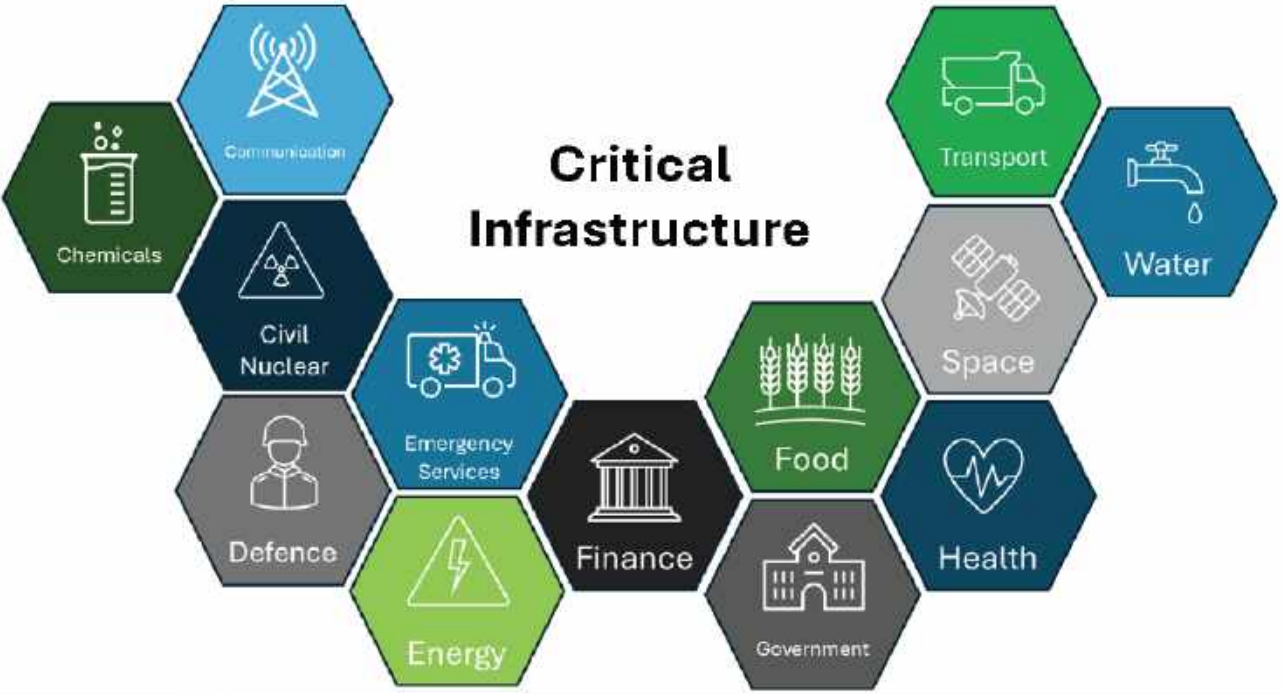
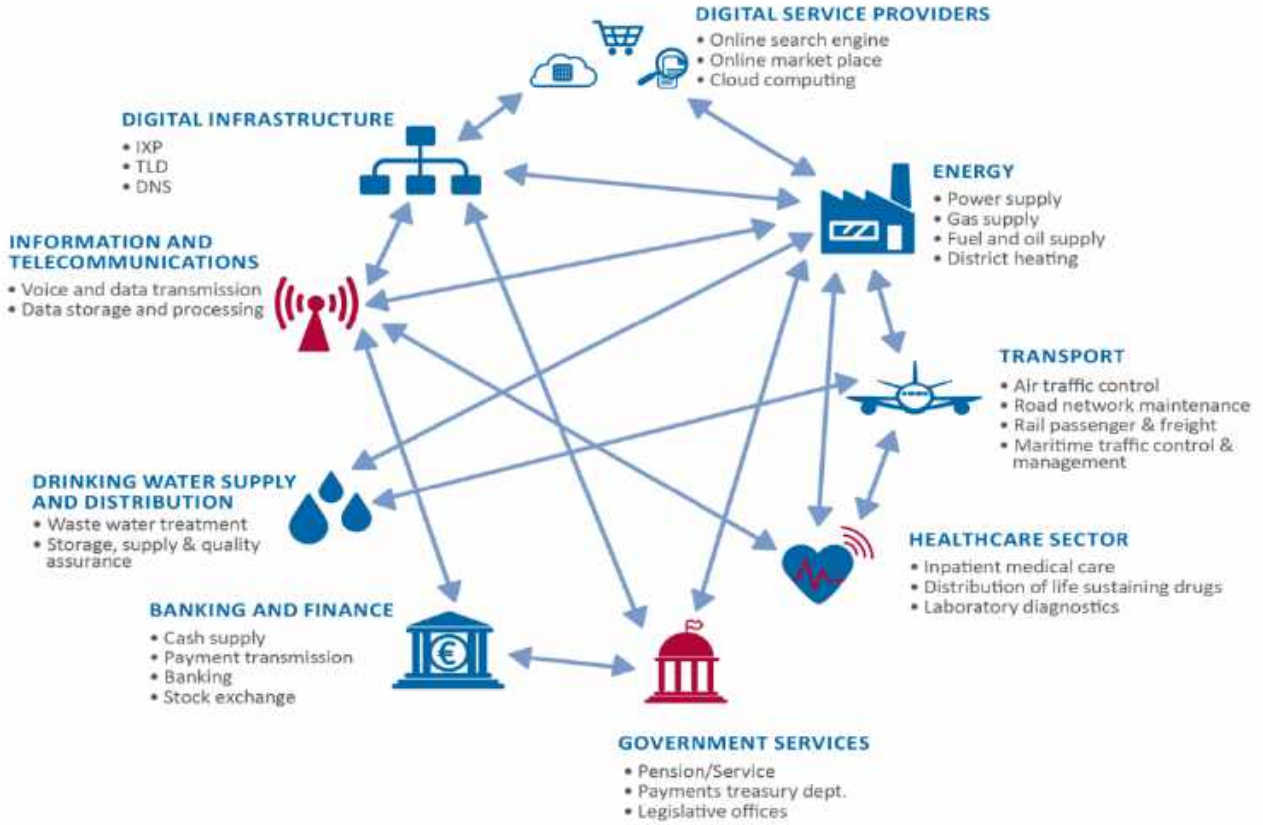
Hyb Arloesedd Seiber
Cyber Innovation Hub

