# Assessment of Current Status of Cyber Security Measures for OT equipment in Cyber-Physical Power Systems

CIGRE D2 Data Science and Next Generation Communications in Electricity Networks

30/06/2023

MANCHESTER 1824

The University of Manchester

cigre

For power system expertise

nationalgrid

SP ENERGY NETWORKS

Speaker: Dr Haiyu Li

University of Manchester,

# Completed and Ongoing Projects

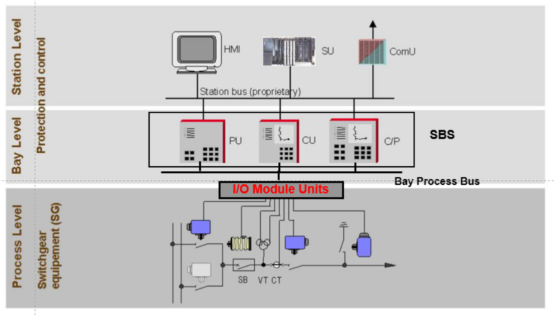
- 2008 – 2011 National Grid (NG) NIA " Architecture of Substation Secondary System (AS3) project – Based on the assessment of digital substation reliability vs life cycle cost, Manchester designed and delivered a reliable, flexible and agile architecture for substation secondary systems.
- 2015 – 2017 NG NIA "Virtual Substation Acceptance Test and Training (VSATT) project - Manchester built VSATT facility with 5 vendor PAC bay solutions in the lab and helped to test and prove AS3 solution.
- 2016 – 2020 Scottish Power (SPEN) NIC "Future Intelligent Transmission NEtwork SubStation ( FITNESS)" project - Manchester helped, assessed and tested PRP and HSR configuration performance for PAC system using VSATT.
- 2019 – 2021 NG NIA IEC61850 Cyber Resilient Electric Substation Technologies (CREST) project - Manchester conducted assessment of current cyber security technologies and tested some commercial available cyber security tools and solutions, such as Omicron StationGuard.
- 2020 – 2021 NG NIA "Cyber Security Solutions for Legacy Equipment (CSLE)" - Manchester conducted the assessment of some vendors cyber security solutions for legacy equipment. Also conducted risk assessment using Markov Process Model.
- 2023- 2025 SPEN and NG NIA "Cyber Security for Active and Flexible Energy Networks (Cyber-SAFEN)". The main focus is to develop defense methods for Protection, Automation and Control (PAC) and SCADA systems.

# Completed Projects

## AS3 (2008-2011)

Architecture of Substation Secondary System (AS3) Project

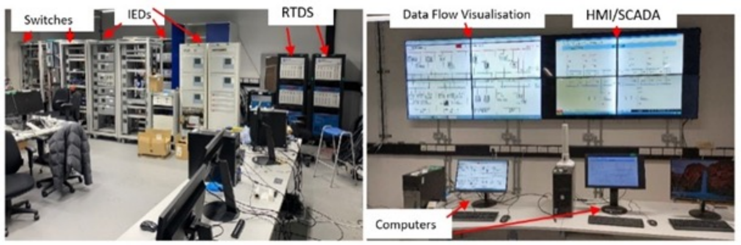
- To form a new policy for substation light current systems aimed at maintaining high availability and reliability of the transmission network by balancing the whole life-cycle risk, performance and cost of assets;
- To develop a new architecture for substation secondary system targeting on a quicker, safer and easier approach for the installation and replacement of protection and control equipment beyond 2011 by introducing new technologies



## VSATT (2015-2018)

Virtual digital substation testing platform (VSATT) in lab environment with multi-vendor (5 key suppliers) bay solutions based on the NG AS3 Architecture

- System integration tool based on IEC 61850-6 SCL files,
- Visualisation tool for monitoring digitised data flow well as display all soft links between P&C equipment



## FITNNESS (2018 -2022)

- The first real life digital substation in the UK
- Live operation of the digital substation, including active integration of Protection automation and control (PAC) functions with multi -sensor interoperability,
- Providing the substation functionality to support wide are control and new emerging quality and latency requirements for system frequency and stability controls, and constraints management of renewable generation integration.

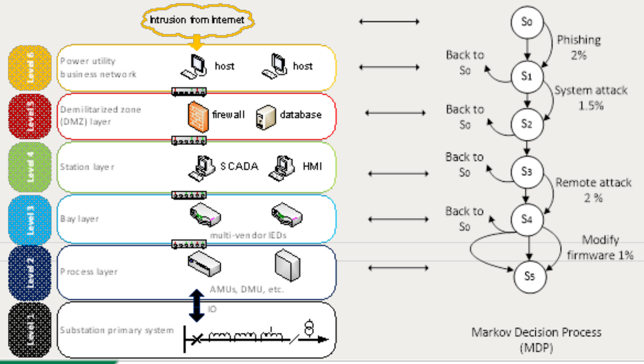
Future Intelligent Transmission NEtwork SubStation (FITNESS)

# Completed and Ongoing Projects

## CREST (2019-2021)

Cyber Resilient Electrical Substation Technology (CREST) project

- First assessment on cyber security, including Literature review; Threats and Standard substation message security;
- Tested various Intrusion detection systems (IDS);
- Software Defined Networks (SDN)
- Cybersecurity implications of IEC 61850 messages;
- Role Based Access control (RBAC);

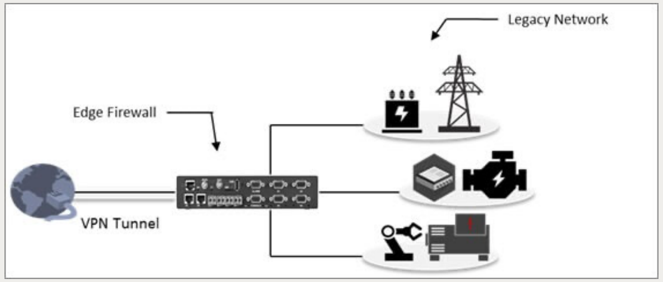


Markov Decision Process (MDP)

## CSLE (2021-2021)

Cyber Solutions for Legacy Equipment (CSLE) – Deliverable 3 Cyber security solutions

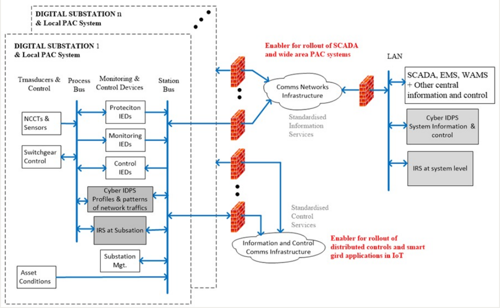
- Methods to secure legacy equipment, including (i) Endpoint security and (ii) Zone enforcement systems,
- Investigated Off-the-shelf products, include: (i) DeepArmor: Endpoint Security Solution, (ii) Kaspersky cybersecurity products, (iii) Floodgate Defender Mark III, (iv)  OpShield from GE Digital



## Cyber SAFEN (2023-2025)

Cyber Security for Active and Flexible Energy Networks (Cyber-SAFEN)

- Development of Defense Methods for PAC and SCADA systems,
- Anomaly detection-based intrusion detection and threat monitoring system using AI and ML,
- The estimation and prediction of any potential cyber-attack using distributed deep learning method
- Validating and testing defense methods for PAC and SCADA systems against the cyber attacks.


