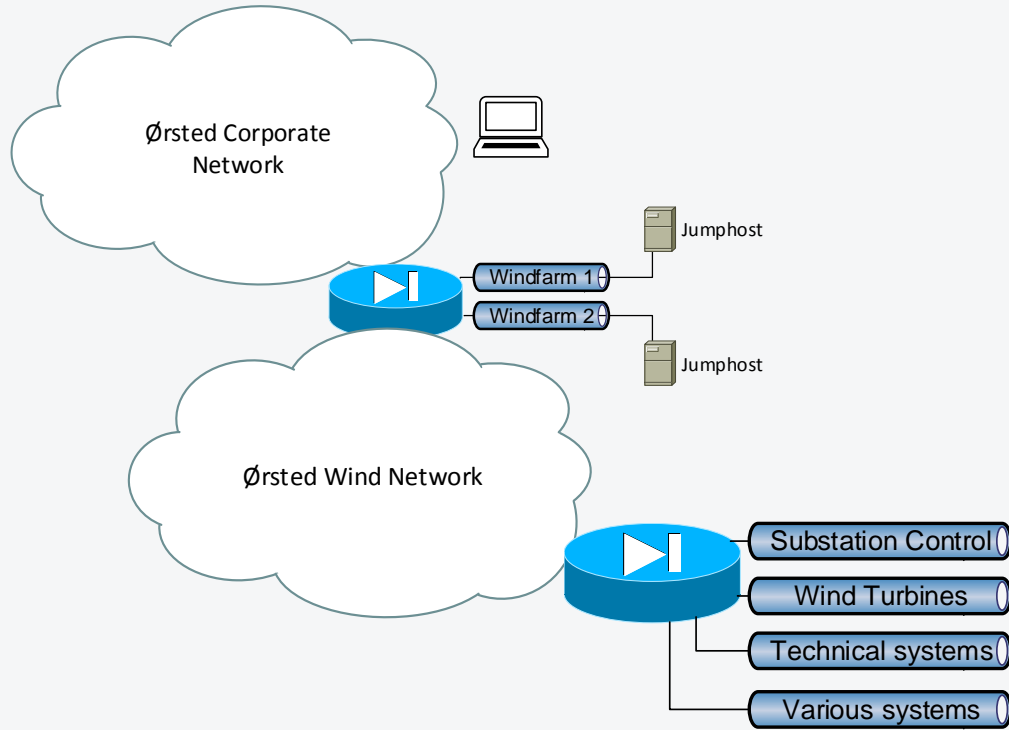


© 2005

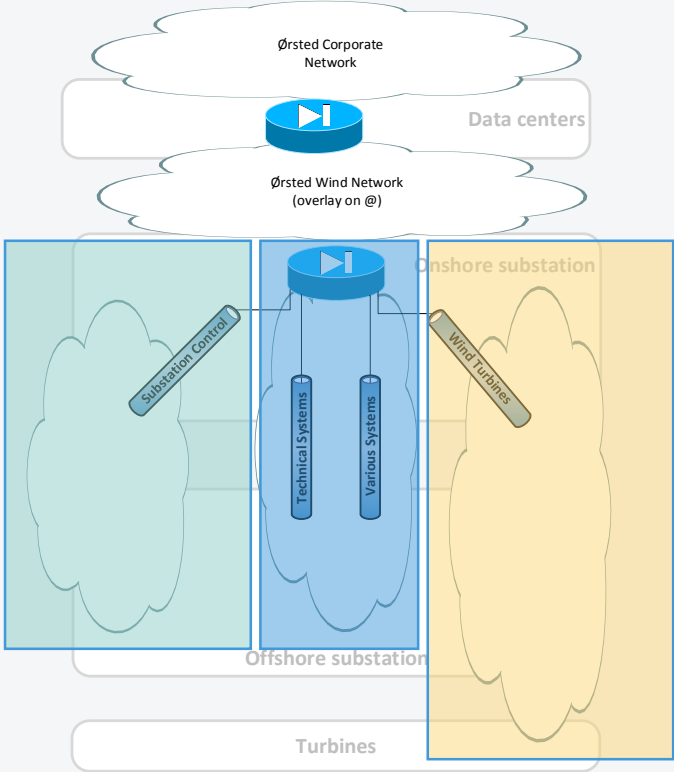


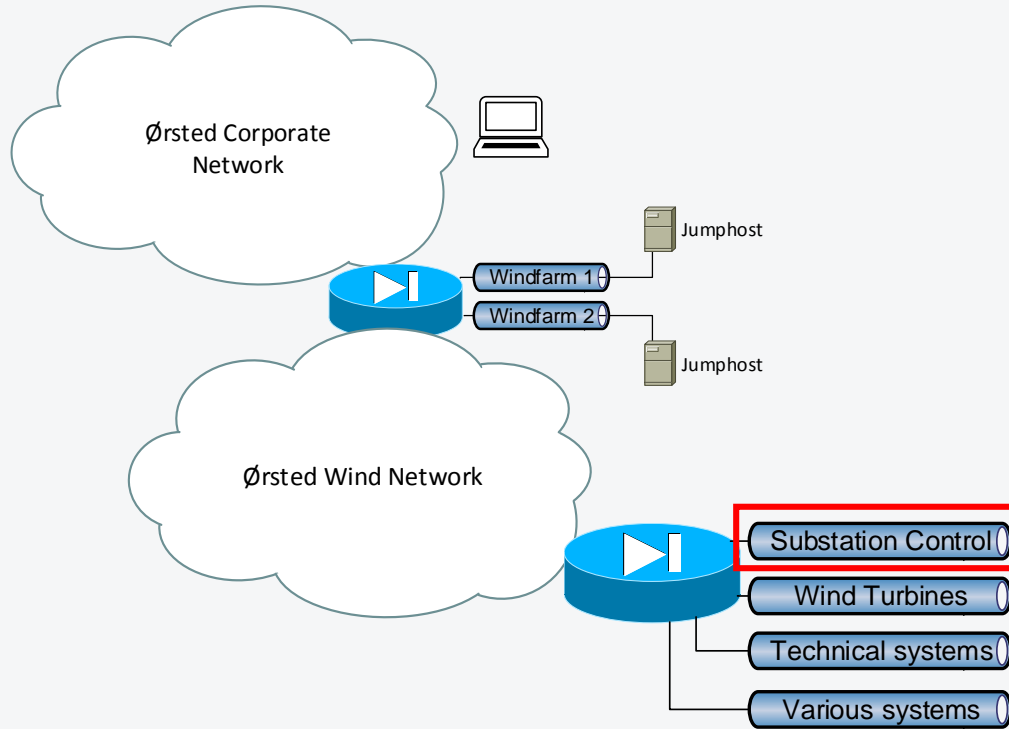