Advancing OT Knowledge Practical Hands-on: An effort by Cyber Innovation Hub (Cardiff University)

Empower individuals and organizations to protect what matters (Critical National Infrastructure)

Critical National Infrastructure Sectors and Interdependencies





Attacks on OT and IT

Year	Campaign	Enterprise/ICS
2000	Maroochy Water Breach	ICS
2010	Iran Nuclear Program	Both
2015	Ukraine Electric Power Attack	Both
2016	Ukraine Electric Power Attack	Both
2017	Saudi Arabia Triton SIS Attack	ICS
2019	Energy, Healthcare, Manufacturing	Both
2022	Ukraine Electric Power Attack	Both
2023	Unitronics Defacement	ICS

OT
Attacks

Year	Institution	Type of Cyber Attack
2015	Carphone Warehouse	Data Breach
2016	National Lottery	Credential Stuffing
2017	WannaCry	Ransomware Attack
2018	British Airways	Data Breach
2018	NotPetya	Ransomware Attack
2019	UK Labour Party	DDoS Attack
2020	Hackney Council	Ransomware Attack
2020	Redcar and Cleveland Council	Ransomware Attack
2021	Gloucester City Council	Phishing/ Ransomware Attack
2022	Electoral Commission Data Breach	Data Breach (Zero-Day Vulnerability)
2023	Greater Manchester Police	Data Breach
2023	British Library	Ransomware Attack
2024	Synnovis	Ransomware Attack
2024	Alder Hay NHS Children's Foundation Trust	Ransomware
2024	Southern Water Supply	Ransomware
2024	Greater Manchester Council Attack	Phishing

IT
Attacks

Vision

- An environment to experience the effects of kinetic cyber physical attacks
- UK Cyber Lab environment hosting testbeds (self-contained, portable, trolleys) for all critical national infrastructure (approx. 14 trolleys)
    - Study red team capabilities, techniques, artifacts, and impacts within specific network configurations
    - Enabling blue teams to hone defensive skills and develop new processes for detecting malicious cyber activity
    - Validate and understand the impact of vulnerabilities within ICS hardware and configurations
- Utilize the above infrastructure to train UK Cyber security workforce
- Explore AI to secure Operational Technology world