DIGITAL SUBSTATION n & Local PAC System
DIGITAL SUBSTATION 1 & Local PAC System
Trnasducers & Control
Process Bus
Monitoring & Control Devices
Station Bus
NCCTs & Sensors
Switchgear Control
Proteciton IEDs
Monitoring IEDs
Control IEDs
Cyber IDPS Profiles & patterns of network traffics
IRS at Subsation
Substation Mgt.
Asset Conditions
Enabler for rollout of SCADA and wide area PAC systems
Comms Networks Infrastructure
Standardised Information Services
LAN
SCADA, EMS, WAMS + Other central information and control
Cyber IDPS System Information & control
IRS at system level
Standardised Control Services
Information and Control Comms Infrastructure
Enabler for rollout of distributed controls and smart gird applications in IoT

# Digitalisation and Cyber Security

- Background
- Problems and Attack Scenarios
- Challenges
- Cybersecurity Frameworks
- Current Status and Reactive Approach

# Background

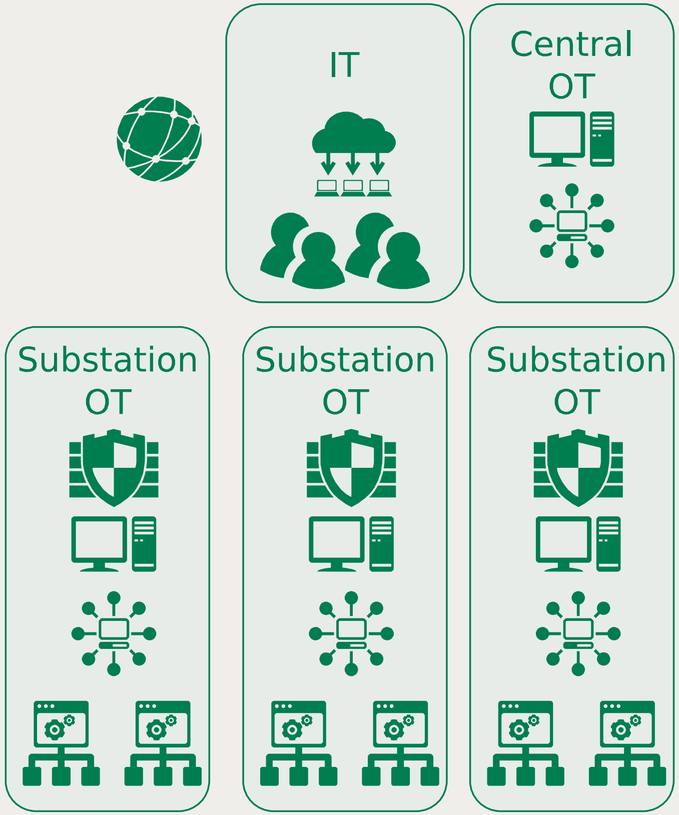
- The cyber - physical components of the energy system are becoming increasingly interconnected as we transition to a net-zero and digital future. As a result, cyber-attacks are becoming a greater threat for the energy system. For examples:
- Ukraine power grid cyberattack took place on 23rd December 2015. It was the first known successful cyberattack on a power grid and resulted in tripping circuit breaker causing power outages for roughly 230,000 consumers in Ukraine for 1-6 hours.
- According to IBM recent security report, the UK became one of the top three most attacked countries in Europe, along with Germany and Italy in 2021. The UK energy system suffered 24% of the overall cyber-attacks which was higher than the manufacturing and financial sectors combined with 19% of all attacks in 2021.
- In January 2023, Pakistan suffered a nationwide power outage for two days. Pakistan energy minister claims that power outages could have been caused by cyberattack,
- WannaCry cyber-attack in 2017 affected 45 NHS organisation and costed the NHS £92m after 19,000 appointments were cancelled
- The impact of wide spread of cybercrime is difficult to quantify but is estimated to cost the UK roughly £27bn per year.

# Problems

- Electricity network serves as the interface between distributed generation, active demand and local flexibility market,
- Digital substations are enablers for the network power flow to be controlled and directed safely and securely from generation to demand,
- These making  digital transformation of power network, in particular, digital substation, a highly attractive target for cyber-attackers aimed at disrupting operations.

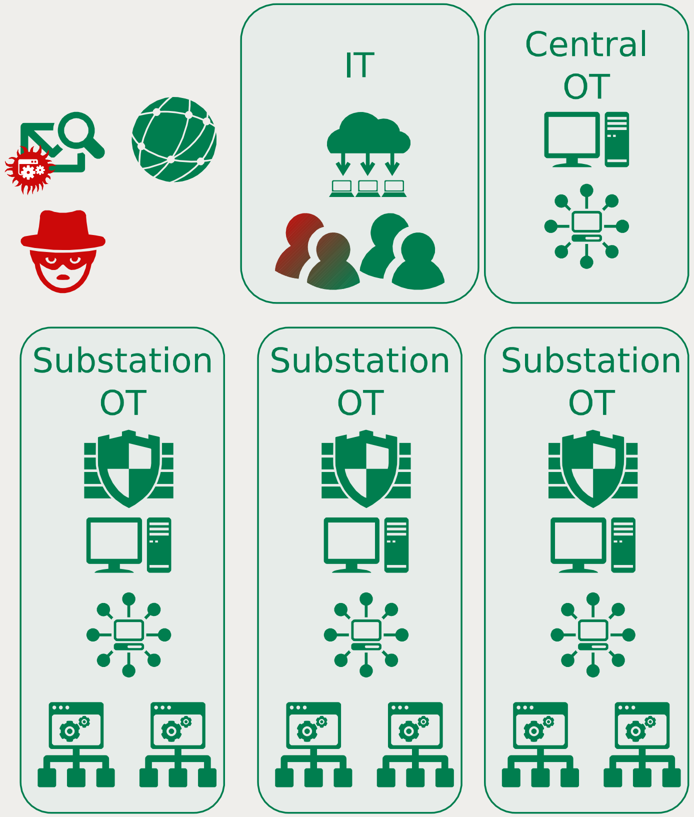
# Attack Scenarios

1. Gain access to IT network;
2. Use access to infiltrate SCADA systems;
3. Search the network for targets;
4. Use connection to controllers to perform the attack;
5. Destroy communication infrastructure to delay recovery.



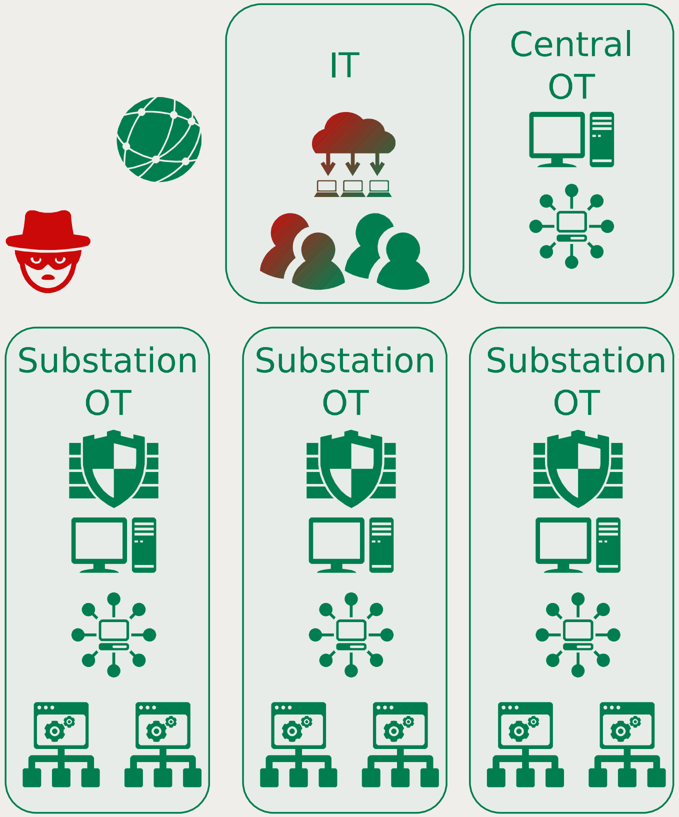
# Attack Scenarios

1. Gain access to IT network;
2. Use access to infiltrate SCADA systems;
3. Search the network for targets;
4. Use connection to controllers to perform the attack;
5. Destroy communication infrastructure to delay recovery.



