Notes on Completion: Please refer to the appropriate NIA Governance Document to assist in the completion of this form. The full completed submission should not exceed 6 pages in total.

NIA Project Registration and PEA Document

Date of Submission

Jun 2025

Project Reference Number

NIA_SPEN_0114

Project Registration

Project Title

Cyber V-PROTECTS

Project Reference Number

NIA_SPEN_0114

Project Licensee(s)

SP Energy Networks Distribution

Project Start

June 2025

Project Duration

1 year and 10 months

Nominated Project Contact(s)

Lara Cardoso Figueiredo

Project Budget

£176,000.00

Summary

Cyber V-PROTECTS will develop a comprehensive, representative system within a virtual environment that can simulate various cyber-attacks against OT systems and their communication protocols. The system will leverage known techniques, tactics and procedures employed by cyber threat actors, providing a realistic platform for both offensive and defensive cyber operations.

Third Party Collaborators

Glasgow Caledonian University

Nominated Contact Email Address(es)

innovate@spenergynetworks.co.uk

Problem Being Solved

Power companies face increasing cybersecurity threats, including ransomware, data loss, malware, Distributed Denial-of-Service (DDoS) attacks, and espionage, which can lead to operational disruptions, financial losses, and regulatory non-compliance. The rapid digitalisation of substations, integration of cloud technologies, and deployment of Industrial Internet of Things (IIoT) devices further expand the attack surface, introducing new vulnerabilities that are challenging to address without disrupting live operations.

Another key challenge in securing Operational Technology (OT) systems is the inability to test cybersecurity controls on live infrastructure without risking system stability, safety, and compliance. Testing in real-world environments could cause unintended disruptions, including system downtime, misconfigurations, or operational failures that impact critical power infrastructure and customer supply. Additionally, many cyber threats evolve rapidly, making it difficult to validate defences against emerging attack

techniques without a dedicated, safe, and controlled environment for experimentation.

The increasing convergence of IT and OT systems presents further challenges, as traditional IT security solutions often fail to address the unique constraints of critical infrastructure. Additionally, supply chain vulnerabilities introduced by third-party vendors and IoT devices require thorough assessment before deployment.

Training and education play a pivotal role in mitigating the financial and operational impact of cyber-attacks. According to IBM's 2024 Cost of a Data Breach Report, organisations that invest in well-trained personnel and informed workflows saved an average of USD 2.2 million compared to those that did not. Furthermore, the report found that breaches took significantly longer to identify and contain in organisations suffering from security skill shortages. These findings reinforce the urgent need for structured training programs and educational platforms to close the skills gap, accelerate incident response, and reduce the cost and duration of cyber incidents.

The 2024 Verizon Data Breach Investigations Report further highlights that the human element was involved in 68% of breaches, often due to unintentional mistakes rather than malicious intent. This underscores the critical need for continuous and accessible cybersecurity awareness training across all organizational layers. Importantly, the report concludes that if organizations could improve the security behaviour of their workforce, they could potentially mitigate the impact of over two-thirds of the breaches observed. Therefore, by facilitating practical, scenario-based training in controlled environments, this project directly addresses one of the most consequential factors in breach prevention and resilience.

As IT and OT systems continue to converge, it is no longer sufficient to train these domains in isolation. Cross-disciplinary training that bridges the knowledge gap between IT cybersecurity experts and OT engineers is essential. The 2015 Ponemon Institute Global Report noted that executive-level involvement and broader institutional awareness in security practices correlated with reduced breach costs, highlighting the benefits of integrated approaches. In the context of IT/OT convergence, cross-disciplinary training fosters mutual understanding of unique system constraints, operational needs, and security priorities, thereby enabling cohesive defence strategies and more effective incident response across both domains.
Currently, there is a lack of controlled environments where cybersecurity teams, engineers, and incident responders can safely test, develop, and validate cybersecurity controls for OT systems. Without a representative environment for testing SCADA (Supervisory Control and Data Acquisition) systems, field devices, and Programmable Logic Controllers (PLCs), organisations struggle to understand the real-world consequences of cyber-attacks on physical infrastructure and to deploy proactive cyber defences.