OT environments

1. VOT: Open-source environments

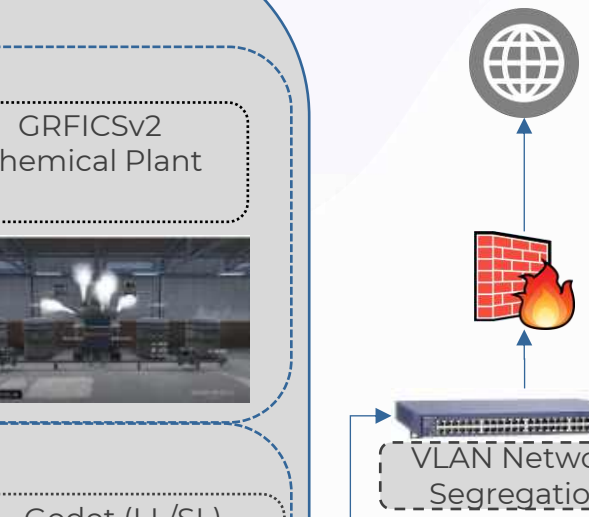
- VirtuaPlant (Bottle filling plant)
- MetroRail Emulator (Simulate rail running with intersections)
- GRFICSv2 Chemical Plant

2. VOT: Digital Twins

- FactoryIO
  a. Airport Baggage Handling System
  b. Storage Tank – Water Bottle Filling System
- AnyLogic
  a. Cardiff Airport
  b. Cardiff Central Station
  c. Cardiff Port
- Unity/RealEngine
  a. Tennessee Eastman Process
  b. Steel/Cement making
  c. Building Digital Twin
- Godot (LL/SL)
  a. Circular Table Saw
  b. Electrical Road Barrier
  c. Reactor Emergency System
  d. Temporary Traffic Lights

3. Physical OT small-scale environments (Trolley-based or not)

- Electrical Grid (Transmission and Distribution)
- Electrical Vehicle Charging Station
- Railways
- Oil & Gas
- Smart Home/Building Management
- Manufacturing



VLAN Network Segregation

OT environments

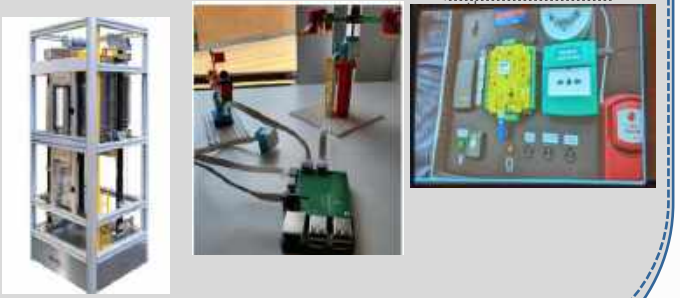
4. 3D Demonstrator Tiles

- Renewable Energy
- Hospital
- Oil & Gas

5. Portable Testbeds (Briefcase/Table-based or not)

- Conveyor Belt
  LJCreate Industrial Control Work-Cell
- SCADA
  LJCreate Petra II Advanced Industrial Control
- Smart Building
  ETS Kit with KNX Programmable Board, Heater, Dimming, Blinds

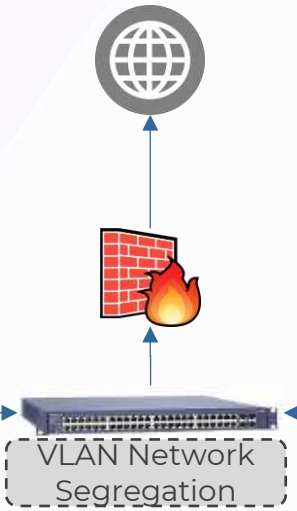
- Elevator System
  Two lifts with multiple floors
- Cyber Fun Fare
  Lego parts representing FunFare for Kids
- Access Control
  Fire-alarms, door controls and



Cyber Escape Rooms

6a. Virtual Escape Rooms?
- Vivda Cyber

6b. Physical Escape Rooms?
- Different Themes (Password Security, Network Discovery, Internal Threats)