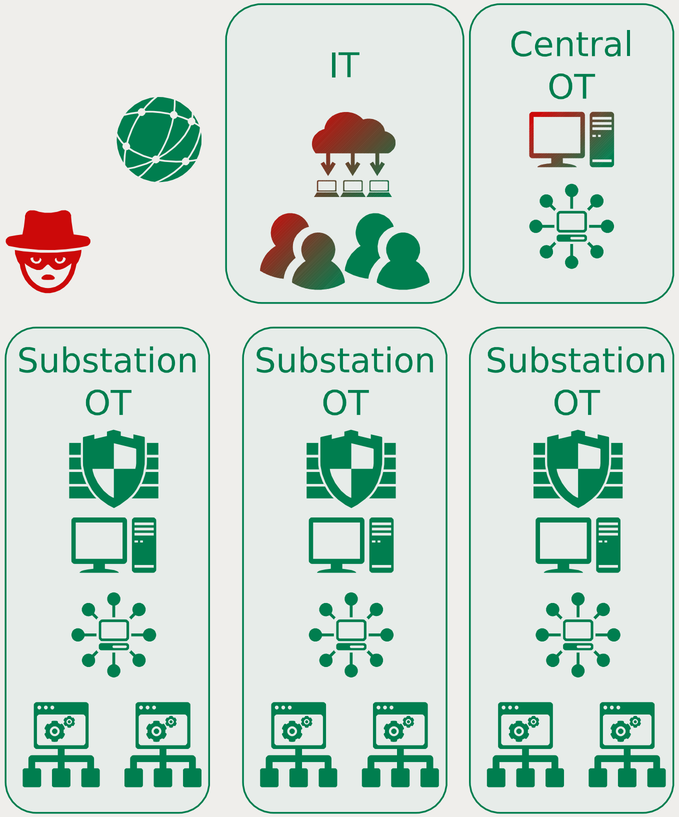
# Attack Scenarios

1. Gain access to IT network;
2. Use access to infiltrate SCADA systems;
3. Search the network for targets;
4. Use connection to controllers to perform the attack;
5. Destroy communication infrastructure to delay recovery.



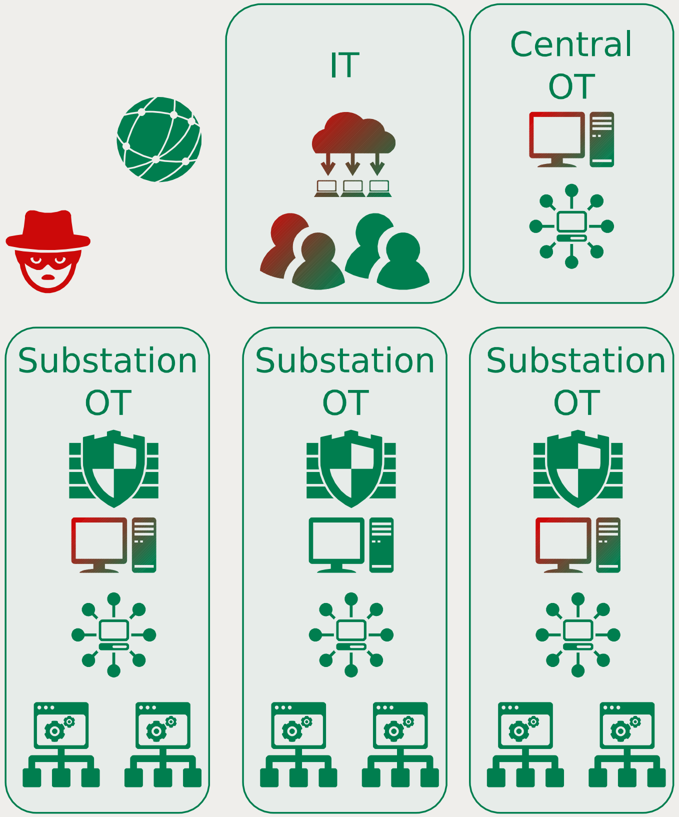
# Attack Scenarios

1. Gain access to IT network;
2. Use access to infiltrate SCADA systems;
3. Search the network for targets;
4. Use connection to controllers to perform the attack;
5. Destroy communication infrastructure to delay recovery.



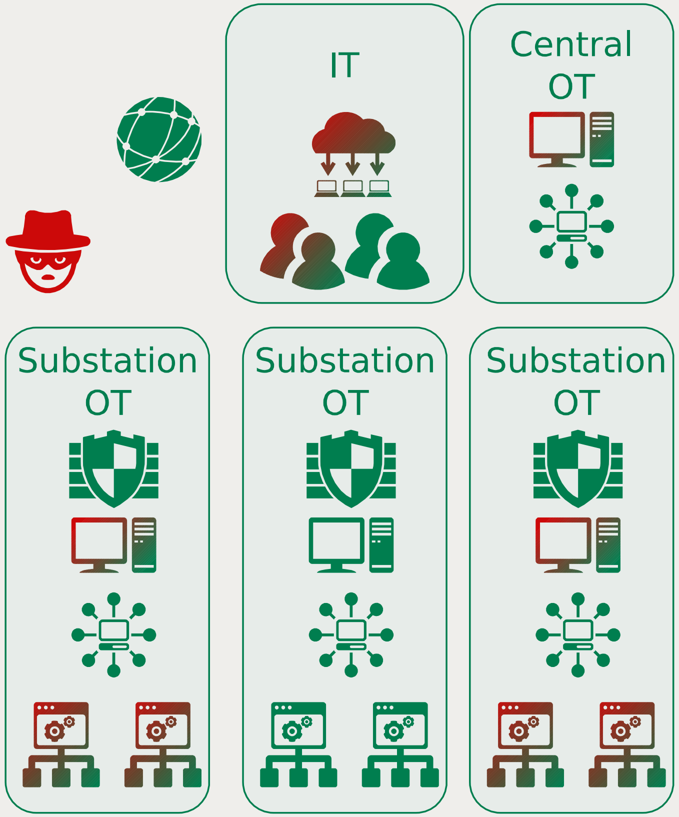
# Attack Scenarios

1. Gain access to IT network;
2. Use access to infiltrate SCADA systems;
3. Search the network for targets;
4. Use connection to controllers to perform the attack;
5. Destroy communication infrastructure to delay recovery.



# Attack Scenarios

1. Gain access to IT network;
2. Use access to infiltrate SCADA systems;
3. Search the network for targets;
4. Use connection to controllers to perform the attack;
5. Destroy communication infrastructure to delay recovery.



# Challenges

- Cybersecurity is the technology arms race in which the cybersecurity teams and the attackers aim to achieve their goals by adapting their behaviour in response to their opponent actions. Leaning from the past, the attackers can launch new attacks while the cybersecurity teams need to develop new countermeasures.
- Cybersecurity measures/protection are costly and yet unable to provide 100% bullet-proofing protection for the system, i.e. it is impossible to eradicate the cyber-attack to the system, especially to future a need of digitised electricity energy systems.
- Unlike extreme weather events that can be forecasted, cyber-attacks are highly random and unpredictable.
- Cyberattack from inside is potentially more severe than attacks from outside as the inside attackers know the most critical equipment in the cyber-physical system.
- Substations becoming software intensive and digitally connected to the grid cyberspace, they are vulnerable to cyber-attacks that may, in the worst case, be used to trip circuit breakers or to prevent IEDs in the substation from working in the case of an actual fault. This requires IEDs not only be able detect faults, but also malicious tripping attacks on circuit breakers or switches. Yet no such capability.