Ørsted Architecture



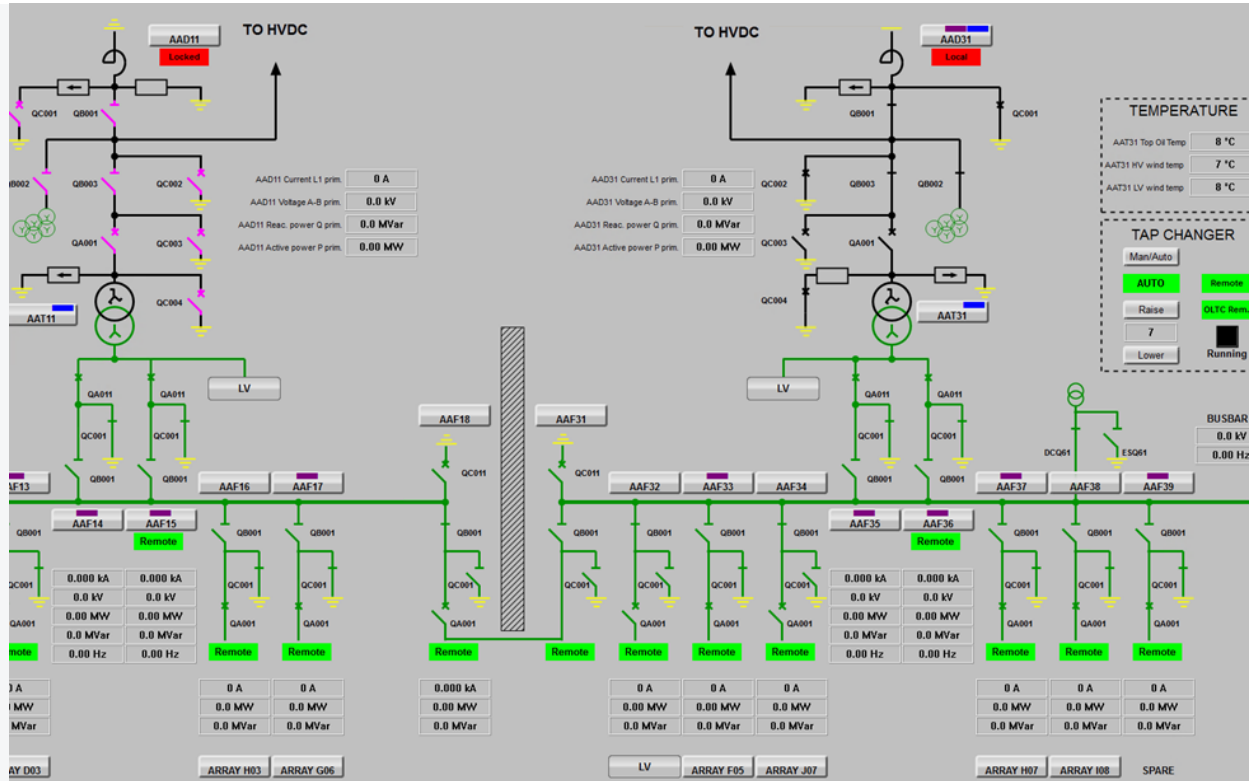


Network Deliveries





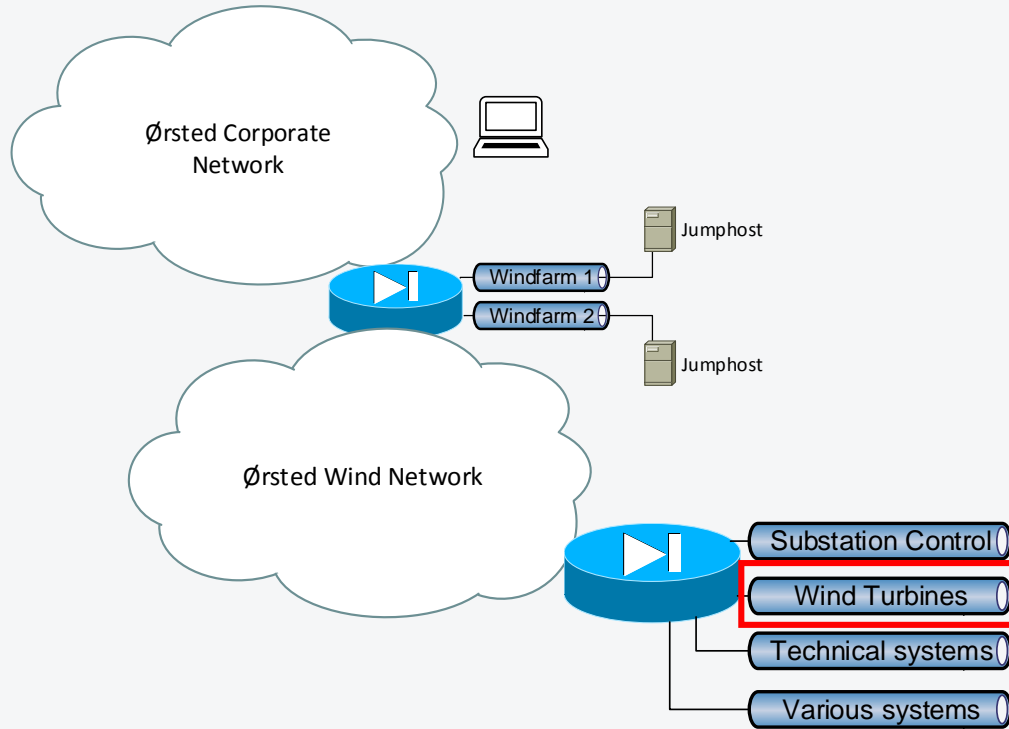
Substation Control System