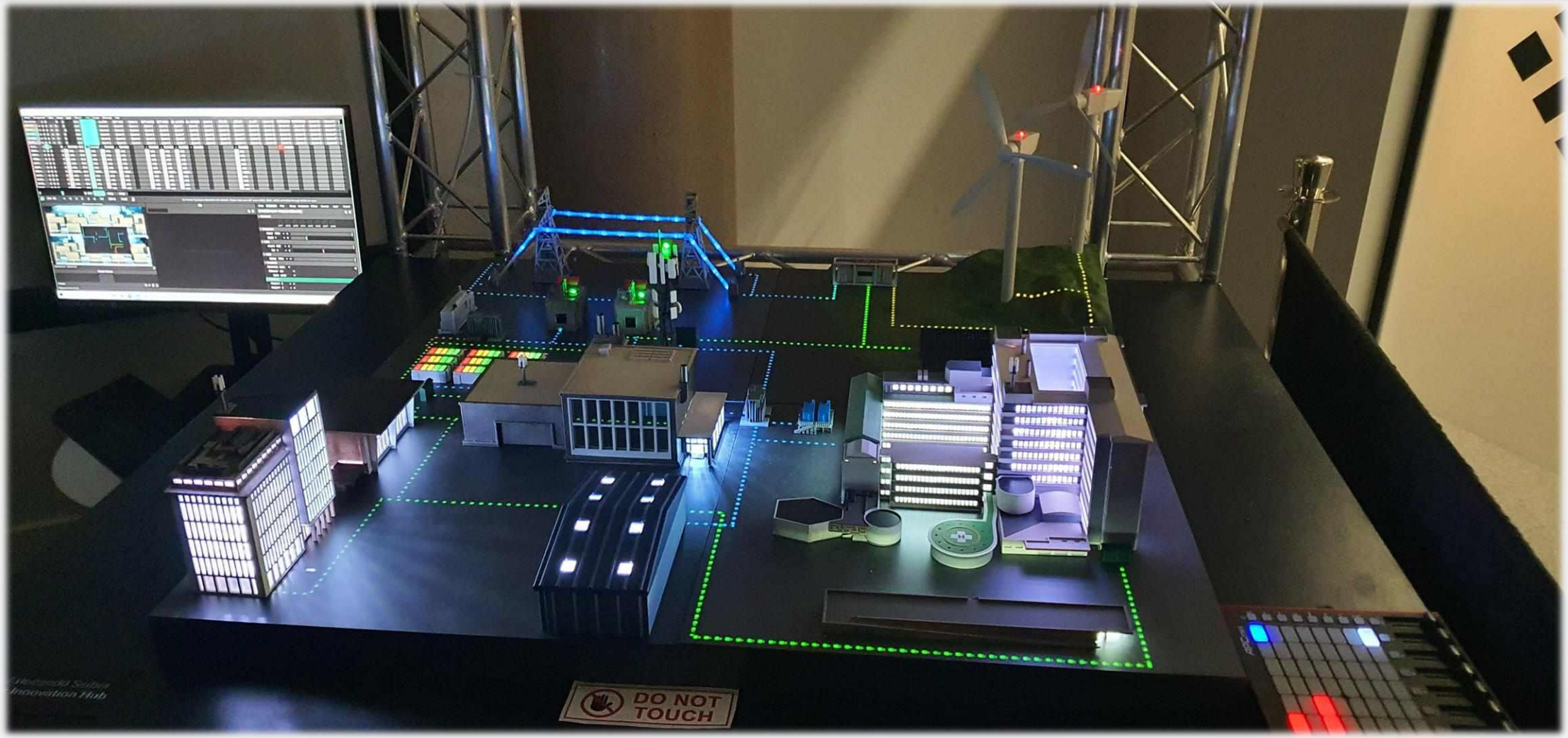
VLAN Network Segregation

Red/Blue Team Environment

7a. Work with MoD to design something similar like NATO Cyber Defence Exercises

- Working with Tarian Regional Cyber and Economic Crime Units (ROCU) (police officers and police staff seconded from the three forces of South Wales, Gwent and Dyfed-Powys.)
- Plans to utilize Hydra Simulation Facility across the UK for scalability.