# Cybersecurity Framework

**NIST Cybersecurity Framework (U.S. federal government)**

- The cybersecurity framework established by the National Institute of Standards and Technology (NIST) in 1990 is the most widely used by American companies. Offering detailed guidance on everything from risk assessment and continuous monitoring to incidence response and awareness training.

**ISO 27000 Cybersecurity Framework Series (International Standards)**

- Like the NIST, the ISO is designed to provide a framework for achieving a certified level of data security compliance that meets external assessment standards.

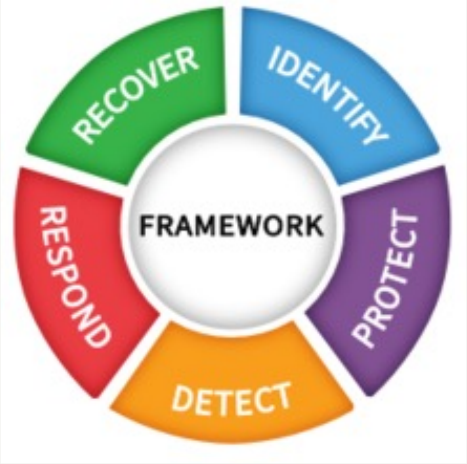
**The Cyber Assessment Framework 3.1 (UK Government)**

- Cyber Assessment Framework (CAF) published by the UK National Cyber Security Centre (NCSC), referencing NIST cybersecurity framework, supports the CAF's core users - organisations within the UK Critical National Infrastructure (CNI), those subject to the Network and Information Systems (NIS) Regulations, and those involved in cyber-related public safety, to help improve their cyber resilience.

[1] https://www.nist.gov/cyberframework, [2] https://www.ncsc.gov.uk/collection/caf

# Cybersecurity Framework

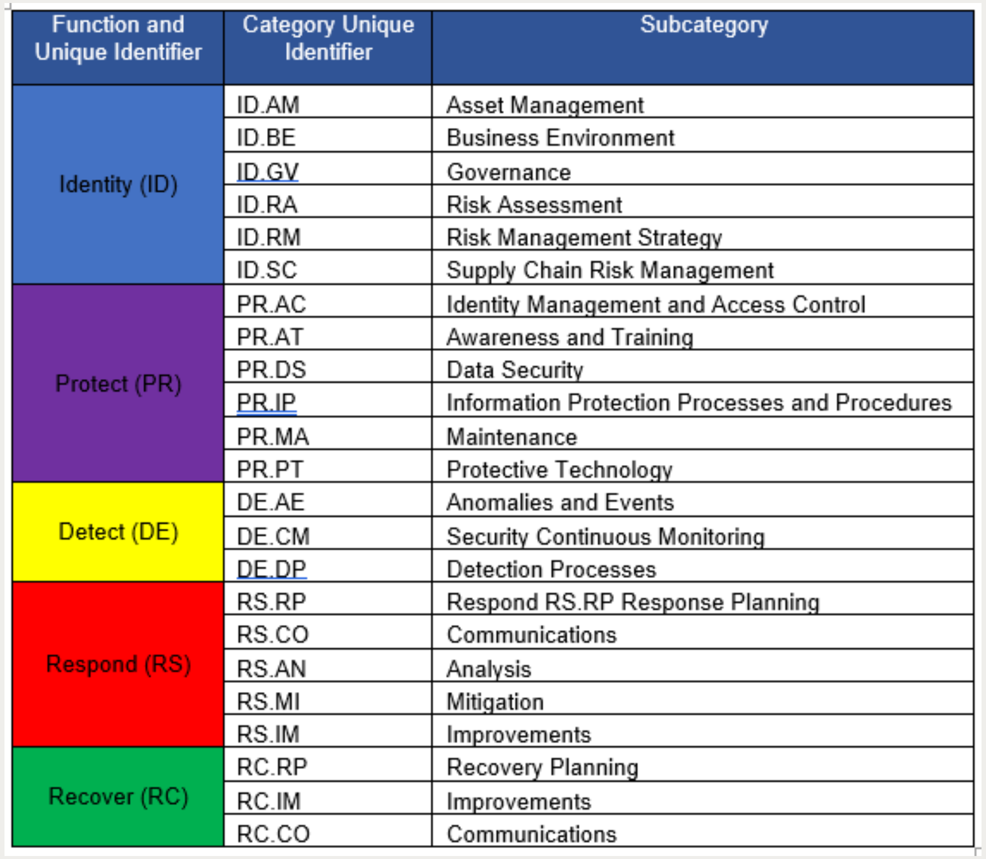
- **NIST Cybersecurity Life Cycle**



- **Identify** - Risk assessment of asset
- **Protect** - Protect assets by implementing policies and IEC cybersecurity standards associated technologies, such as password, firewalls, spam email filtering techniques
- **Detect** - Anomaly intrusion detection with various techniques, such as white or black lists or analysis of data traffic profiles, or combated with ML and AI.
- **Respond** - deploying suitable defence strategies for the countermeasures to mitigate any attack risk to the system,
- **Recover** - Recovery from the comprised systems and learnt lessons

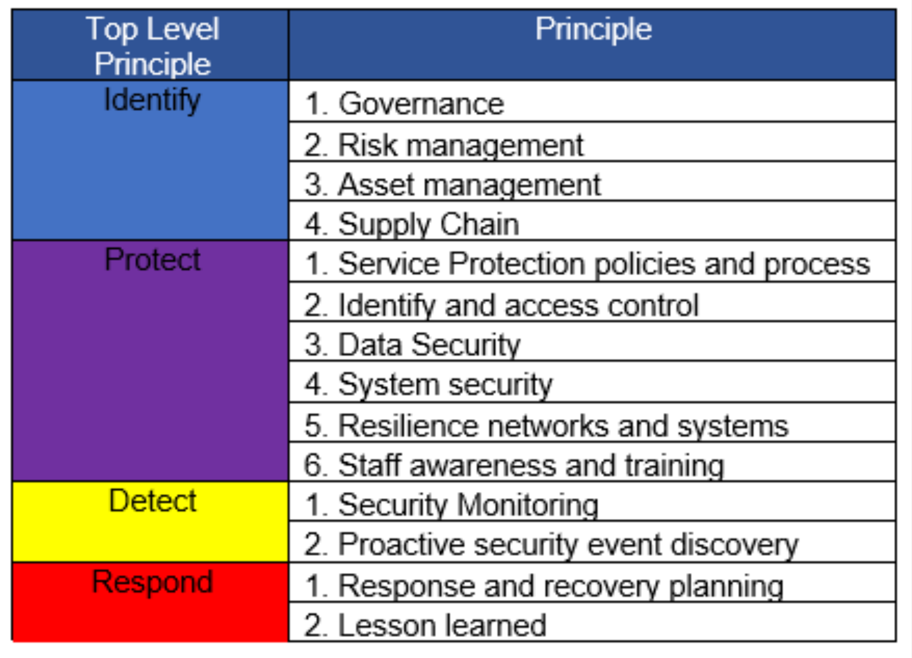
# Cybersecurity Framework

## NIST V1.1 (US Federal Governance)



| Function and Unique Identifier | Category Unique Identifier | Subcategory |
|---|---|---|
| Identity (ID) | ID.AM | Asset Management |
| | ID.BE | Business Environment |
| | ID.GV | Governance |
| | ID.RA | Risk Assessment |
| | ID.RM | Risk Management Strategy |
| | ID.SC | Supply Chain Risk Management |
| Protect (PR) | PR.AC | Identity Management and Access Control |
| | PR.AT | Awareness and Training |
| | PR.DS | Data Security |
| | PR.IP | Information Protection Processes and Procedures |
| | PR.MA | Maintenance |
| | PR.PT | Protective Technology |
| Detect (DE) | DE.AE | Anomalies and Events |
| | DE.CM | Security Continuous Monitoring |
| | DE.DP | Detection Processes |
| Respond (RS) | RS.RP | Respond RS.RP Response Planning |
| | RS.CO | Communications |
| | RS.AN | Analysis |
| | RS.MI | Mitigation |
| | RS.IM | Improvements |
| Recover (RC) | RC.RP | Recovery Planning |
| | RC.IM | Improvements |
| | RC.CO | Communications |