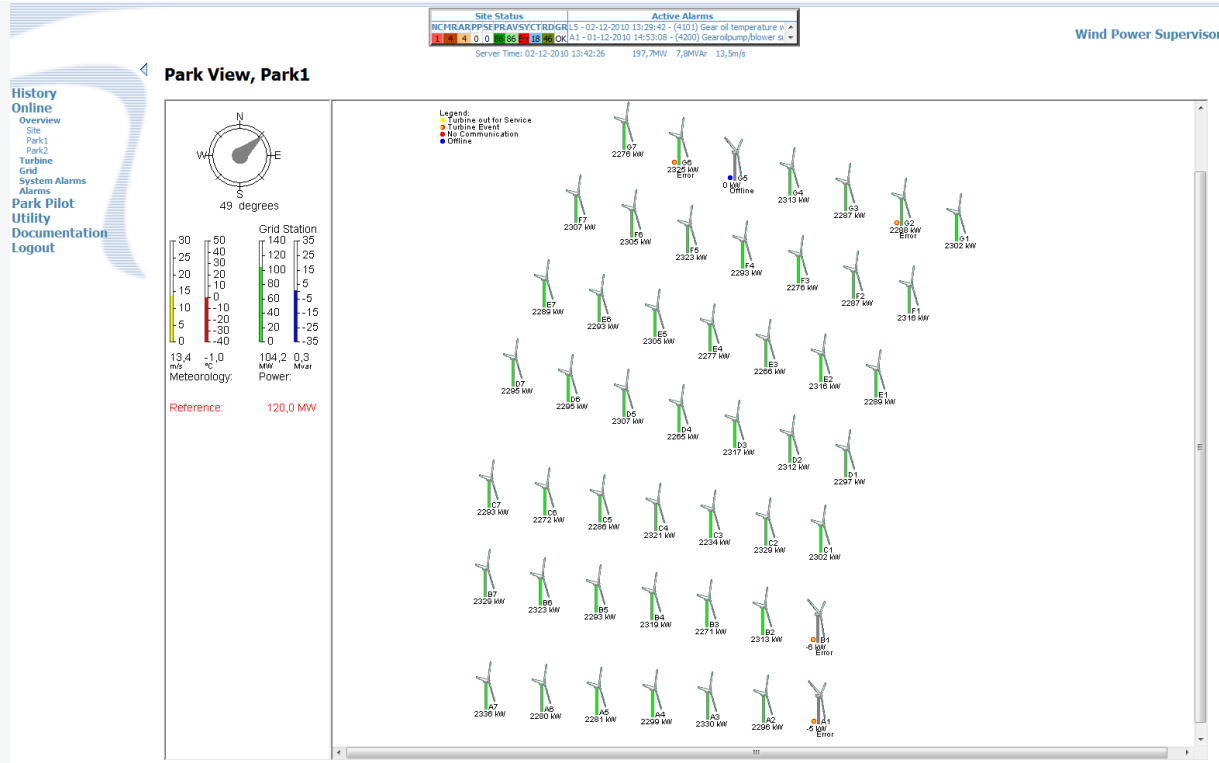
Substation Control System



Ørsted Architecture



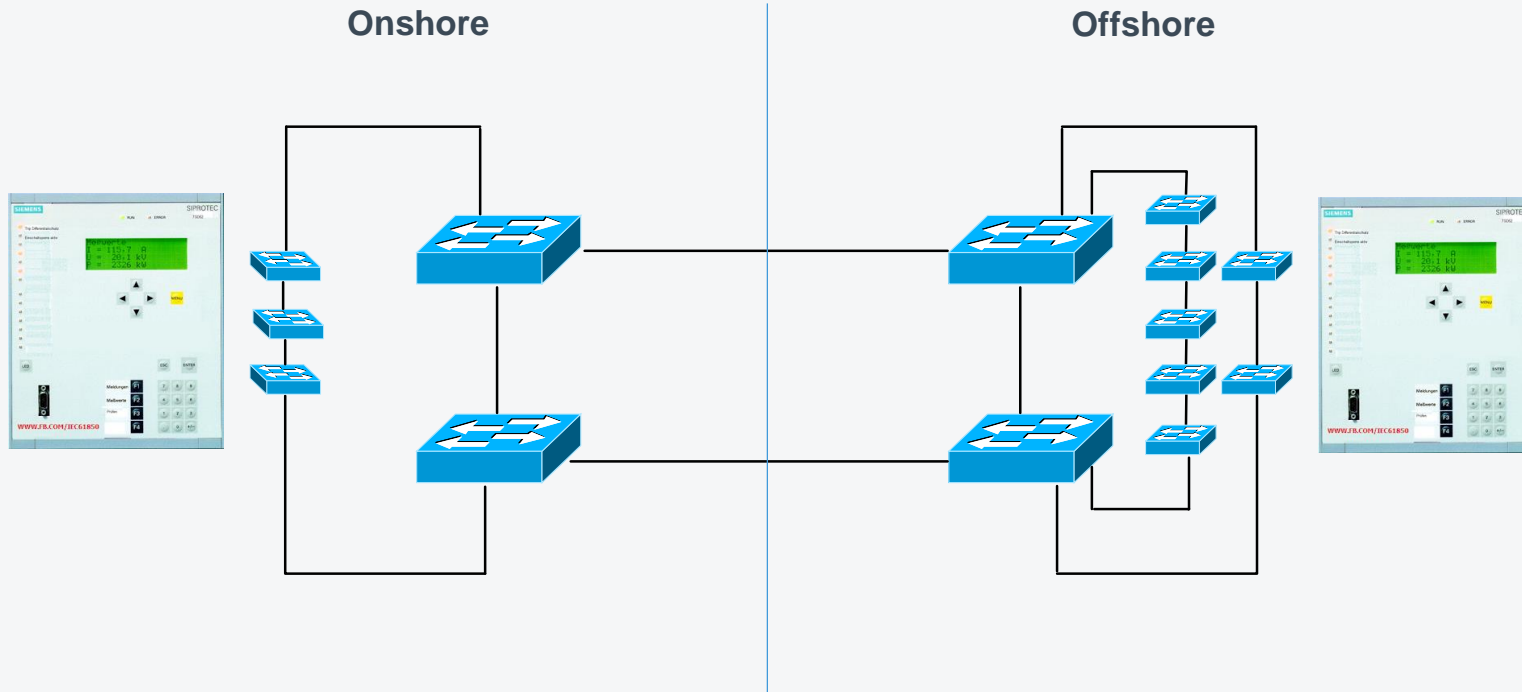