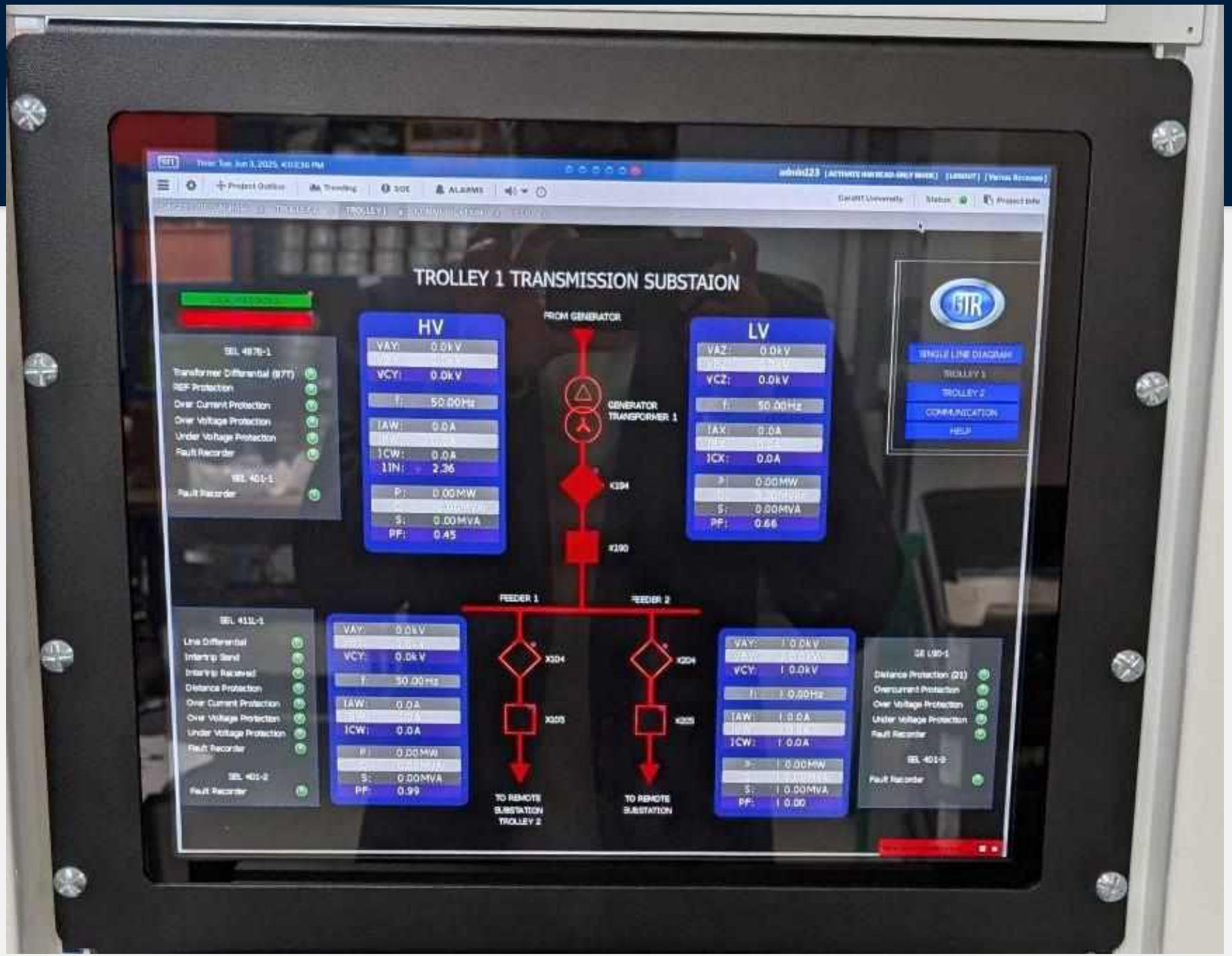
Demonstrator Table



Helps see cascading effects on Critical National Infrastructure

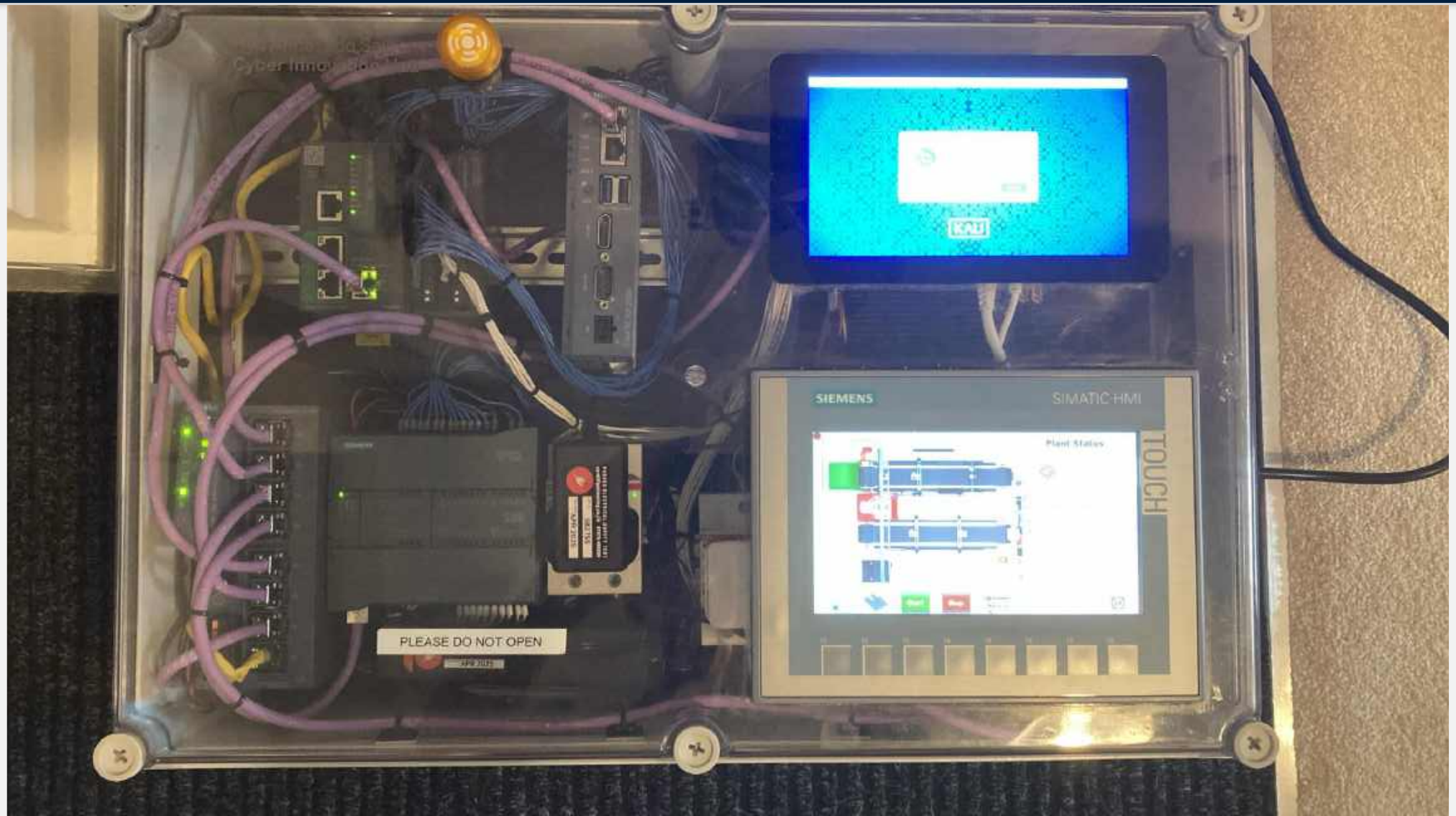
Electrical Grid (Transmission and Distribution)


DISCONNECTOR
CIRCUIT BREAKER
DISCONNECTOR
CIRCUIT BREAKER
DISTRIBUTION CONTROL


TROLLEY 1 TRANSMISSION SUBSTAION
HV
LV
FROM GENERATOR
GENERATOR TRANSFORMER 1
FEEDER 1
FEEDER 2
TO REMOTE SUBSTATION TROLLEY 2
TO REMOTE SUBSTATION
SINGLE LINE DIAGRAM
TROLLEY 1
TROLLEY 2
COMMUNICATION
HELP

PursueCyber Box

Fieldsite-in-a-Box



Smart Motorway

- Project with UK National highways
- Show realistic scenarios
  - Gantry Hacking
  - Car failures
  - Camera failures
- From the ROC (Regional Operations Centres) point of view