## CAF 3.0 (UK NCSC)



| Top Level Principle | Principle |
|---|---|
| Identify | 1. Governance |
| | 2. Risk management |
| | 3. Asset management |
| | 4. Supply Chain |
| Protect | 1. Service Protection policies and process |
| | 2. Identify and access control |
| | 3. Data Security |
| | 4. System security |
| | 5. Resilience networks and systems |
| | 6. Staff awareness and training |
| Detect | 1. Security Monitoring |
| | 2. Proactive security event discovery |
| Respond | 1. Response and recovery planning |
| | 2. Lesson learned |

# Identify - Risk and Vulnerability Assessments

## Methodologies:

1. **Statistical methods**:  Actuarial risk assessment though statistical sampling, establishing probability distributions, using Bayse's theorey, Regression analysis, etc.

   **Example:** Probabilistic model currently under investigation to establish the likelihood of successful cyber-attack for each threat route.

2. **Modelling Approach**: - Event trees, fault trees, Markov Decision Process (MDP),

   **Example**: MDP under consideration to establish the severity of each attack route. This can be done dynamically

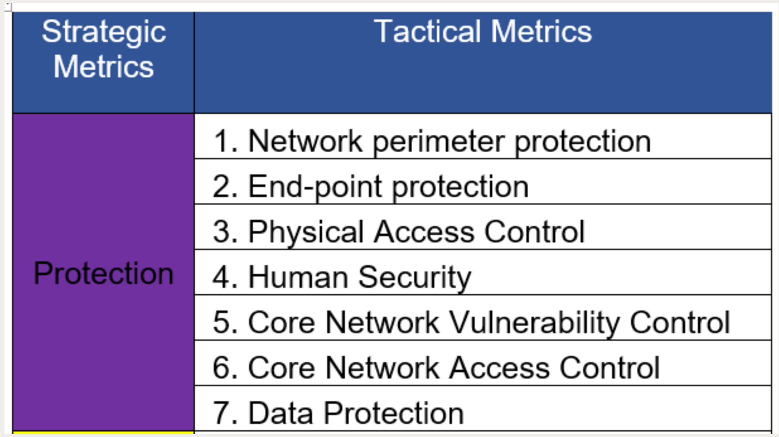
3. **Risk Estimation:**  Risk indexes either individual risk and impact risk under investigation.

4. **Systems Theoretic Process Analysis (STPA)**: A top-down process addressing system components interactions and hazards such as design errors, software, or component interaction failures [4]

# Protect - Cybersecurity Measures

1. EPRI Cybersecurity Metrics

   EPRI cybersecurity matrix uses a quantitative-based framework to assess cybersecurity profile of a target system. In terms of structure, EPRI is quite similar to CAF 3.0 and NIST



| Strategic Metrics | Tactical Metrics |
|---|---|
| Protection | 1. Network perimeter protection |
| | 2. End-point protection |
| | 3. Physical Access Control |
| | 4. Human Security |
| | 5. Core Network Vulnerability Control |
| | 6. Core Network Access Control |
| | 7. Data Protection |

2. IEC 62443: cybersecurity for operational technology (OT) in automation and control systems

3. IEC 62351: for handling the security of TC 57 series of protocols, including;
   - SCADA EC 60870-5 series, IEC 60870-6 series,
   - Digital substation IEC 61850 series,
   - Energy management system IEC 61970 (Transition) series & IEC 61968 (distribution) series.

   The different security objectives include authentication of data transfer through digital signatures.

# Protect - Cybersecurity Measures

**Zones and conduits:**

Zones - Groups of assets;
Conduits - groups of communications;

**Physical security:**

Separation of networks;

Access enforcement (e.g. doors, padlocks, keys)

**Access control:**

Mechanical access

Network role-based access, password, etc

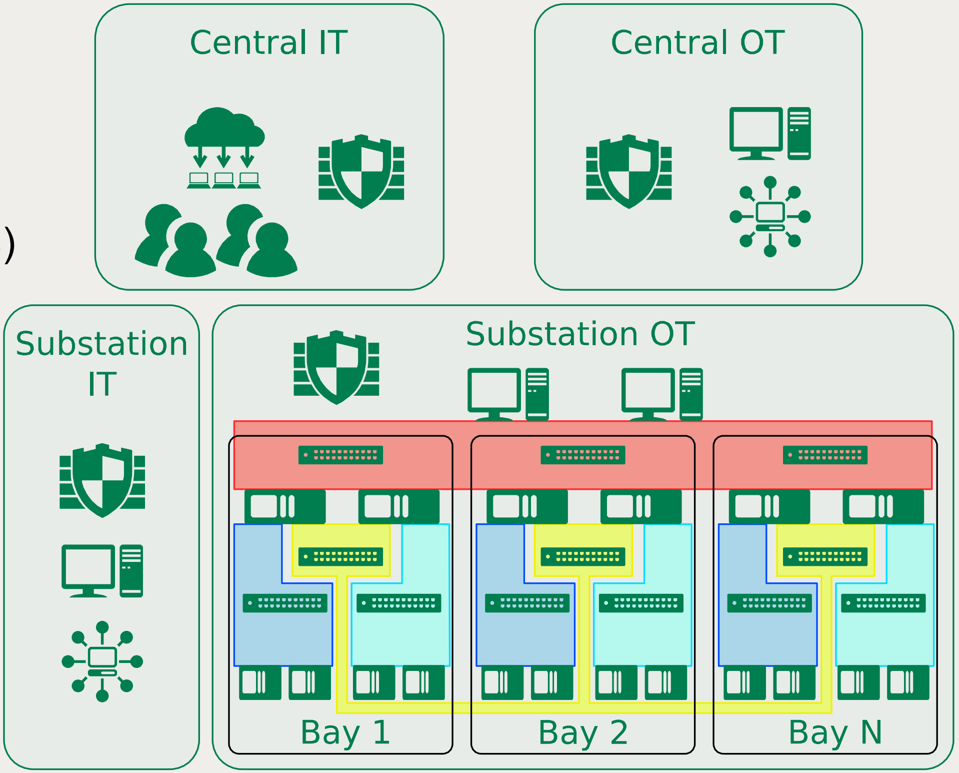
**Network architecture:**

Firewalls;

Software Defined Networks (SDN) [5]

IEC 62443

IEC 62351-10 Security arctecture



[5] H. Li, L. Chan, Z. Wu, D. Texidor Dantas, T. Charton, R. Zhang, "Assessment of Dynamic and Programmable Network Redundancy Management Method based on Software Defined Network Technology in a Fully Digital Substation", CIGRE Paris Session 2020

