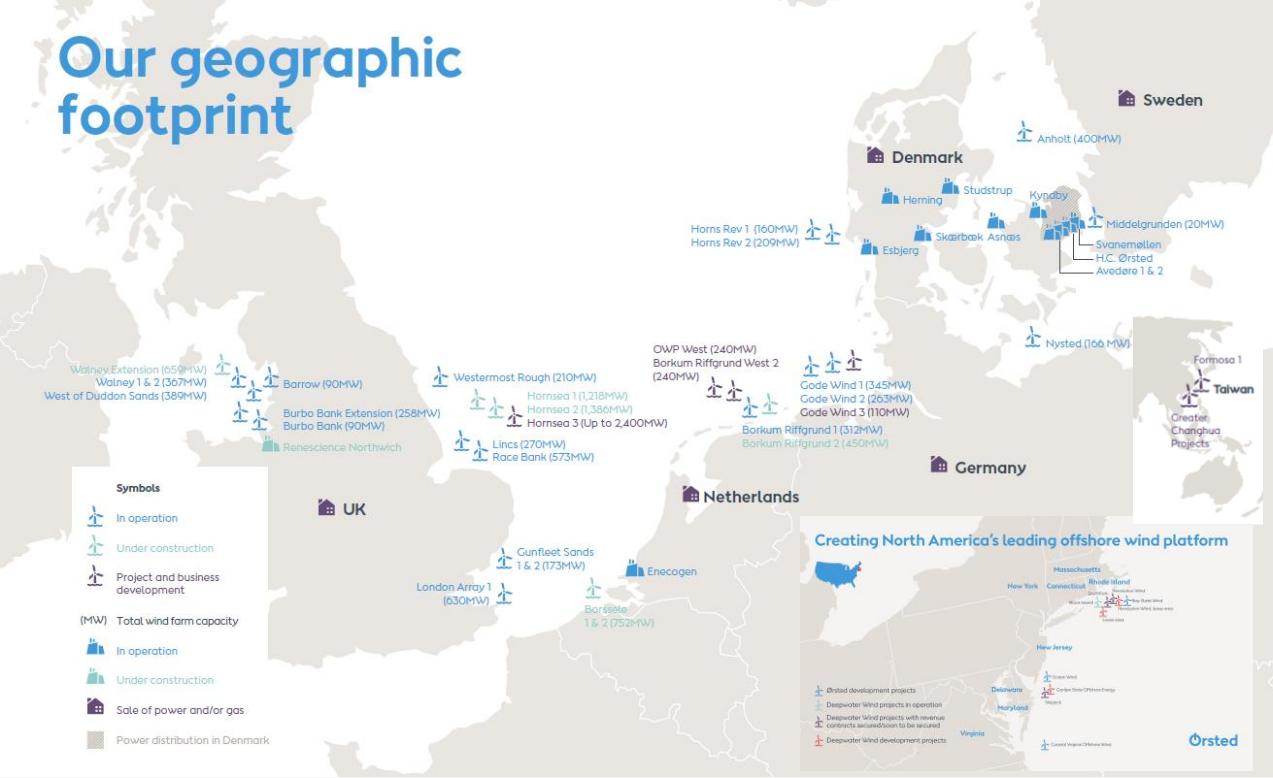
OT-Networks

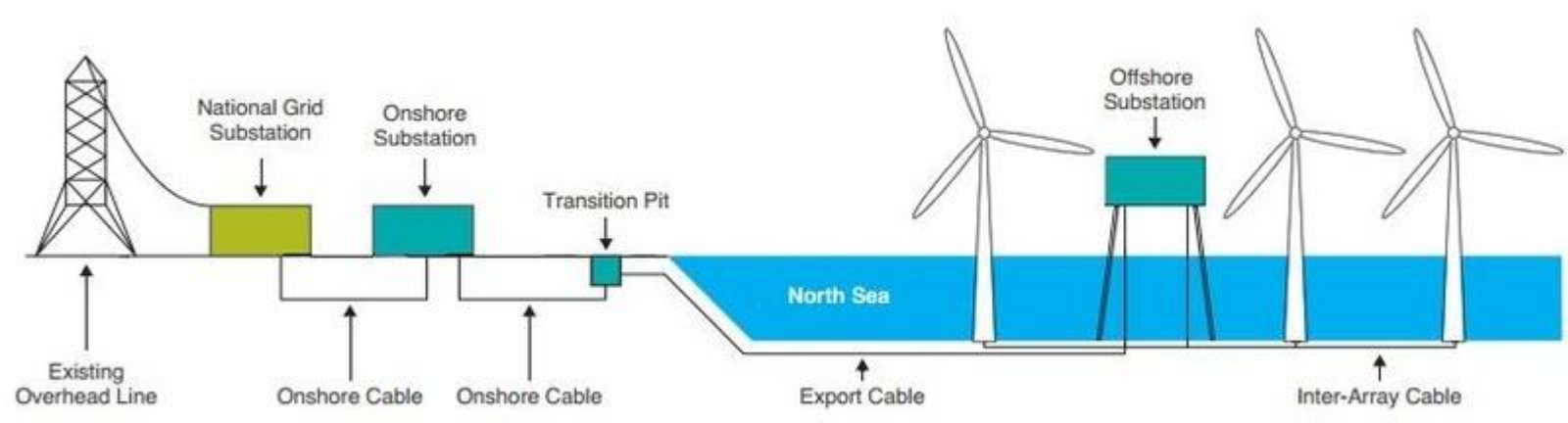
How is Ørsted working with architecture and security. What are the funtional requirements to the neworks seen from the system side

