MANCHESTER 1824

The University of Manchester

nationalgrid

SP ENERGY NETWORKS

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

Digitalisation and Data Science Conference – Enabler for Net Zero

cigre

For power system expertise

Speaker: Dr. Sugandh Khanna on behalf of
Dr. Haiyu Li from University of Manchester

OUTLINE

1. Completed Digitisation Projects at Manchester
2. Background and Problems
3. Current Cyber Security Focuses
4. Research Gaps and Needs
5. Cyber-Safen Solution
   - Aims and Scopes
   - Novelty of Cyber-Safen
   - Methodology
   - Dual Defence Systems - IDS and IRS
6. Conclusions

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

.

BACKGROUND

- UK government's new legally-binding target to cut greenhouse gas emissions by 78% (to 1990 levels) by 2035 and net zero by 2050.
- To address the net zero challenges, the main drives for innovation in RIIO Tier 2 submission are:(i) Decarbonization, (ii) Decentralization and, (iii)**Digitisation**
- Power system digitization and automation play a key role and provide essential functions to keep the increasingly decarbonized and decentralized energy system running in a reliable, sustainable, and cost-effective manner.
- The digital transformation of the power network, in particular, digital substation, become a highly attractive target for cyber-attackers aimed at disrupting operations.
- Notable incidents include the Ukraine power grid attack, which disrupted power for 230,000 consumers, the 2017 WannaCry cyberattack that impacted 45 NHS organizations, costing £92 million and leading to 19,000 canceled appointments, and Pakistan's two-day nationwide blackout in January 2023, suspected to be a cyberattack, among several others.

PROBLEMS / CHALLENGES

- **Importance of electricity network**: The electricity network PAC, SCADA and WAMS are critical systems as they must provide a contingency control for rare events and must protect the electricity network infrastructure against any types of faults and must prevent any mal-operation against the cyber-attacks.
- **Real-time technical challenges**: Typical control action time for PAC system is less than 100 ms, for WAMS within a few seconds and for SCADA from tenth seconds to a few minutes. These systems must response to malicious attack quickly and prevent false operation or false circuit breaker tripping against any malicious control actions.
- **Cyber Security Challenges -** cyber security is the technology arms race in which the system designers and the attackers aim to achieve their goals by adapting their behaviour in response to their opponent actions
- **Cyber response (or defence) challenges:** Up to date there is no evidence that any existing cyber security technologies or tools could be able to provide sufficient bullet-proofing cyber intrusion detection and defences against advanced cyber threats for power system PAC and SCADA systems.

CYBER SECURITY LIFECYCLE AND FOCUSES

- Cyber security life cycle - 4 stages
- **Intrusion prevention** - Implementing company policies and cybersecurity standards, such as IEC 62351 and 62443, relies on effective risk assessments. These assessments, guided by frameworks like CAF 3.0 (NCSC, UK), NIST, or EPRI metrics (USA), determine the complexity and scope of preventive measures.
- **Intrusion detection** – Intrusion Detection Systems (IDS) identify malicious activities in a network using strategies like whitelists, blacklists, traffic analysis, and AI/ML technologies to detect both known and emerging threats.
- **Intrusion response** - Intrusion Response involves deploying effective defense strategies to mitigate attack risks and protect systems. However, most existing response mechanisms are reactive, responding to threats after they occur, rather than proactively preventing potential attacks.
- **Learnt lessons or Recovery** - helping the system designers to continuously develop corrective measures against the cyber threats or strategy and plan to recovery any disrupted system quickly.

RESEARCH GAPS AND NEEDS

- Cyberattacks are an unavoidable reality, with potentially devastating consequences for power system operations, protection, and control. For example, a malicious actor could launch an attack to alter Intelligent Electronic Device (IED) settings or manipulate Generic Object-Oriented Substation Event (GOOSE) signals. Such actions could lead to widespread false tripping of circuit breakers, causing blackouts and severe disruption.

- Research conducted at Manchester demonstrates the alarming ease with which a self-learned GOOSE device, implemented on a low-cost platform like Raspberry Pi and equipped with malware, could shut down an entire digital substation. This highlights the system's vulnerability to targeted attacks.

- Given the rapid response times required in power systems—where Protection and Control (PAC) systems must act in milliseconds to seconds—an Intrusion Response/Defence System (IRS) along with IDS is essential. Such a system must provide instantaneous detection and mitigation capabilities to counter false tripping and ensure the stability and resilience of power system operations. Without this level of real-time defense, the cascading effects of even a single compromised node could have catastrophic consequences.

CYBER-SAFEN

- Cyber-SAFEN aims to build and demonstrate an Integrated Cyber Defence (ICD) platform to provide a foundation on which to build essential cyber safe and resilient functions for electricity network PAC, WAMS and SCADA systems to protect against advanced cyber-attacks. Cyber-SAFEN uniquely focuses on a combined Intrusion Detection System (IDS) and Intrusion Response System (IRS) powered by advanced AI and machine learning technologies to build a dual defence system against advanced cyber threats.
- **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.
  - AI or cooperative control of distributed multi-devices strategy to build resilience for PAC system against the cyber infected substations.