# Detect - Intrusion Detection System (IDS)

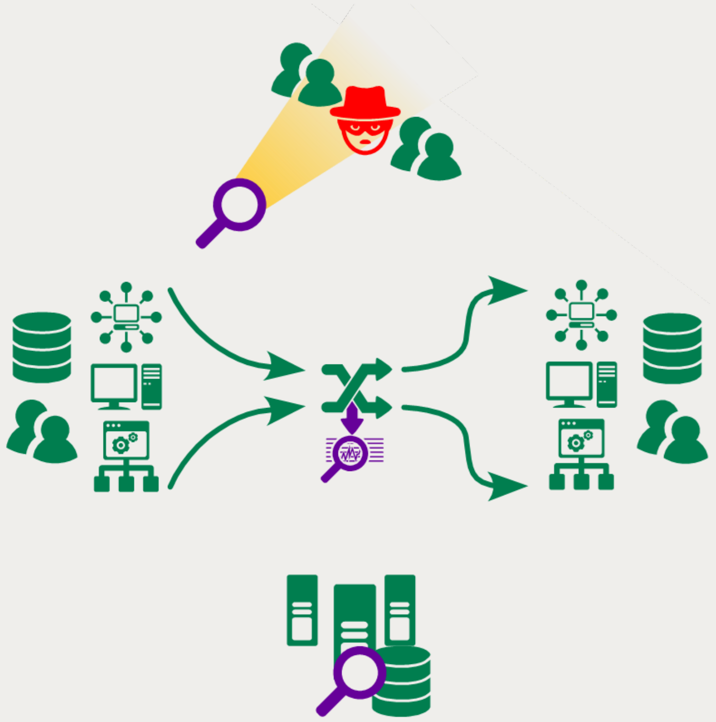
Physical alarm systems, guards and etc.

Cyber space based IDS:

- Anomaly-based (Whitelisting)
  - SCL file reading;
  - Database constructing;
- Signature-based (Blacklisting)
  - Known threats;
  - Neural network;

Endpoint IDS (anti-virus) ;

IEC 62351-7 and NIS



# Detect - Network-based IDS

## Anomaly-based (Whitelisting)

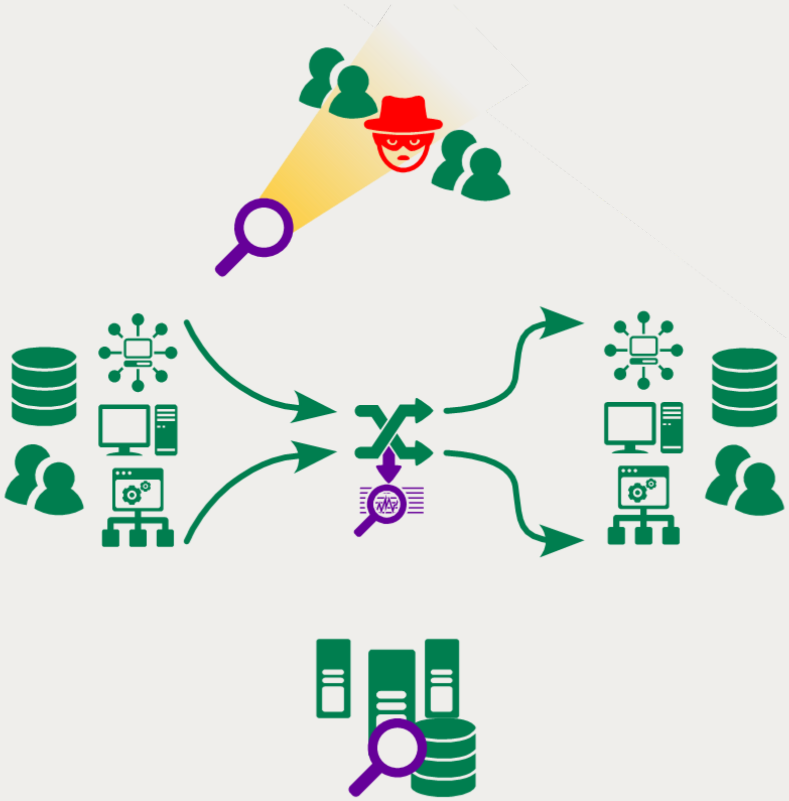
- Project-based configurations;
- SCL file reading;
- SDN flow exceptions;
- Database constructing;

## Signature-based (Blacklisting)

- Known threats;
- Known threats database upgrade architecture;
- Neural network;

## Machine Learning and AI

- Can identify both white Listing and Backlisting
- Traffic pattern identification



# Current Cyber Security Focuses

- **Cyber Security Measure/Protection Methods**

  **Intrusion prevention** - implementation of company policies and cyber security standards, such as IEC 62351 or 62443 associated technologies. The complicity of cyber security prevention is largely dependent on cyber risk assessment outcomes. Risk assessment is based on cybersecurity framework, such as Cyber Assessment Framework (CAF) 3.0 by the National Cyber Security Centre (NCSC) of United Kingdom or NIST risk framework or EPRI cyber assessment metrics in USA. Currently often used risk assessment methods are (i) probability based event tree, (ii) Systems Theoretic Process Analysis (STPA) and (iii) Markov decision process, etc.

- **Intrusion Detection Systems**

  **Intrusion detection Systems (IDS) -** a device deployed with the objective of identifying malicious activities performed by a possible intruder in a network. Those devices can work using different strategies and be categorized accordingly, such as simple whitelist or black lists or analysis of data traffic profiles, or artificial intelligent (AI) and Machine Learning (ML) technologies to identify known or unknown threats.

  **IDSs** can be divided into active (inquiring devices to check responses) and passive (not injecting any network traffic) and between signature-based (looking for known threats) or anomaly-based (detecting unusual behaviour)

# IDS Tested some IDS systems in Manchester

- **White List**:

  Presented a very direct Whitelisting approach for deploying Intrusion detection systems in substation. Substation Configuration Language (SCL) files are used to identify devices and protocols in the substations. Devices are not described in SCL file can be added using a role strategy which combines pertinent activities to devices in order to simplify configurations (e.g. describe a computer as HMI enable multiple protocols).

- **Hardware IDS**

  Anomaly-based hardware IDS which provides four functions: 1) threat detection, 2) risk and vulnerability, 3) visibility of assets, and 4) asset inventory. It uses AI through data traffic analysis to identify all potential vulnerabilities and corresponding risks in a network and then to determine the likeliest paths through which an attacker could compromise it.

- **Endpoint Cybersecurity Software**

  Anomaly-based IDS. It is an anti-malware system powered strictly by artificial intelligence, which runs on Windows, MacOS and Linux machines. It uses advanced algorithms and cognitive analytics to reveal threats for enterprises such as power plant and wind farm. Its natural language processing is capable of classifying cyber events as malicious or benign.

# Respond and Recovery Strategy

NIS directive;

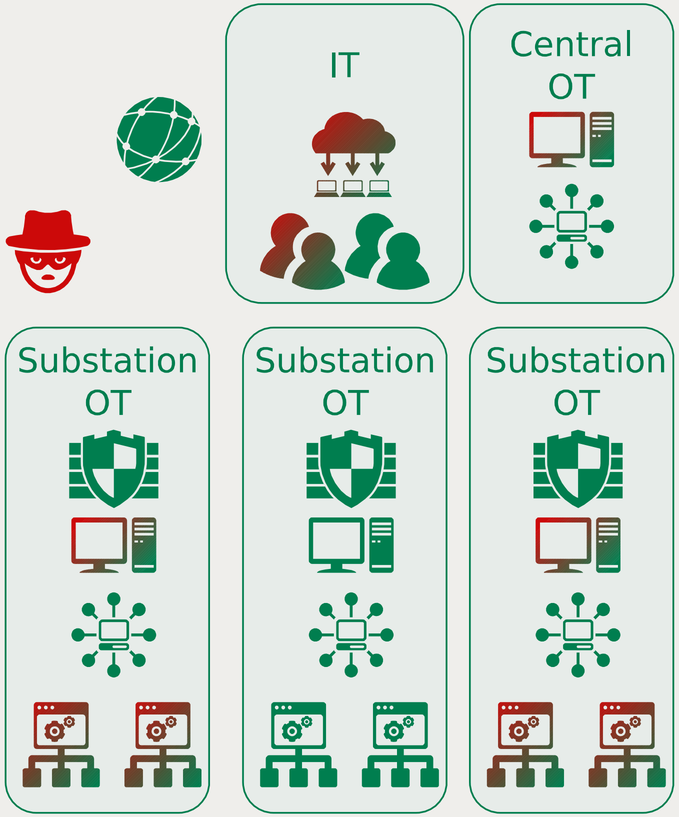
IEC 62351-10;

IEC 62443-2;

IEC 62443-3.