Mads Thorsted Nielsen
Manager SCADA Communication
30 Oct 2018

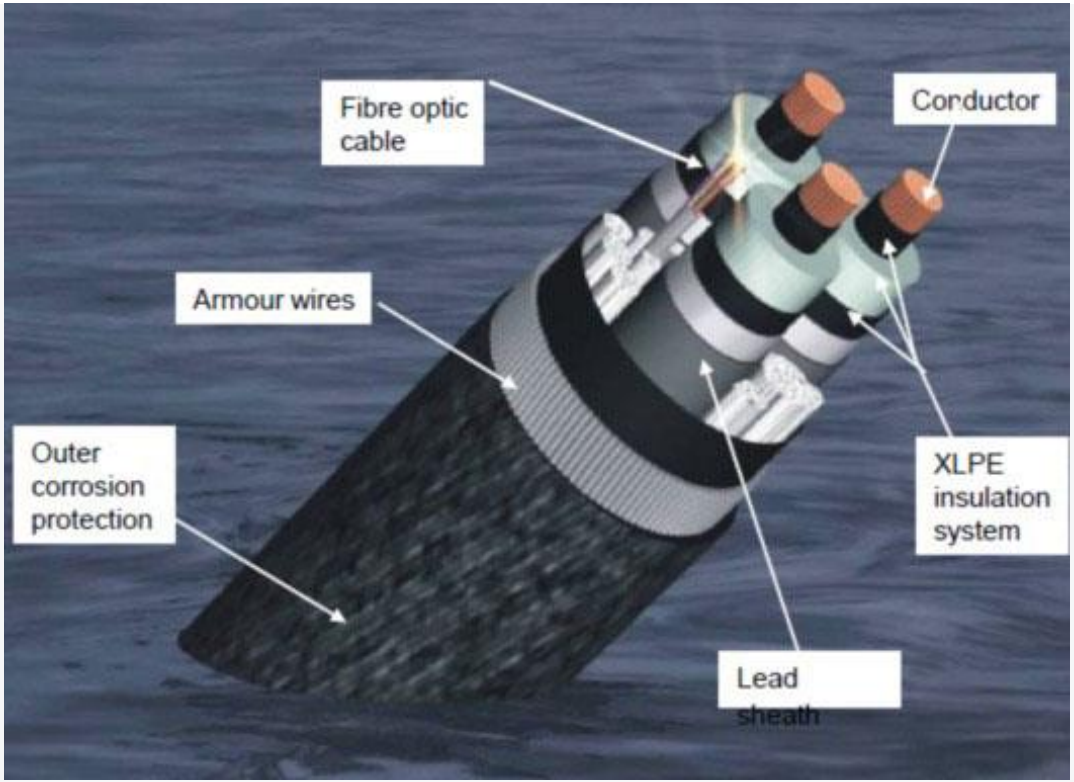
Our geographic footprint



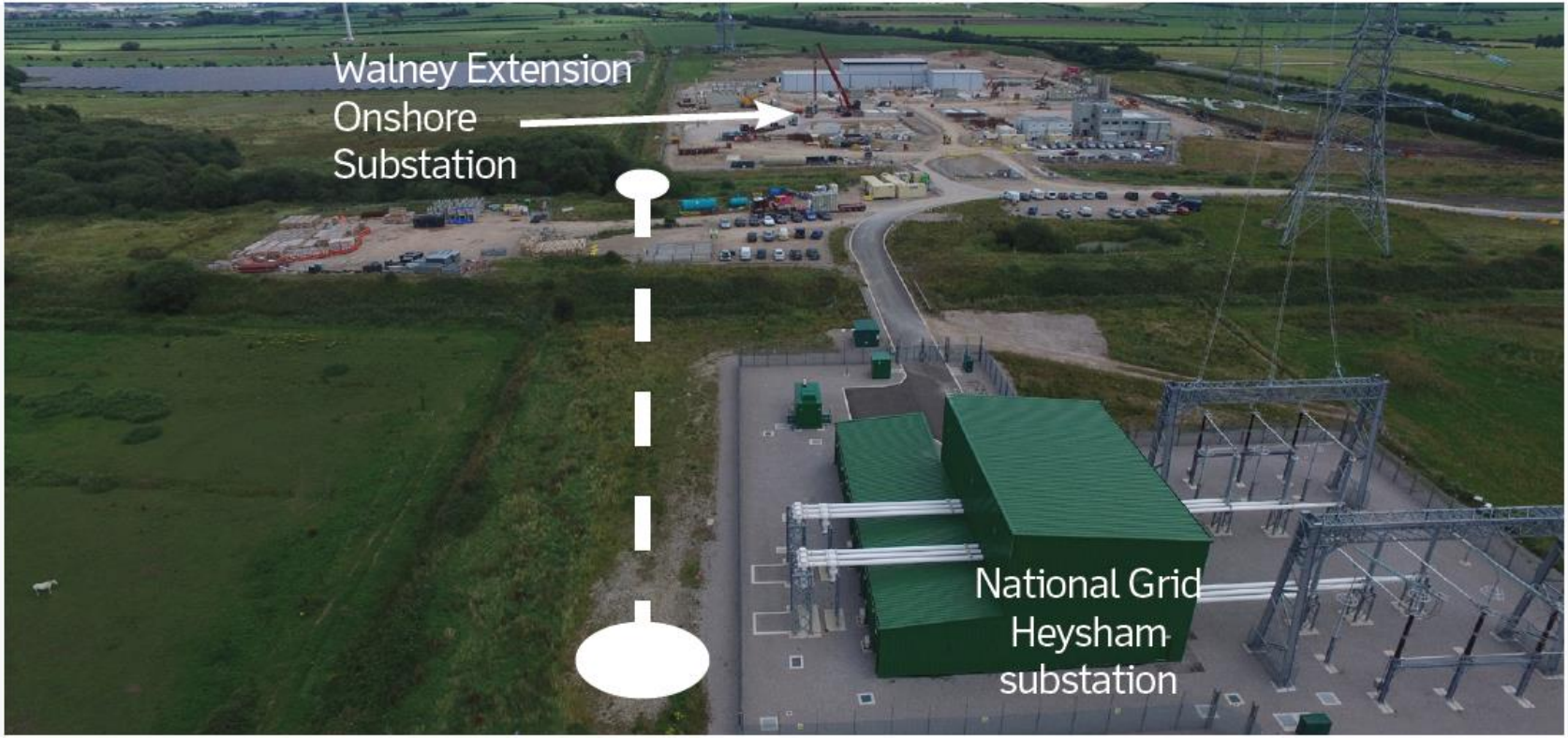
An offshore windfarm



Export cable



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

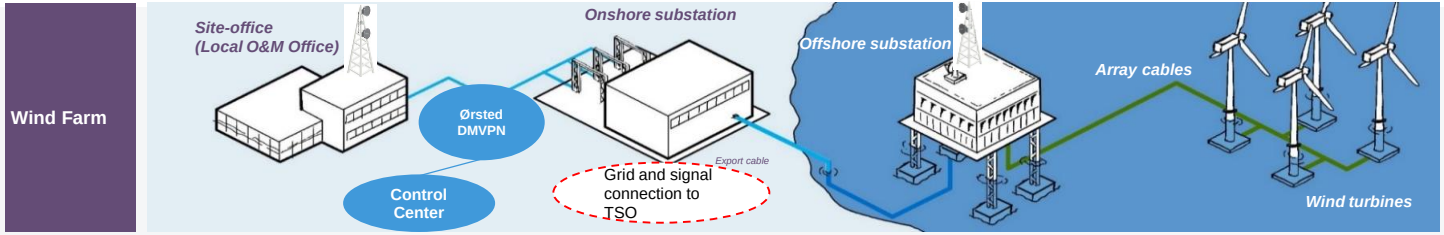


Ørsted

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)