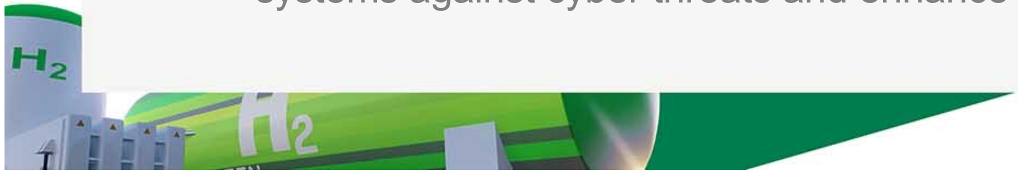
CYBER-SAFEN –FOCUS(NOVELTY)

Intrusion Response (or Defense) System (IRS)

There has been limited research on the IRS. CyberSAFEN seeks to explore and implement effective defense strategies to mitigate the risks posed by cyberattacks targeting PAC systems in substations and SCADA systems in control centers. Key areas of research include, but are not limited to:

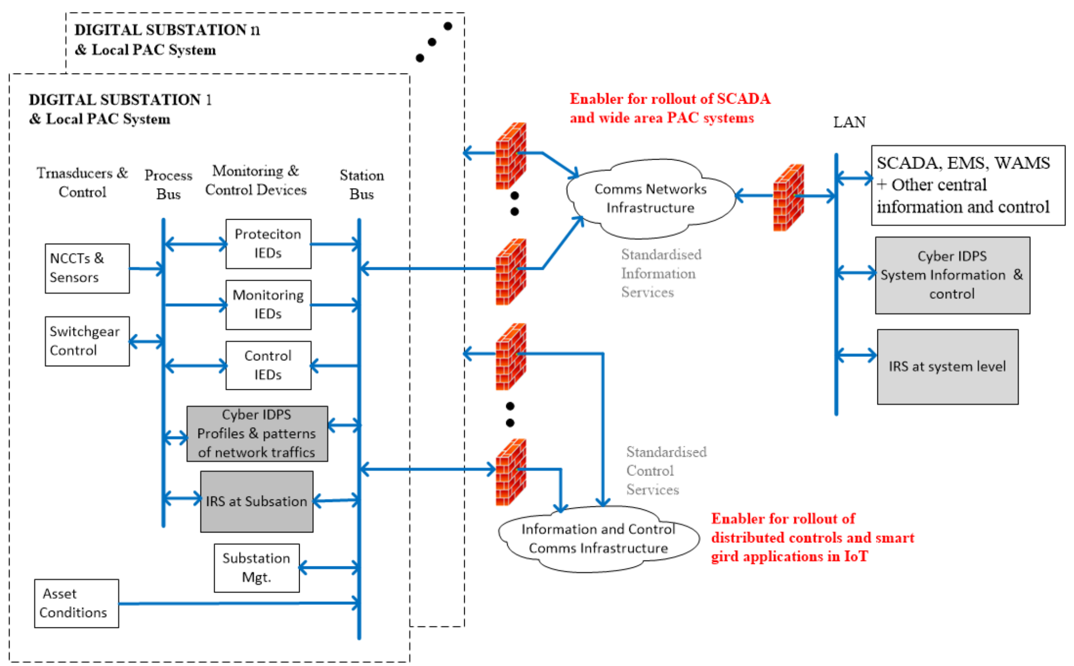
- **Defense Solutions:** Development of advanced defense strategies, including AI-based or collaborative defense mechanisms, to secure IEDs from tampering in Electrical Cyber-Physical Systems.
- **Machine Learning (ML) and Collaborative Defense:** Use of ML and collaborative defense methods to prevent false tripping of IEDs caused by malicious actions in Electrical Cyber-Physical Systems.
- **AI and ML for Data Integrity:** Application of AI and ML techniques to ensure the security and integrity of data transmitted over communication networks, such as SCADA data or other digitized power system data, protecting against cyberattacks.

By focusing on these research areas, CyberSAFEN aims to strengthen the resilience of power grid systems against cyber threats and enhance their operational security.

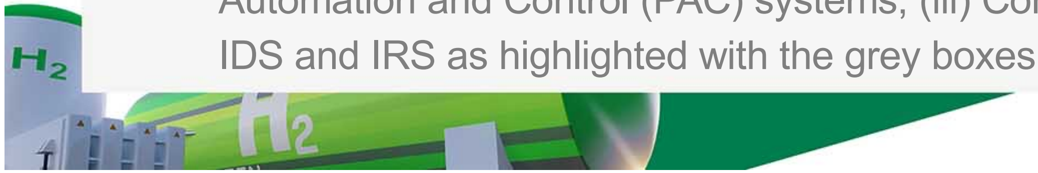


METHODOLOGY

Cyber-SAFEN solution or dual defence system – Intrusion Detection and Prevention System (IDS) and Intrusion Response System (IRS)