Wind Turbine SCADA



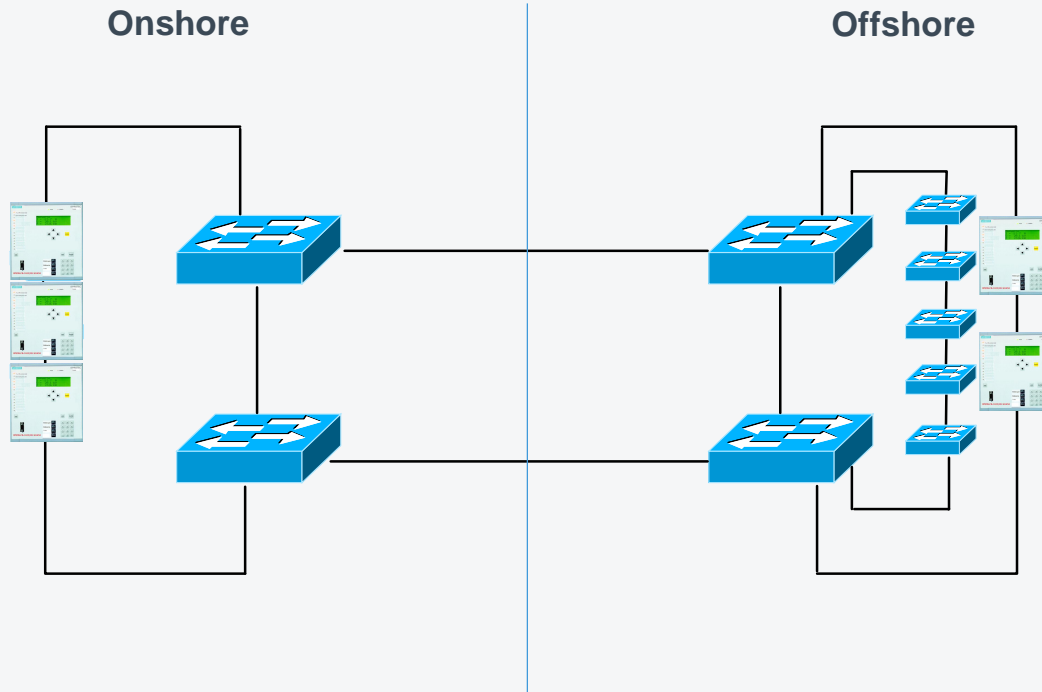
Wind Turbine SCADA



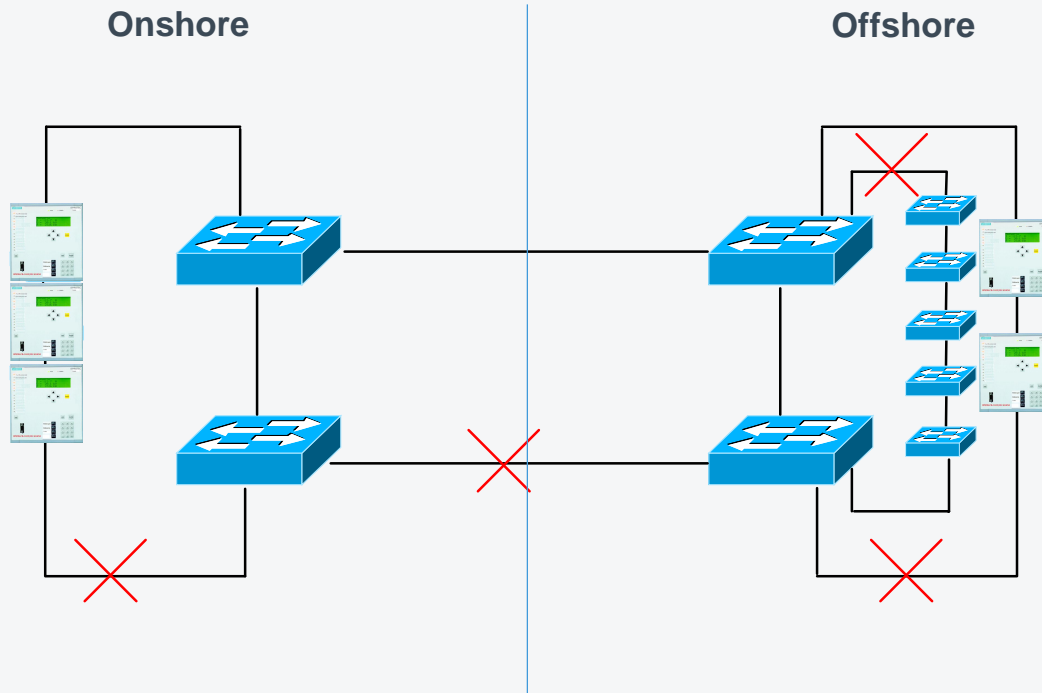
Typical design of the OT-network