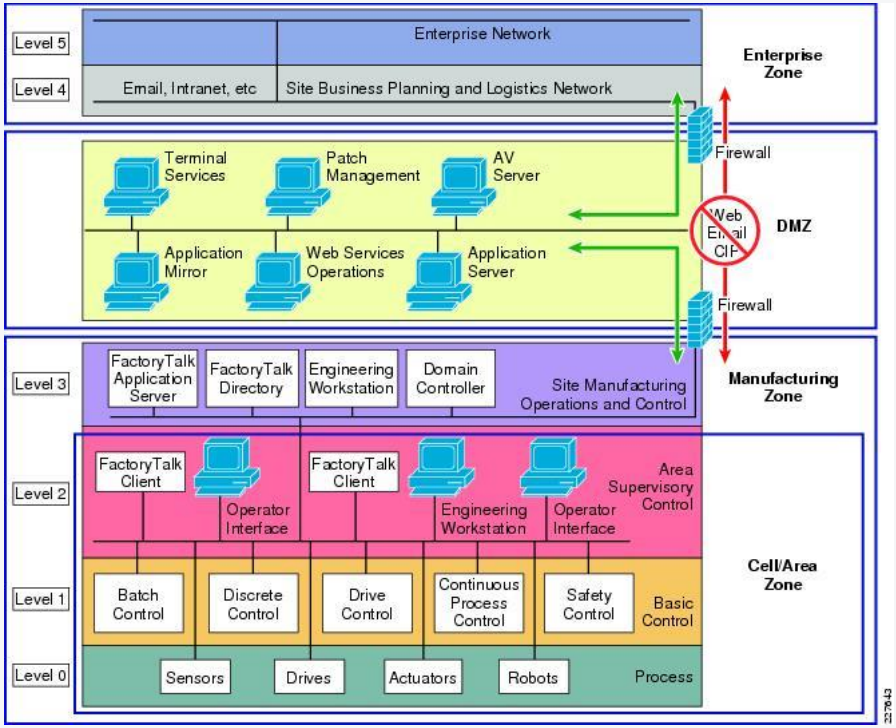
Measurement Systems
Wind Measurement (LIDAR), Wave Buoys

IT vs OT

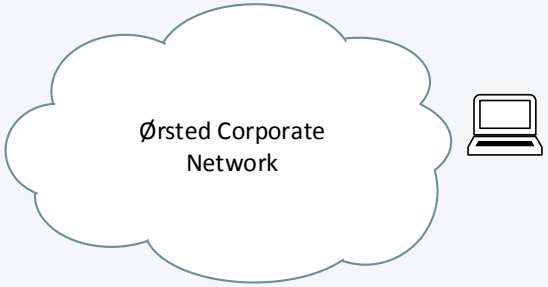
IT is dynamic	OT is deterministic
IT: Data is king	OT: Process is king
IT: Confidentiality is priority #1	OT: Control is priority #1
IT: Patch Tuesdays	OT: Patch…decade?