Finally, there is significant skills gap in cybersecurity for critical infrastructure, affecting not only power engineers but also professionals across the energy sector, academia, and training institutions. The lack of specialised cybersecurity education, industry-focused training, and hands-on learning opportunities in OT environments limits the ability of engineers, researchers, and future professionals to assess and respond to cyber risks effectively.

Method(s)

The project follows an evidence-based research and development approach. Latest research in this field establishes hybrid cyber-physical testbeds (CPT) as a balance between cost, fidelity, flexibility, and scalability, making them an effective solution for cybersecurity testing, research, and training in OT environments. By integrating virtual, emulated, and physical components, hybrid CPTs provide a realistic controlled environment to assess cyber risks, validate security controls, and develop skills without disrupting live critical infrastructure. Such a CPT accompanied by specialised training materials also addresses the critical skill gap in OT security. These materials are designed to support engineers, cybersecurity professionals, and researchers in developing practical skills through structured exercises, real-world attack simulations, and guided incident response scenarios. The platform, therefore, ensures that users gain both theoretical understanding and practical proficiency, bridging the gap between IT and OT cybersecurity practices.

Digital simulation of physical environment: A high-fidelity, virtual representation of power generation, transmission and distribution infrastructures will be built to accurately simulate the behaviour of real-world physical systems, including the physical impact of cyber-attacks. This mimics the live operational environments without the risks associated with real-world testing.

High-fidelity IT and OT network is developed following the Purdue Enterprise Reference Architecture (PERA) model architecture. Taking advantage of virtualisation technologies, the design emulates several components such as, end devices, personal computers, servers, firewalls, intrusion detection and prevention systems (IDPS), SCADA, human machine interface (HMI), PLC and end field

devices (sensors and actuators). These components are designed to be independent and modular to support future scalability and seamless upgrades without reconfiguring the entire CPT. Therefore, allowing the platform to be evolved as new technologies, cybersecurity threats, and industry standards emerge. The modularity and virtualisation also facilitate rigorous cybersecurity testing, allowing different configurations to be validated. Finally, each emulated component can be replaced by a physical component for pre-deployment validation and testing of new technologies and protocols, without impacting the rest of the CPT.

The third element of the CPT is threat modelling and cyber-attack simulation by following well-established guidelines and frameworks. For example, the Cyber Kill Chain methodology is used to simulate advanced persistent threats (APTs) by demonstrating how attackers progress through different attack stages, while the Industrial Cyber Kill Chain extends this model to OT specific attacks, focusing on process manipulation and physical consequences. MITRE ATT&CK for ICS is used to systematically replicates adversary tactics, techniques, and procedures (TTPs) in real-world attacks against OT environments. Additionally, frameworks such as Cyber Assessment Framework (CAF), STRIDE, PERA, and MITRE's CREF are incorporated to ensure a holistic approach to cyber risk assessment and regulatory compliance.

Hence, the CPT facilitates the simulation, analysis, and mitigation of a diverse range of cyber-attack scenarios, including network-based threats (such as denial-of-service, man-in-the-middle), OT protocol vulnerabilities (such as Modbus exploitation), and cyber-physical attacks such as sensor manipulation and transduction attacks. By enabling proactive threat modelling and security control validation, the platform supports the development of robust detection, prevention, and incident response strategies to enhance the resilience of critical infrastructure.

Scope

The scope of the project is to develop a comprehensive, representative system within a virtual environment that can simulate various cyber-attacks against OT systems and their communication protocols. The system will leverage known techniques, tactics and procedures employed by cyber threat actors, providing a realistic platform for both offensive and defensive cyber operations.

The system will be designed to simulate a wide range of cyber-attacks including network layer attacks, such as denial of service, attacks on SCADA, such as remote code execution, and attacks on field devices and PLC (Programmable Logic Controllers). It will also be able to simulate natural disasters, loss of power, safety shutdowns and loss of safety controls.

The project's scope and focus are:

WP1 – Project Scope Development.