in a Substation Control System



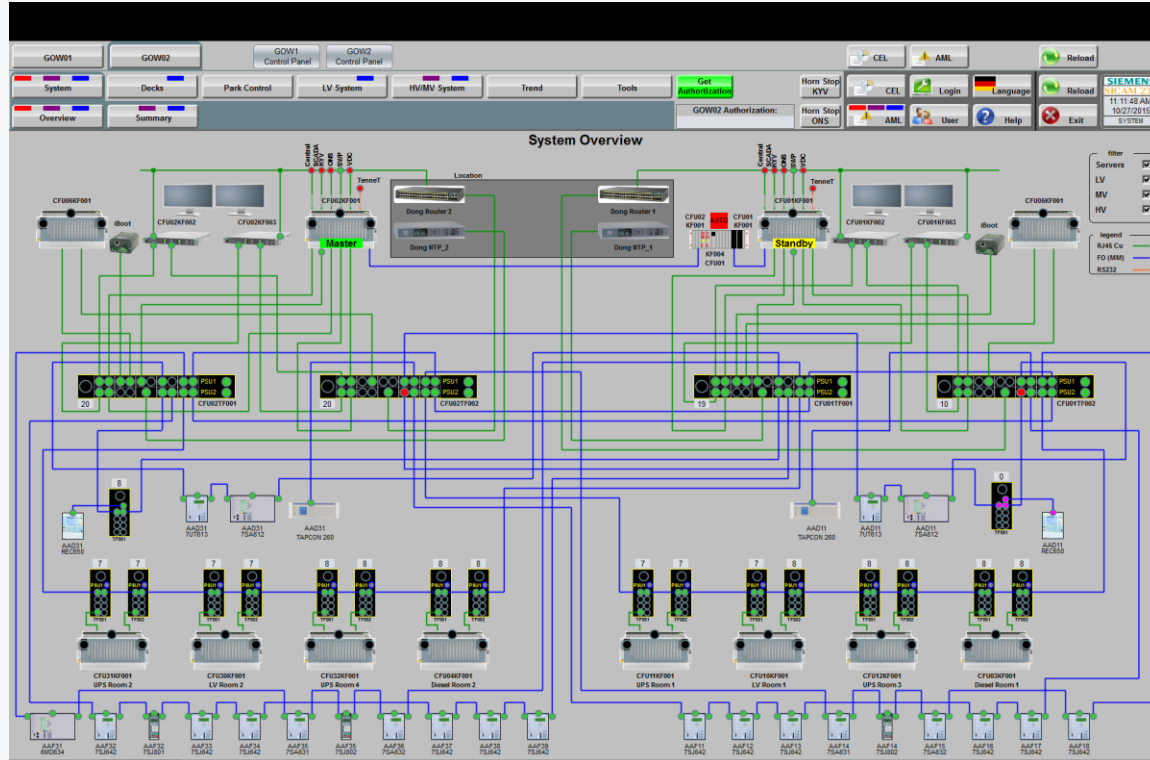
Typical design of the OT-network in a Substation Control System