Ørsted

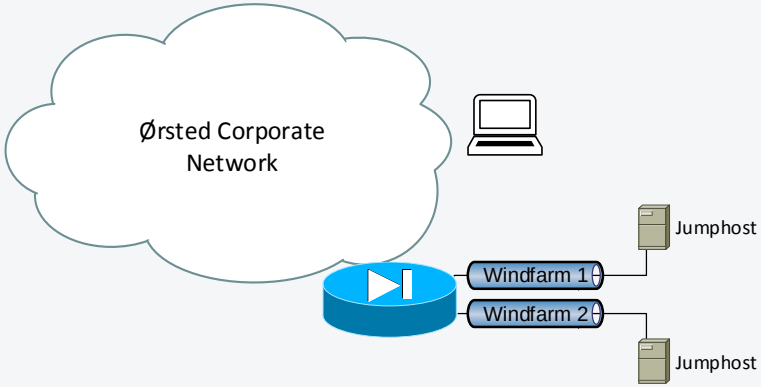
The architectural design



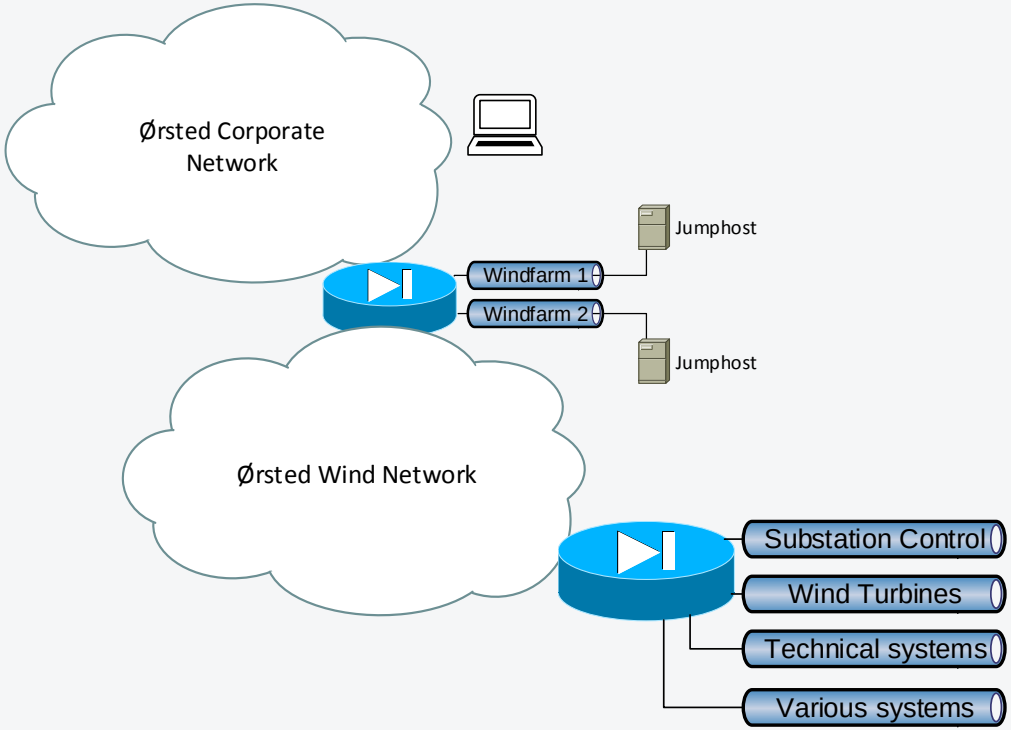
Ørsted Architecture



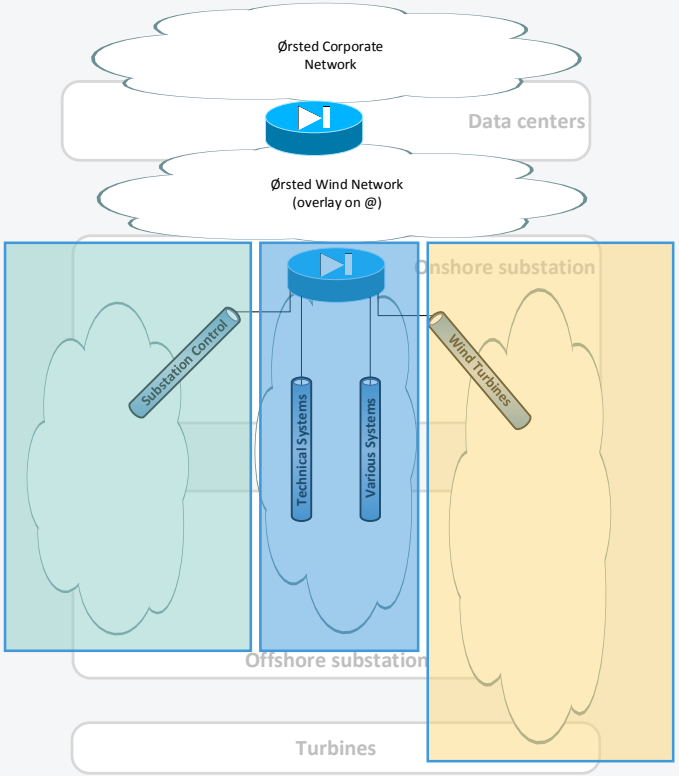
Ørsted Architecture



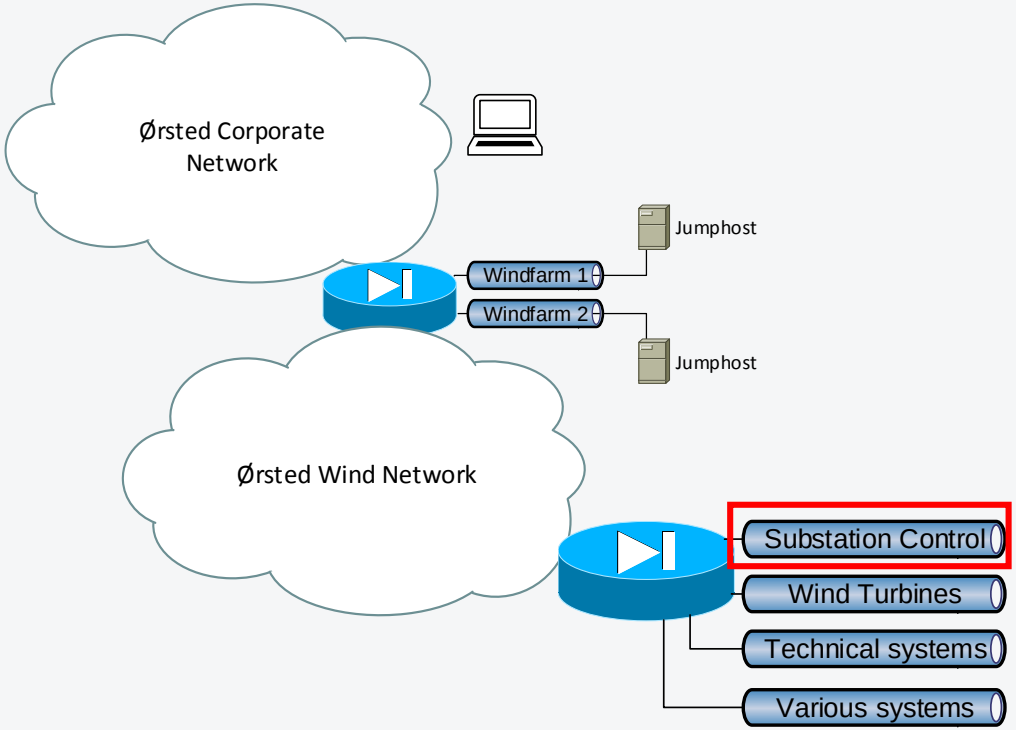