- **WP1.1 Set project Scope** – Define boundaries of the testbed, including the theme (smart grid) and industrial control system components (ICS) within the power generation, transmission and distribution zones.
- **WP1.2 Requirement specification** - Details the functional requirements, such as performance criteria, security constraints, and system features.
- **WP1.3 Risk Assessment** - Identifies potential risks and propose mitigating solutions for the development process.
- **WP1.4 Feasibility Study and technology assessment** - Review existing cybersecurity frameworks and OT security standards to inform CPT development. Assess best practices for CPT design to ensure the platform achieves high fidelity, modularity, and scalability. Conceptualise the physical environment of the CPT in collaborating with Scottish Power Energy Network, agree on the overall architecture and individual components.
- **WP1.5 SPEN review and approval** - Formal meeting with SPEN to review all planning documents (scope, requirements, risks, etc.) and ensure alignment with their expectations. Discuss potential adjustments and secure SPEN's sign-off on planning deliverables before proceeding to the design phase.

WP1.6 Project Plan with Gantt Chart - A detailed timeline showing dependencies between activities, resource allocation, and deadlines.

WP2 – System Architecture Design.

- **WP2.1 System architecture development** - Produce a high-level diagrams that depict the structure of the testbed, including how the cyber-physical components are connected and interact with the virtualized environment.
- **WP2.2 Game Design** - Develop and design the physical environment, and the physics to simulate the smart grid, following the system architecture (agreed upon during the planning).

- **WP2.3 Network topology** - Describes the network topology, including communications between virtual and physical components, firewall settings, and protocols used.
- **WP2.4 Security or vulnerability design** - Defines the security features of the testbed, design intentional vulnerabilities and measures to simulate cyber-attacks, and design kill switch mechanism to prevent the testbed from accidently connecting to the internet.
- **WP2.5 Human Machine Interface** - Draft and design the HMI for controlling and monitoring the overall industrial process, generation, transmission and distribution.
- **WP2.6 System Integration Plan** - Describes how the different components (virtual and physical) will be integrated and how simulation fidelity will be ensured.

WP3 – Prototype Development.

- **WP3.1 Prototype Development** – Develop a working version of the system with core components in place.
- **WP3.2 Full Scale Development** - Implementation of custom code, scripts, and automation logic, firewalls, networking, routing and industrial protocols for emulating the entire ICS.
- **WP3.3 Optimization and configuration** - The setup of virtual machines, containers, and operating system virtualization for sandboxing the simulation. Configure individual components of the system (HMI, SCADA, SIEM, PLC, Firewall etc.
- **WP3.4 Initial Documentation** – Creation of early versions of user manuals, system documentation, and technical guides for the CPT.
- **WP3.5 Cyber attack simulation scenarios** – Creation of scripts or framework for simulation of different types of cyber attack on the smart grid (denial of service, man-in-the-middle, ransomware, etc) informed by research performed in WP1.

WP4 – Testing, Training and Final Documentation.

- **WP4.1 Test Plan** – Development of comprehensive plan outlining test cases, methodologies, functionality, performance testing, and success criteria for each aspect of the system.
- **WP4.2 Performance testing and validation** - Validate the accuracy and realism of network behaviour and OT traffic. Ensure the scalability and modularity of the testbed. Test security control effectiveness (IDS, firewalls, logging) Simulate real-world cyber-attacks scenarios (DDoS, malware, protocol exploits, etc). Evaluate network resilience and incident response performance. Benchmark detection, prevention, and recovery times. Conduct rigorous testing and validation of the CPT to ensure overall functionality, accuracy, reliability, and effectiveness in replicating cyber-attack scenarios and evaluating security controls. If required, adjust testbed design based on SPEN's feedback.
- **WP4.3 User acceptance testing** - Feedback from SPEN (researchers, developers, operators) who test the testbed to ensure it meets project objectives and expectations.
- **WP4.4 Final Documentation** - Complete technical documentation, user guides, and reports summarizing the system's operation and functionality.
- **WP4.5 Deployment and Training** - Create scenario-based cybersecurity training materials. Implement interactive hands-on labs. Deliver and deploy the CPT and provide support and training sessions. Conducting interviews and surveys to evaluate the impact and effectiveness of the CPT. Disseminate the project findings and share with community.