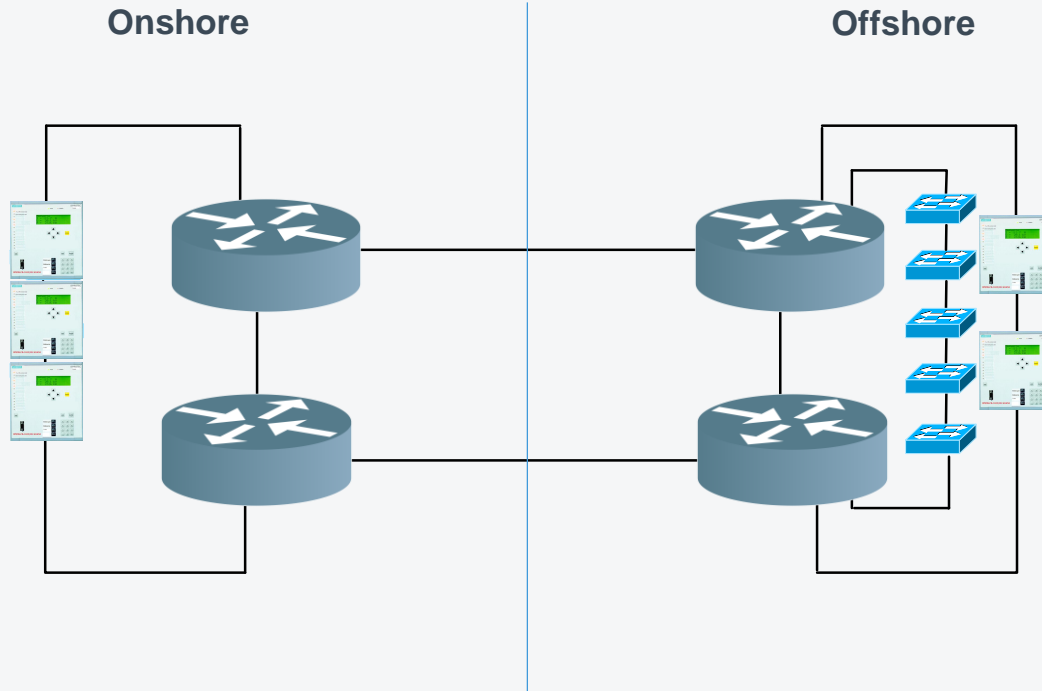
Typical design of the OT-network in a Substation Control System



SCS Network seen from the HMI



Simplified solution to the problem



L2 networks are limited by introducing routing

Primary protection is not depending on network protocols

Ørsted Information Security

Internal
Requirements
&
IEC 62443

Europe:
EU NIS

US:
NERC-CIP

Taiwan:
CIP&CIIP

Requirements for networks (and other OT systems)

Regulatory Compliance is getting more and more important!

NERC CIP as an example

The CIP standards and requirements have many dates and activities necessary for compliance. There are A LOT of recurring tasks that can easily slip through the cracks. Below is an outline of timing for performing against various CIP standards.

CIP COMPLIANCE PROCESS MANAGEMENT

AS NEEDED

- CIP-003: Update to CIP Senior Manager and Delegations
- CIP-004: Granting/Removal Physical and/or Cyber Access
- CIP-006: Visitor Escort and Logging into PSP
- CIP-007: Patch Install or Mitigation Plan Development/Update
- CIP-007: Malicious Code Signature Update
- CIP-008: Incident Response and Update to Incident Response Plan
- CIP-009: Lessons Learned & Plan Updates
- CIP-010: Baseline Updates and Documentation

ONGOING

- CIP-006: Monitor and Response to Unauthorized access into PSP
- CIP-006: Monitoring and Alarming of Unauthorized Access to PACS
- CIP-006: PSP Activity Logging and Log Retention
- CIP-007: System Logging, Alerting, and Log Retention

NERC CIP as an example

15 CALENDAR DAYS

- CIP-007: Sample Log Review

35 CALENDAR DAYS

- CIP-007: Patch Evaluation
- CIP-010: Baseline Review

CALENDAR QUARTER

- CIP-004: Security Awareness Reinforcement
- CIP-004: Verify Individuals with Active Electronic Access or Unescorted Physical Access