Ørsted Architecture



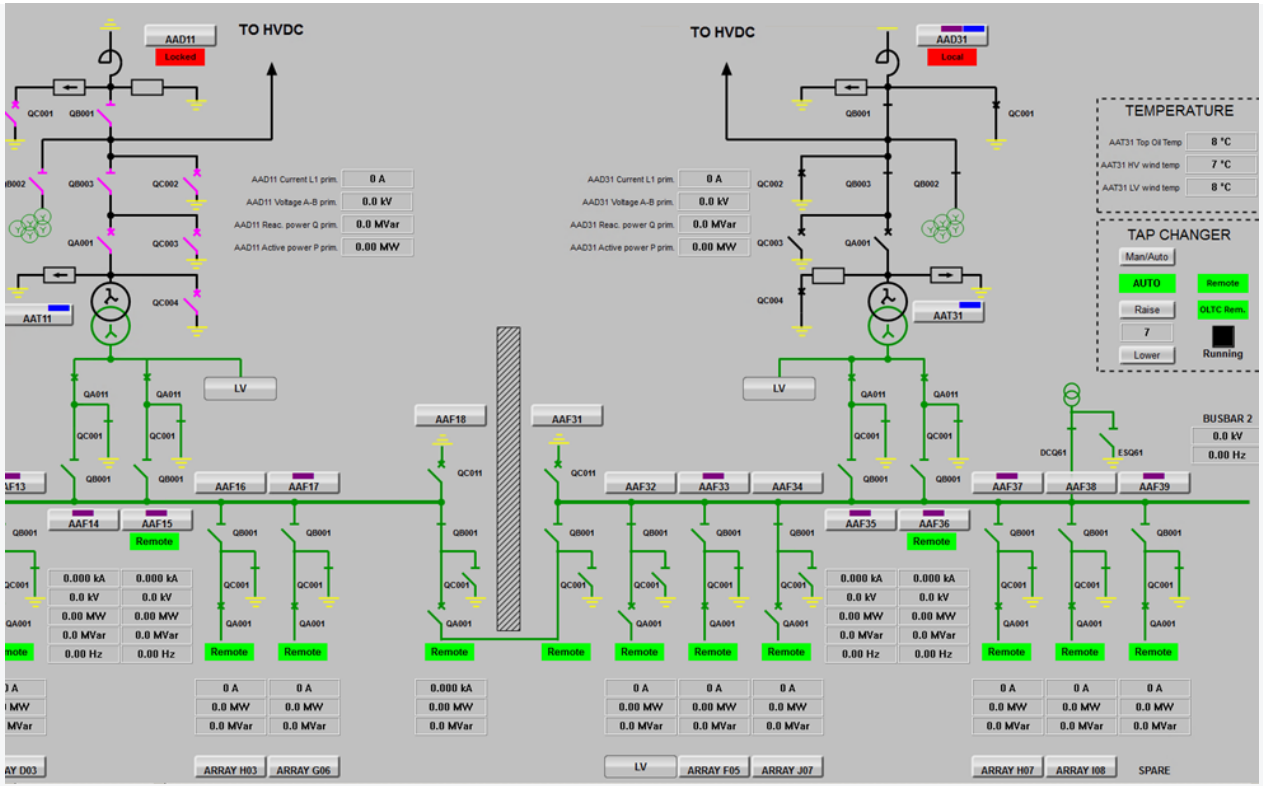
Network Deliveries



Ørsted Architecture

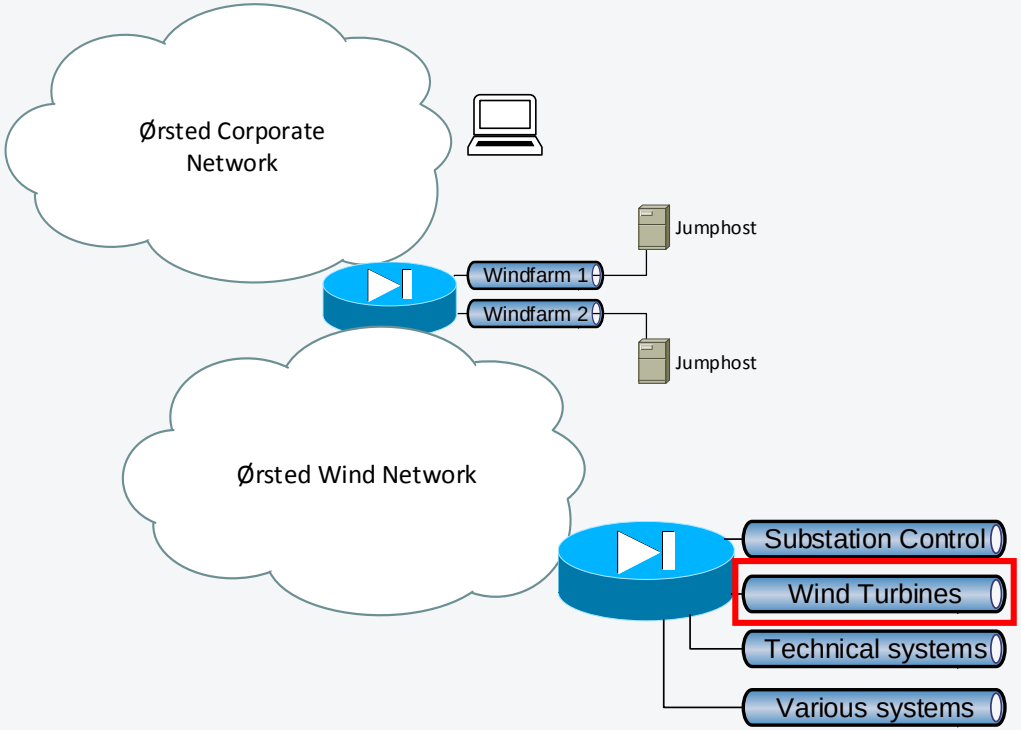


Substation Control System

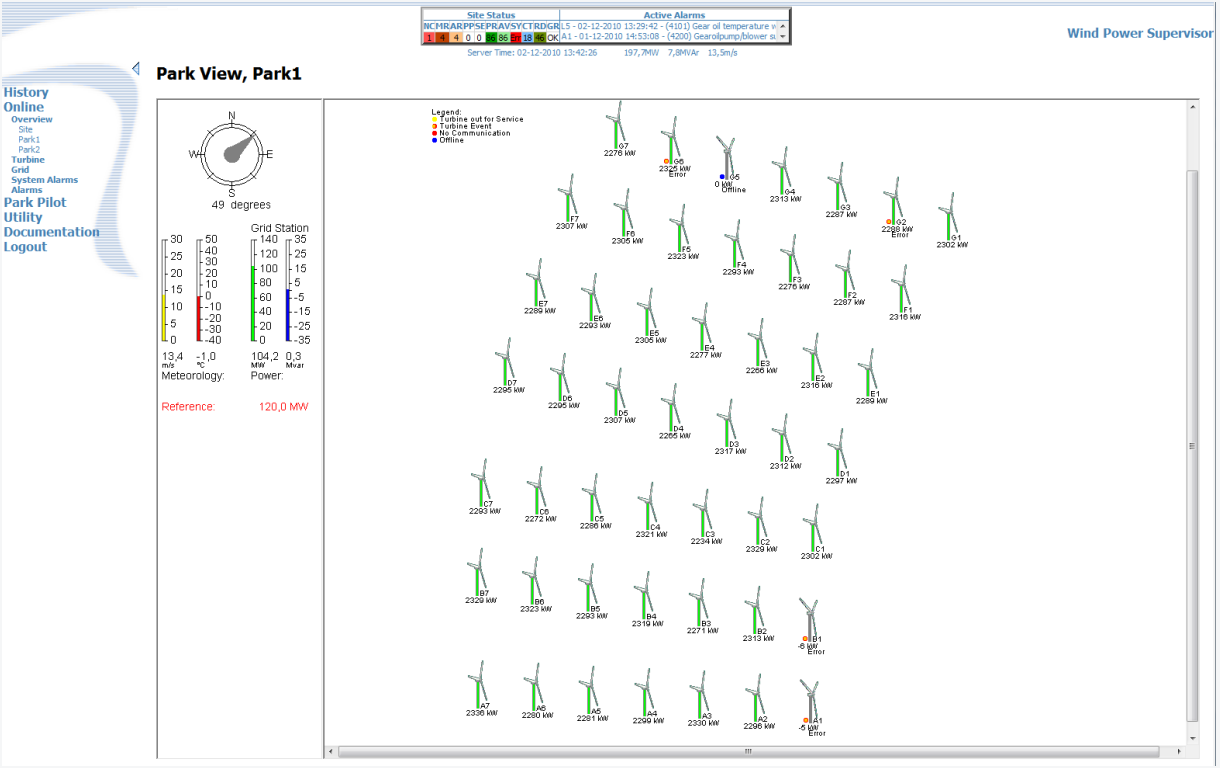


Substation Control System