Documentation;

System backups.



# Respond and Recovery Strategy

NIS directive;

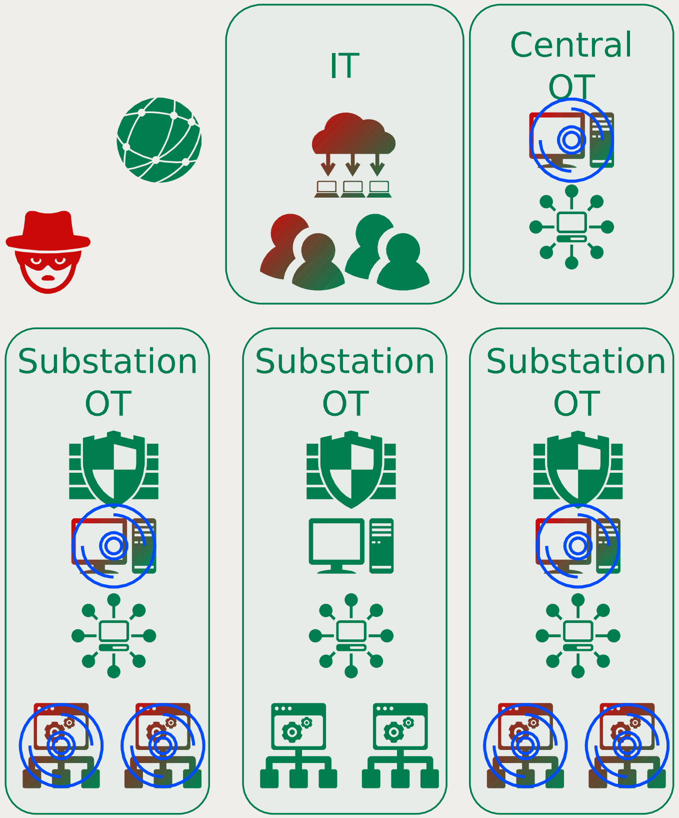
IEC 62351-10;

IEC 62443-2;

IEC 62443-3.

Documentation;

System backups.



# Respond and Recovery Strategy

NIS directive;

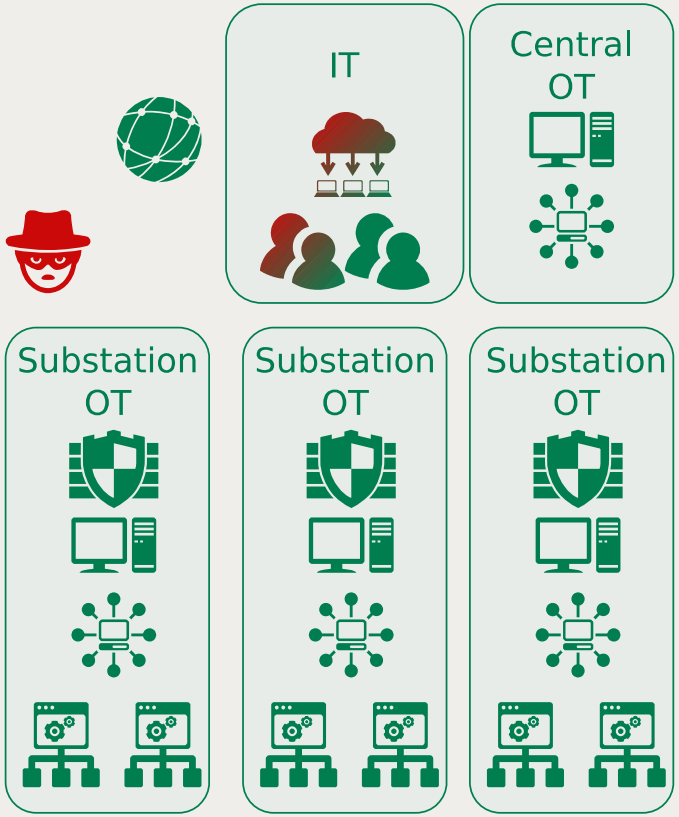
IEC 62351-10;

IEC 62443-2;

IEC 62443-3.

Documentation;

System backups.



# Research Gaps and Need Defense to Respond

- **Importance of cyber systems in electricity network**: The cyber systems, including PAC system, SCADA and WAMS are critical systems as they are used to automate power system operations and protect the electricity network infrastructure against anomaly and faults. They must provide contingencies control action for rare events and must prevent any mal-operation against the cyber-attacks.
- **Real time technical challenges:** Typical control action time for PAC system is less than 100ms, for WAMS is within a few seconds and for SCADA system is from tenth seconds to a few minutes. These systems must response malicious instruction quickly and prevent power system false operation or false circuit breaker tripping against any malicious control actions.
- **Cyber security and defense challenges:** Up to date there are no evidence to show that the existing cyber security technologies or tools could be able to provide sufficient bullet-proofing cyber intrusion prevention and defense against advanced cyber threats for power system PAC and SCADA systems.

# Current Defense Methods and Strategies

## SCADA Systems relevant to DoS and FDI

- Moving Target Defense, such as SDN
- Data-Driven Approaches based on ML and AI
- Temporally-Relevant Defense with data correction capability. e.g. State Estimation

## Digital Substations relevant to PAC devices

- Collaborative Defense of Transmission and Distribution Protection and Control devices against cyber-attacks (CODEF)
- Improving the Cyber Resiliency and Security Posture of Public Power
- Cyber attack resilient distance protection and circuit breaker control for digital substation

# Current Defense Methods and Strategies

## SCADA Systems relevant to DoS and FDI

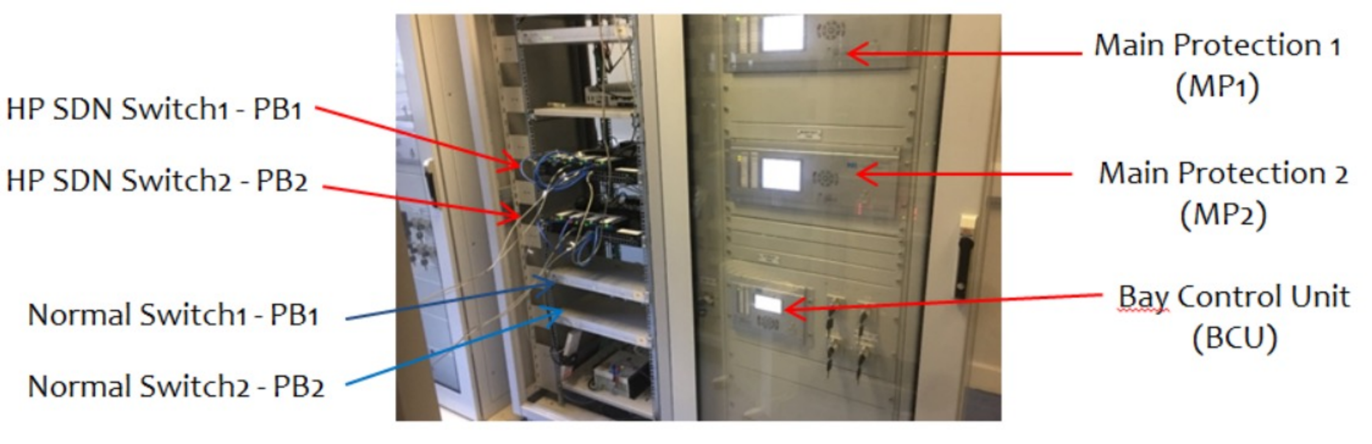
- Moving Target Defense and centralised comms network management, e.g. SDN
- Data-Driven Approaches based on ML and AI
- Temporally-Relevant Defense with data correction capability. e.g. State Estimation