Baseline for netstat and task list output

```
C:\Documents and Settings\tetra>netstat -ao

Active Connections

Proto Local Address           Foreign Address         State       PID
TCP   BSC-20000732:echo      0.0.0.0:0                 LISTENING  1684
TCP   BSC-20000732:discard  0.0.0.0:0                 LISTENING  1684
TCP   BSC-20000732:daytime  0.0.0.0:0                 LISTENING  1684
TCP   BSC-20000732:gqtd      0.0.0.0:0                 LISTENING  1684
TCP   BSC-20000732:chargen  0.0.0.0:0                 LISTENING  1684
TCP   BSC-20000732:telnet   0.0.0.0:0                 LISTENING  1812
TCP   BSC-20000732:epmap    0.0.0.0:0                 LISTENING  1224
TCP   BSC-20000732:microsoft-ds 0.0.0.0:0             LISTENING  4
TCP   BSC-20000732:1027     0.0.0.0:0                 LISTENING  276
TCP   BSC-20000732:1801     0.0.0.0:0                 LISTENING  276
TCP   BSC-20000732:2103     0.0.0.0:0                 LISTENING  276
TCP   BSC-20000732:2105     0.0.0.0:0                 LISTENING  276
TCP   BSC-20000732:2107     0.0.0.0:0                 LISTENING  276
TCP   BSC-20000732:3306     0.0.0.0:0                 LISTENING  772
TCP   BSC-20000732:3389     0.0.0.0:0                 LISTENING  1172
TCP   BSC-20000732:netbios-ssn 0.0.0.0:137           LISTENING  4
TCP   BSC-20000732:3389     0.0.0.0:0                 ESTABLISHED 1172
TCP   BSC-20000732:netbios-ssn 0.0.0.0:137           LISTENING  4
TCP   BSC-20000732:1024     0.0.0.0:0                 ESTABLISHED 208
TCP   BSC-20000732:1024     0.0.0.0:0                 ESTABLISHED 208
TCP   BSC-20000732:1024     0.0.0.0:0                 ESTABLISHED 208
TCP   BSC-20000732:1024     0.0.0.0:0                 ESTABLISHED 208
TCP   BSC-20000732:1051     0.0.0.0:0                 ESTABLISHED 208
TCP   BSC-20000732:42024    0.0.0.0:0                 LISTENING  208
TCP   BSC-20000732:42389    0.0.0.0:0                 LISTENING  208
TCP   BSC-20000732:42389    0.0.0.0:0                 ESTABLISHED 208
TCP   BSC-20000732:42390    0.0.0.0:0                 LISTENING  208
TCP   BSC-20000732:42390    0.0.0.0:0                 ESTABLISHED 208
TCP   BSC-20000732:42390    0.0.0.0:0                 ESTABLISHED 208
TCP   BSC-20000732:42392    0.0.0.0:0                 LISTENING  208
TCP   BSC-20000732:42392    0.0.0.0:0                 ESTABLISHED 208
TCP   BSC-20000732:42392    0.0.0.0:0                 ESTABLISHED 208
TCP   BSC-20000732:42392    0.0.0.0:0                 ESTABLISHED 208
TCP   BSC-20000732:microsoft-ds 0.0.0.0:137           ESTABLISHED 4
TCP   BSC-20000732:1028     0.0.0.0:0                 ESTABLISHED 536
TCP   BSC-20000732:1029     0.0.0.0:0                 LISTENING  308
TCP   BSC-20000732:1033     0.0.0.0:0                 ESTABLISHED 536
TCP   BSC-20000732:3306     127.0.0.1:3306          ESTABLISHED 536
```

Image Name	PID	User Name	CPU	Mem Usage
System Idle Process	0	SYSTEM	98	16 K
System	4	SYSTEM	01	220 K
rdpclip.exe	116	tetra	00	4,476 K
BSC_.exe	208	SYSTEM	00	250,600 K
msqsvc.exe	276	SYSTEM	00	6,272 K
msdtc.exe	300	NETWORK SERVICE	00	5,220 K
alg.exe	308	LOCAL SERVICE	00	3,740 K
dhcprv.exe	392	SYSTEM	00	2,964 K
LogServerTray.exe	528	tetra	00	2,816 K
LogServer.exe	536	SYSTEM	00	354,228 K
mqtgsvc.exe	704	SYSTEM	00	4,088 K
winlogon.exe	732	SYSTEM	00	5,768 K
mysqld.exe	772	SYSTEM	00	29,412 K
smss.exe	828	SYSTEM	00	400 K
csrss.exe	880	SYSTEM	00	4,604 K
winlogon.exe	904	SYSTEM	00	5,264 K
services.exe	948	SYSTEM	00	4,212 K
lsass.exe	960	SYSTEM	00	2,908 K
csrss.exe	1008	SYSTEM	00	2,916 K

15 CALENDAR MONTHS

- CIP-002: BES Cyber System Identification
- CIP-003: CIP Senior Manager Approval of Policies
- CIP-004: Verify Access to BES Cyber System Information
- CIP-004: Verify Access Privileges
- CIP-004: Cyber Security Training
- CIP-004: Cyber Security Awareness Reinforcement
- CIP-007: Password Change
- CIP-008: Incident Response Plan Test
- CIP-009: Test Sample of Recovery Information
- CIP-009: Recovery Plan Test for High & Medium
- CIP-010: Paper or Active VA

Fines under NERC CIP

- **Violations of the NERC-CIP Standards**

- Are discovered via:

- SR = Self Report SC = Self Certification CA = Compliance Audit SPC = Spot Check CI = Compliance Investigation

- **Real Life Example**

- **Violation of Multiple CIP standards**

- **Company:** Unidentified Registered Entity (URE)

- **NERC Regional Entity Comment:**

- *” The root causes of these violations were **cultural issues** that resulted **in URE management’s lack of awareness, engagement, and accountability for CIP compliance**” (29.02.2016)*