Ørsted Architecture

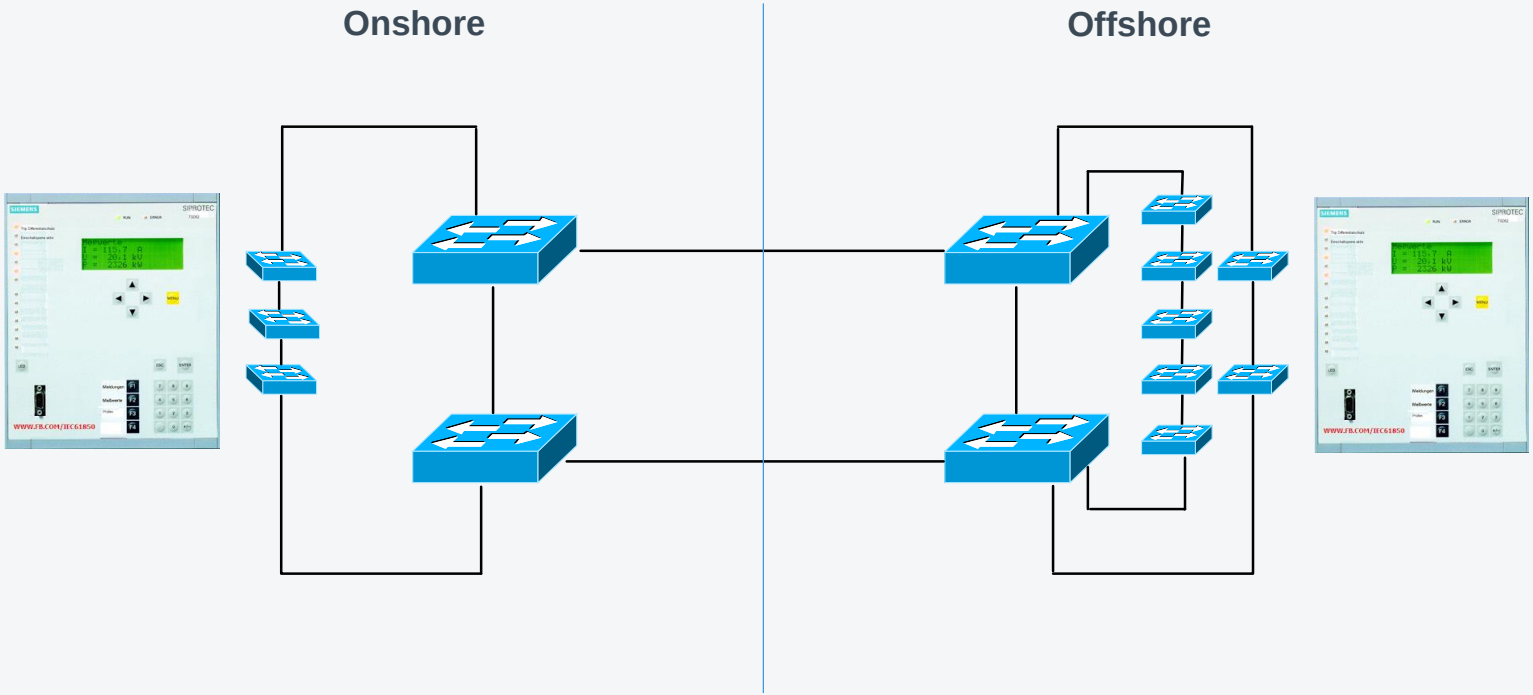


Wind Turbine SCADA

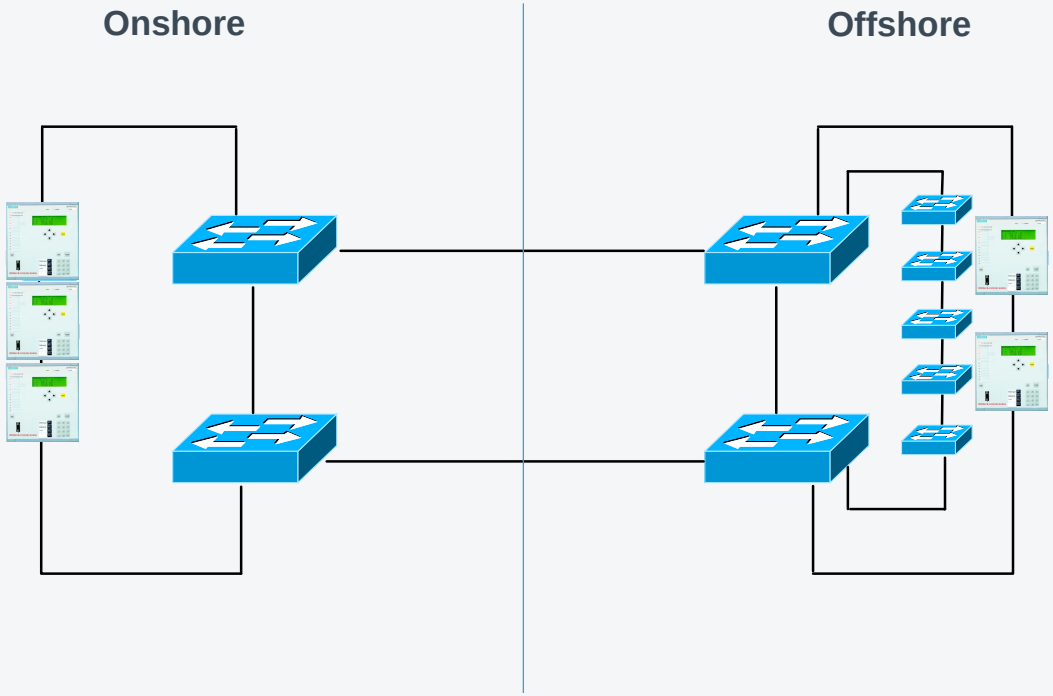


Wind Turbine SCADA

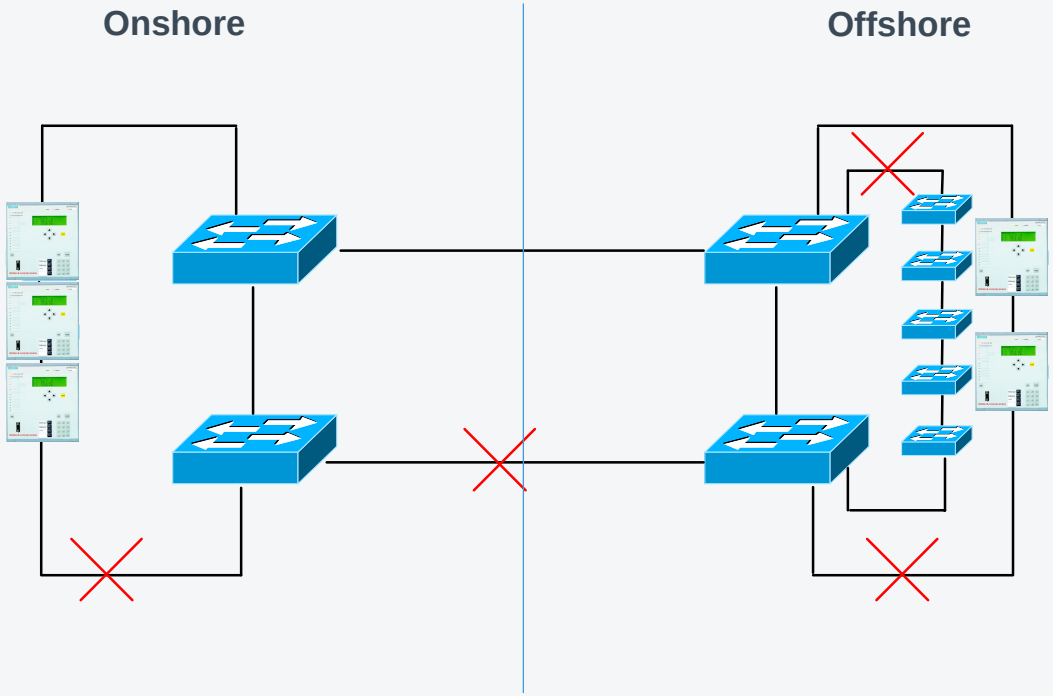
Typical design of the OT-network in a Substation Control System