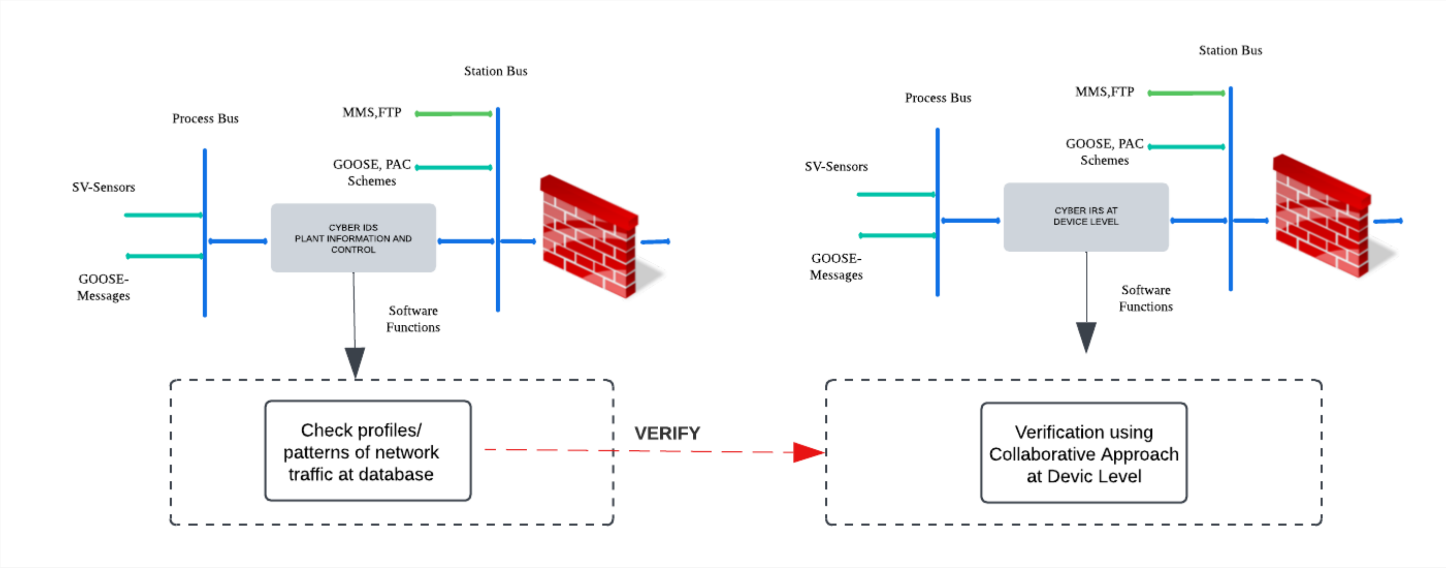

DIGITAL SUBSTATION n
& Local PAC System
DIGITAL SUBSTATION 1
& Local PAC System
Trnasducers & Control
Process Bus
Monitoring & Control Devices
Station Bus
NCCTs & Sensors
Switchgear Control
Asset Conditions
Proteciton IEDs
Monitoring IEDs
Control IEDs
Cyber IDPS Profiles & patterns of network traffics
IRS at Subsation
Substation Mgt.
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

It consists of (i) Digital communication network Infrastructures, (ii) substations with Protection, Automation and Control (PAC) systems, (iii) Control centre with SCADA and (iv) Cyber-SFAEN solution IDS and IRS as highlighted with the grey boxes.



CYBER-SAFEN SOLUTION

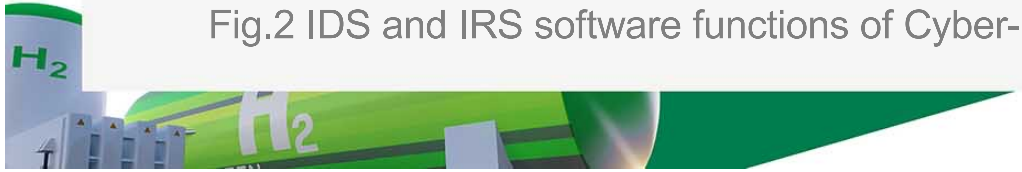
Cyber-SAFEN solution or dual defence system – Intrusion Detection and Prevention System (IDS) and Intrusion Response System (IRS)



(a) The IDS at data exchange level

(b) The IRS among device level

Fig.2 IDS and IRS software functions of Cyber-SAFEN solutions



CONCLUSIONS

Integrated Cyber Defence (ICD) Platform: Cyber SAFEN aims to build an integrated cyber defence platform to test critical security functions for PAC, WAMS, and SCADA systems, ensuring resilience against advanced cyberattacks.

Supports the Digital Transformation of Power Systems: This project addresses the pressing cybersecurity challenges involved in the digital transformation of power systems, ensuring safe and efficient operations.

Enhances Security and Resilience: Cyber SAFEN fortifies energy networks against potential attacks, ensuring that critical functions are protected and operational continuity is maintained.

Facilitates the Net-Zero Transition: By securing and automating energy networks, Cyber SAFEN supports the transition towards a digital, net-zero energy future, driving sustainability and operational efficiency.

Any Question?

Haiyu.li@manchester.ac.uk
Sugandh.Khanna@manchester.ac.uk

cigre

For power system expertise