- **Original Penalty Amount:** Undisclosed

- **Agreed Settlement:** **\$1.7 million**

- **Source:** http://www.nerc.com/pa/comp/CE/Enforcement%20Actions%20DL/PUBLIC_CIP_FinalFiled_NOC-2463_Full_NOP_Settlement_REV.pdf

1

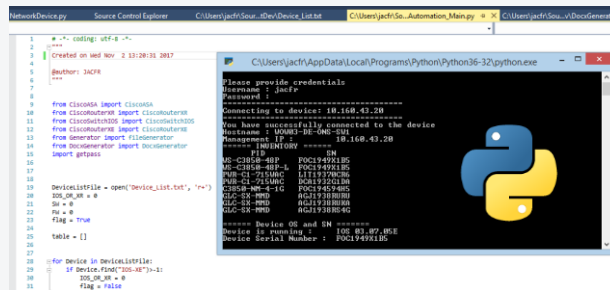
Network inventory is automatically gathered using the ANSIBLE framework.

2

Automated Test of the network with custom scripts written in python

3

MS Word document is generated with recommended actions.

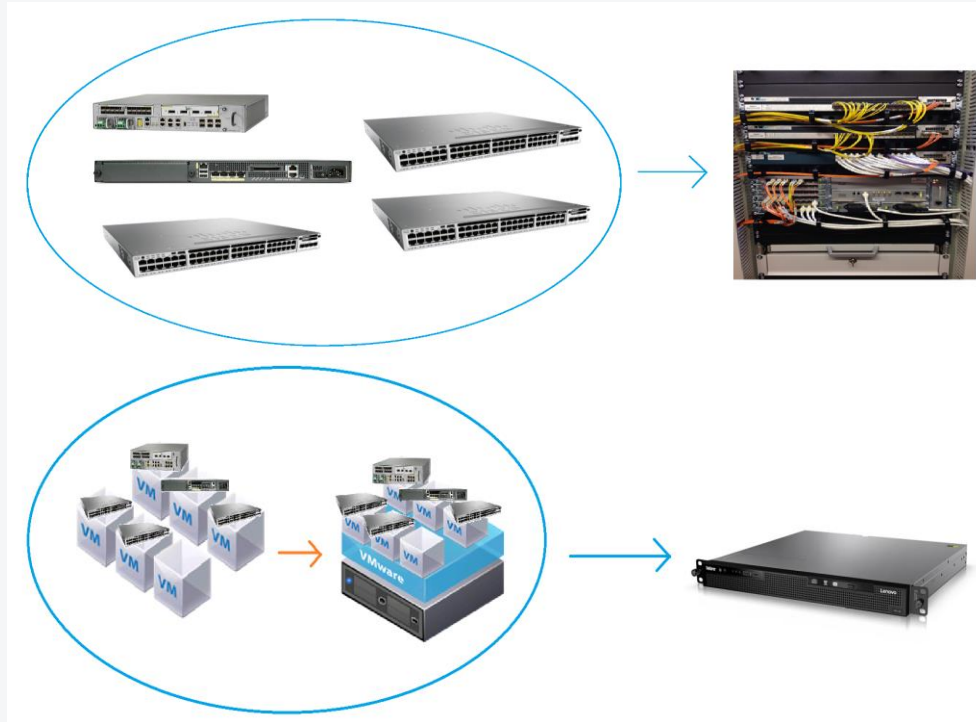


```
NetworkDevice.py  Source Control Explorer  C:\Users\jacfr\Gou...>Dev\Device_Liste  C:\Users\jacfr\Go...>Automation_Main.py  C:\Users\jacfr\Gou...>DocuGenerator
```

```
1 # -*- coding: utf-8 -*-
2 # ---
3 # created on wed nov 2 13:20:11 2017
4 #
5 # Author: jacfr
6 # ---
7
8 from ciscoasa import ciscoasa
9
10 from ciscoairtel import ciscoairtel
11 from ciscoairtel import ciscoairtel
12 from ciscoairtel import ciscoairtel
13 from ciscoairtel import ciscoairtel
14 from generator import ciscoairtel
15 from docgenerator import docgenerator
16
17 import getpass
18
19
20 device_listfile = open('device_list.txt', 'w+')
21
22 ssl_on = 0
23
24 flag = 0
25
26 table = []
27
28 # for Device in DeviceListfile:
29 #     if Device.find("IOS-XE")>=1:
30 #         ssl_on = 0
31 #         flag = raise
```

```
Please provide credentials
Username : jacfr
Password :
Connecting to device! 10.100.43.20
-----
You have successfully connected to the device
Username : DOUB3-D1-0NS-SUI
Password: IP e
----- INVENTORY -----
----- SN -----
VC-CISE-48P          FOC1949K1B5
VC-CISE-48P          FOC1949K1B5
PUB-CL-7100MC        L111970K76
PUB-CL-7100MC        DOA1943140
PUB-CL-7100MC        FOC1943140
CUC-IX-PMD           RG1938800
CUC-IX-PMD           RG1938800
CUC-IX-PMD           RG1938800
----- Device OS and SN -----
Device ID number : 100.80.87.85E
Device Serial Number : FOC1949K1B5
```

Network virtualization



The Ørsted Way
Let's create a
world that runs
entirely on green
energy



Q&A