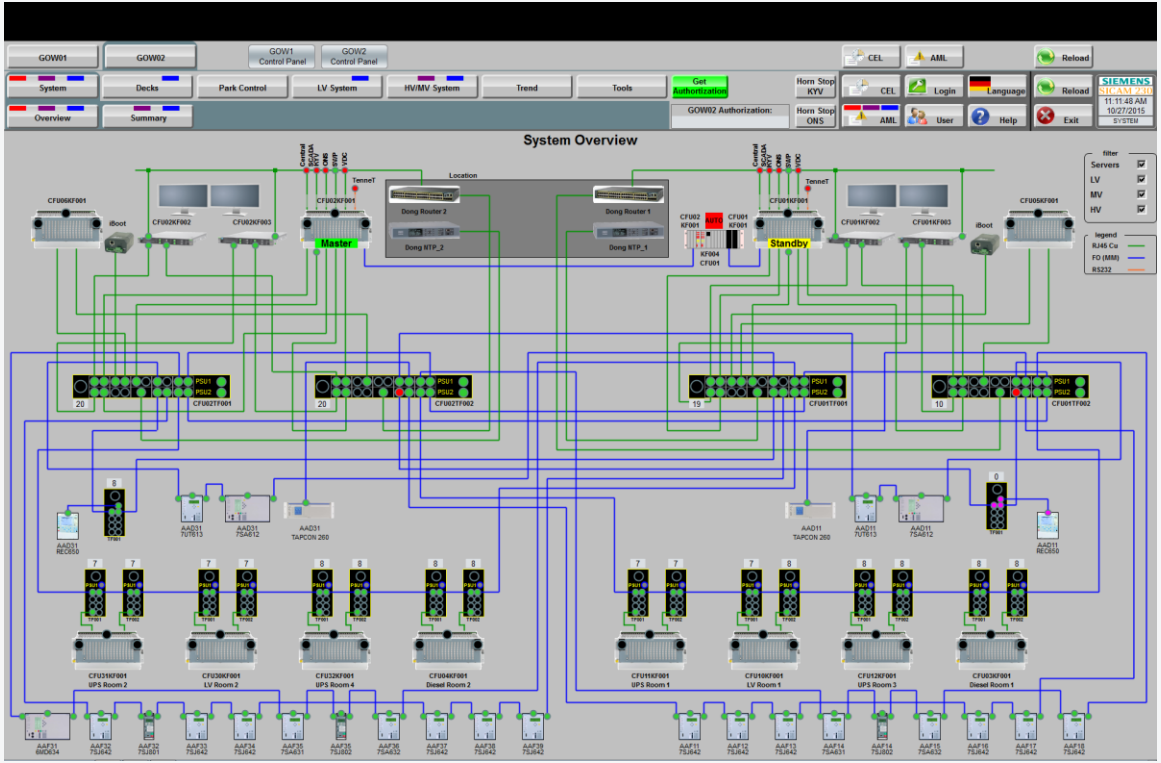
Typical design of the OT-network in a Substation Control System



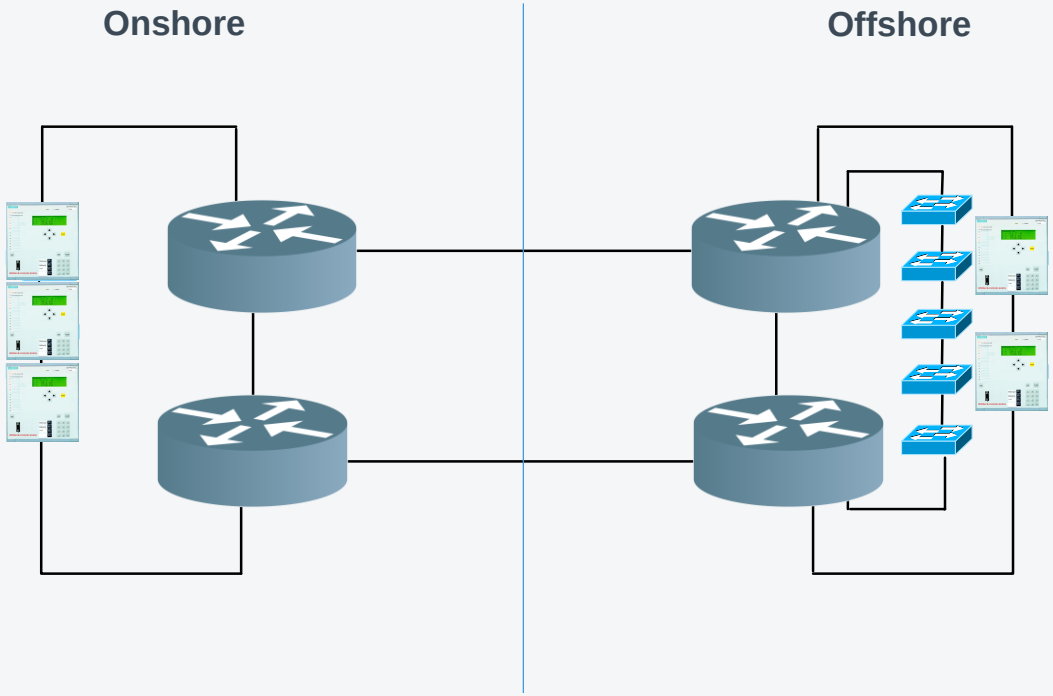
Typical design of the OT-network in a Substation Control System



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

Security Requirements

Ørsted Information Security			
Internal Requirements & IEC 62443	Europe: EU NIS	US: NERC-CIP	Taiwan: CIP&CIIP

Ørsted

Requirements for networks (and other OT systems)

Regulatory Compliance is getting more and more important!