## Digital Substations relevant to PAC devices

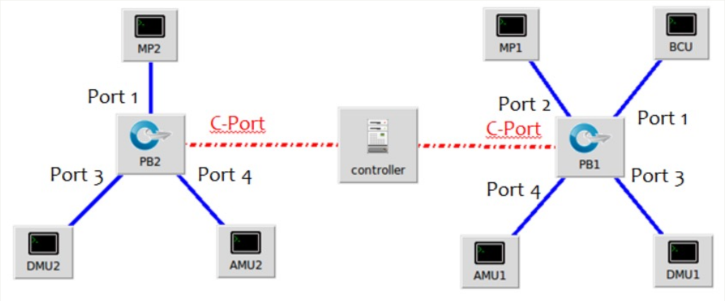
- Collaborative Defense of Transmission and Distribution Protection and Control devices against cyber-attacks (CODEF) [10]
- Improving the Cyber Resiliency and Security Posture of Public Power [11]
- Cyber attack resilient distance protection and circuit breaker control for digital substation [12]

# Example 1  VASTT Platform with SDN

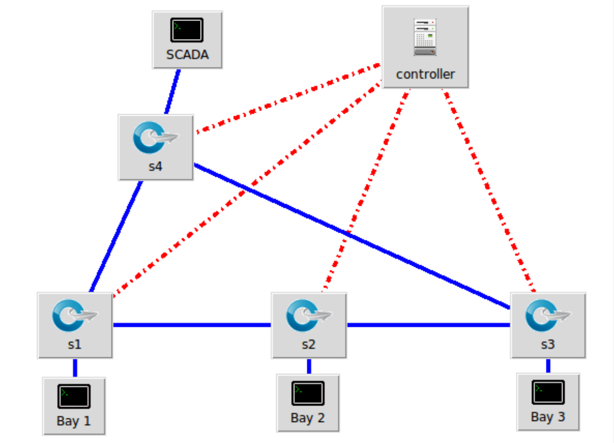
### Lab setup of the SDN switches



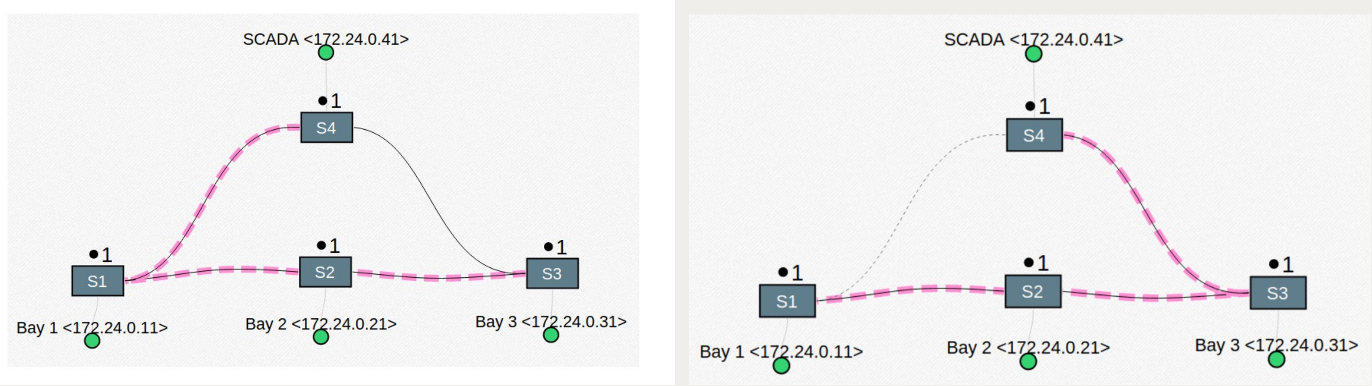
### Implementation of SDN at the process level



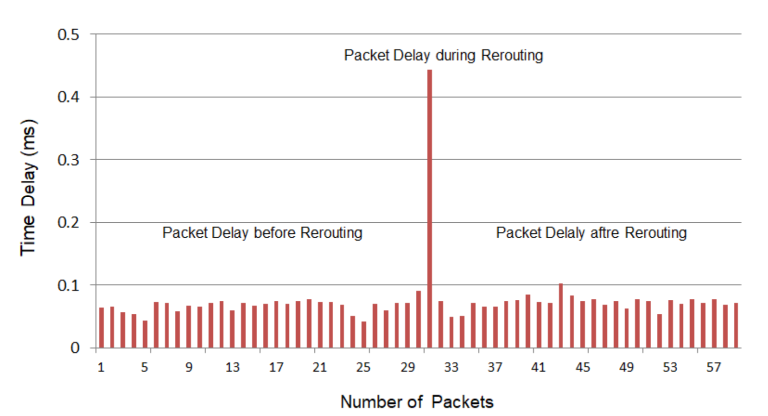
# Example 1  Improved cyber security with SDN



Implementation of SDN at station bus level using Mininet and openflow

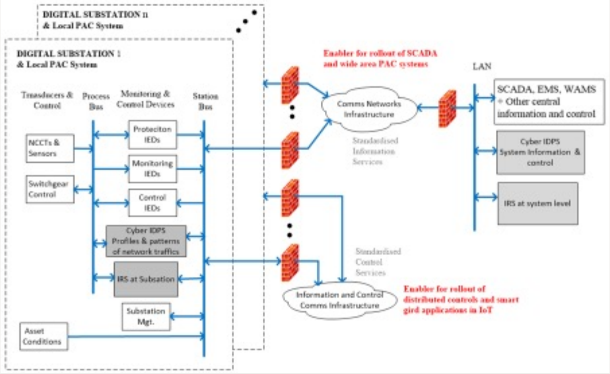


SDN based station bus re-routing transition states in Minitnet



# Example 2 - Cyber-Safen Project

- **Aim**: Cyber Safen is to build distributed cyber safe and resilient functions layer PAC devices or WAMS and SCADA systems against advanced cyber-attacks
- **Scopes**:
  - Advanced data analysis and modelling for identification of normal and abnormal power system operation conditions as well as the new emergent security threats based on activity patterns in the large volumes of data, i.e. big data that is being collected from simulated PAC and SCADA systems,
  - Anomaly detection-based intrusion detection and threat monitoring system using AI and ML,
  - The estimation and prediction of any potential cyber-attack using distributed deep learning method,
  - Development of defense methods and trategies for multi-OT devices to build resilience for PAC and SCADA systems against the cyber infected substations.


DIGITAL SUBSTATION n
& Local PAC System
DIGITAL SUBSTATION 1
& Local PAC System
Transducers & Control
Process Bus
Monitoring & Control Devices
Station Bus
NCCTs & Sensors
Switchgear Control
Protecitori IEDs
Monitoring IEDs
Control IEDs
Cyber IDPS Profiles & patterns of network traffics
IRS at Subsation
Substation Mgt.
Asset Conditions
Enabler for rollout of SCADA and wide area PAC systems
Comms Networks Infrastructure
Standardised Information Services
LAN
SCADA, EMS, WAMS + Other central information and control
Cyber IDPS System Information & control
IRS at system level
Standardised Control Services
Information and Control Comms Infrastructure
Enabler for rollout of distributed controls and smart gird applications in IoT

Any Question?

Haiyu.li@manchester.ac.uk

cigre

For power system expertise