Ørsted

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

Ørsted

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

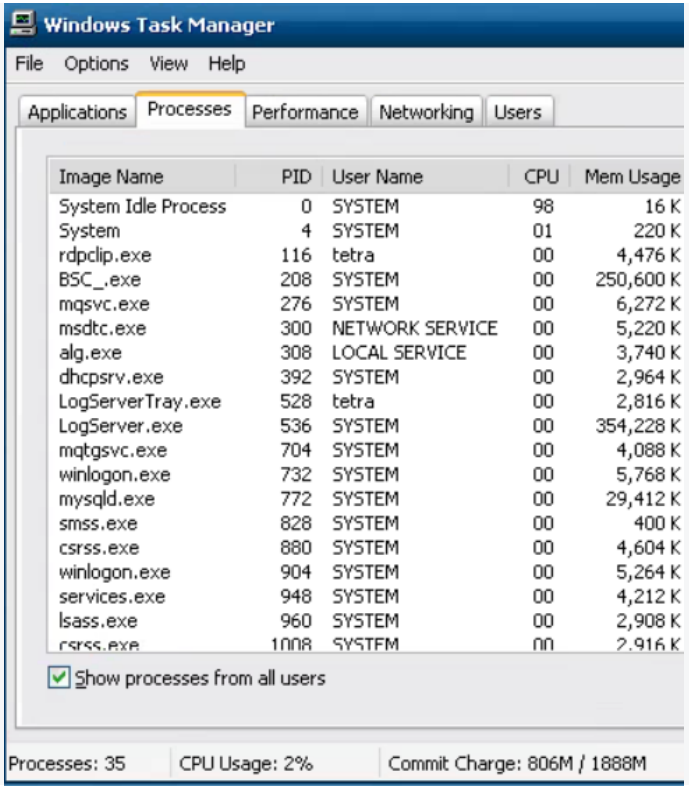
Ørsted

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:qotd      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-s                        LISTENING       4
  TCP    BSC-20000732:3389                             ESTABLISHED     1172
  TCP    BSC-20000732:netbios-s                        LISTENING       4
  TCP    BSC-20000732:1024                             LISTENING       208
  TCP    BSC-20000732:1024                             ESTABLISHED     208
  TCP    BSC-20000732:1024                             ESTABLISHED     208
  TCP    BSC-20000732:1024                             ESTABLISHED     208
  TCP    BSC-20000732:1051                             ESTABLISHED     208
  TCP    BSC-20000732:42024                            LISTENING       208
  TCP    BSC-20000732:42389                            LISTENING       208
  TCP    BSC-20000732:42389                            ESTABLISHED     208
  TCP    BSC-20000732:42390                            LISTENING       208
  TCP    BSC-20000732:42390                            ESTABLISHED     208
  TCP    BSC-20000732:42390                            ESTABLISHED     208
  TCP    BSC-20000732:42392                            LISTENING       208
  TCP    BSC-20000732:42392                            ESTABLISHED     208
  TCP    BSC-20000732:42392                            ESTABLISHED     208
  TCP    BSC-20000732:microsoft                        ESTABLISHED     4
  TCP    BSC-20000732:1028                             ESTABLISHED     536
  TCP    BSC-20000732:1029                             LISTENING       308
  TCP    BSC-20000732:1033      localhost:3306         ESTABLISHED     536
```



Ørsted

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

Ørsted

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

Ørsted

Automation

1

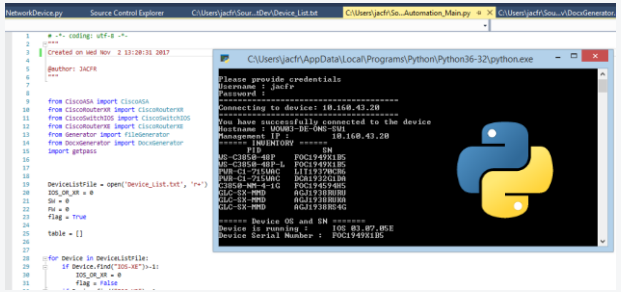
Network inventory is automatically gathered using the ANSIBLE framework.

2

Automated Test of the network with custom scrips written in python

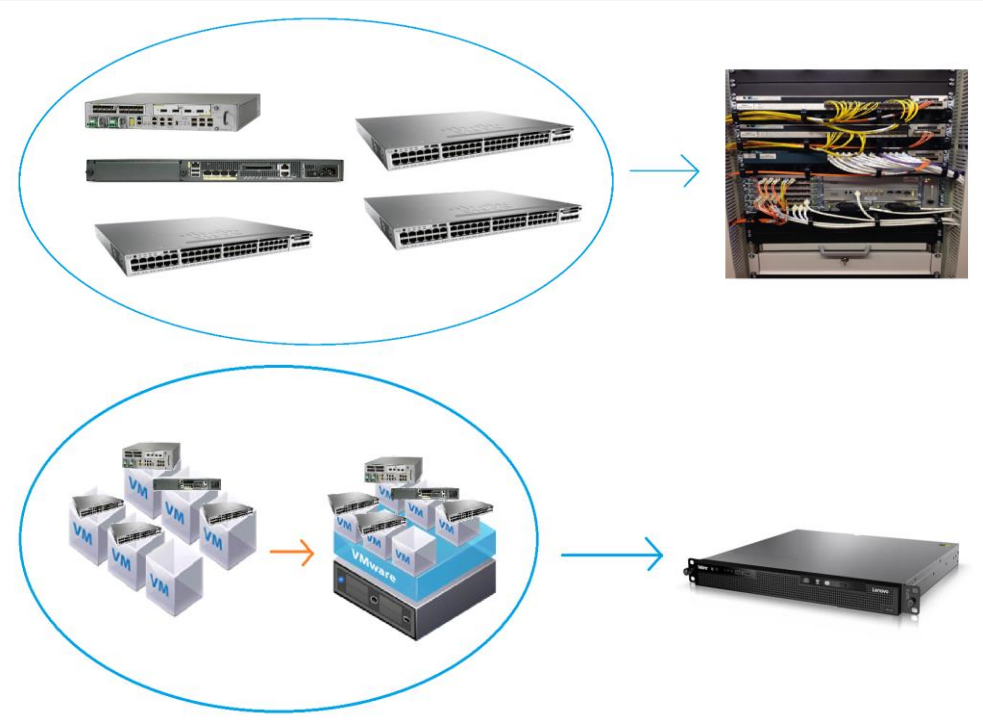
3

MS Word document is generated with recommended actions.



Ørsted

Network virtualization



The Ørsted Way

Let’s create a world that runs entirely on green energy

Q&A

Ørsted