Objective(s)

1. Skills development and cybersecurity training:
   a. Bridging the training and skills gap by providing a practical platform for engineers, cybersecurity professionals, and researchers to develop expertise in OT security.
   b. Enabling collaboration between academia and industry for fostering innovative cybersecurity solution for energy systems.
2. Threat simulation and security testing:
   c. Creating a high-fidelity, modular testbed to safely simulate and analyse real-world cyber threats against OT systems and their communication protocols.
   d. Testing security controls and incident response strategies before deployment in live electricity networks, reducing the risk of service disruptions and financial losses.
3. IT and OT security improvement:
   e. Addressing the growing attack surface due to the digitalisation of substations, integration of IIoT, and IT/OT convergence.
   f. Supporting compliance with cybersecurity regulations and ensuring that utilities meet industry best practices for critical infrastructure protection.

Consumer Vulnerability Impact Assessment (RIIO-2 Projects Only)

The projects aim to improve the networks security and safety. Should a cyberattack take place and lead to network outages effecting vulnerable customers the CPT developed within this project will have led to an increase in preparedness to deal with the attack and restore power faster.

Success Criteria

Two success Criteria have been identified:

1. Development of a fully functioning CPT – Evaluated from feedback from users.
2. Production of MITRE ATT&CK report

Project Partners and External Funding

Glasgow Caledonian University – Development of CPT.

Potential for New Learning

The system will be designed to simulate a wide range of cyber-attack types, including but not limited to network layer attacks, such as Denial of Service, attacks on SCADA (Supervisory Control and Data Acquisition) systems, such as remote code execution, and attacks on field devices and PLCs (Programmable Logic Controllers). Additionally, it will be capable of simulating natural disasters and catastrophic events such as loss of power, safety shutdowns, and loss of safety controls. The learnings from these scenarios can help prepare SPEN and other DNOs further develop procedures.

One of the key objectives of this project is to make this system accessible and usable for a broad audience, ranging from novices to technical experts, covering cyber security students (to enhance their knowledge of operational technology) to expect technical engineers (to enhance their knowledge of cyber security). The system will serve as a visual training tool, enhancing understanding and awareness of cyber threats and defences.

Scale of Project

A minimum of two use cases to be deployed within the model, to be supported and validated by SPEN's Threat Intelligence and Behavioural Cyber experts.

Technology Readiness at Start

TRL3 Proof of Concept

Technology Readiness at End

TRL6 Large Scale

Geographical Area

The Project will take place in Glasgow with collaboration between SPEN and Glasgow Caledonian University.

Revenue Allowed for the RIIO Settlement

0

Indicative Total NIA Project Expenditure

176,000

Project Eligibility Assessment Part 1

There are slightly differing requirements for RIIO-1 and RIIO-2 NIA projects. This is noted in each case, with the requirement numbers listed for both where they differ (shown as RIIO-2 / RIIO-1).

Requirement 1

Facilitate the energy system transition and/or benefit consumers in vulnerable situations (Please complete sections 3.1.1 and 3.1.2 for RIIO-2 projects only)

Please answer **at least one** of the following:

How the Project has the potential to facilitate the energy system transition:

With the energy system transition comes rapid digitalisation of substations, integration of cloud technologies, and deployment of Industrial Internet of Things (IIoT) devices. These open DNOs up to increased cyber security threats and to deal with these threats and ensure a safe transition, innovative solutions to improve system cyber security, such as this project, are required.

How the Project has potential to benefit consumer in vulnerable situations:

n/a

Requirement 2 / 2b

Has the potential to deliver net benefits to consumers

Project must have the potential to deliver a Solution that delivers a net benefit to consumers of the Gas Transporter and/or Electricity Transmission or Electricity Distribution licensee, as the context requires. This could include delivering a Solution at a lower cost than the most efficient Method currently in use on the GB Gas Transportation System, the Gas Transporter's and/or Electricity Transmission or Electricity Distribution licensee's network, or wider benefits, such as social or environmental.

Please provide an estimate of the saving if the Problem is solved (RIIO-1 projects only)

N/A

Please provide a calculation of the expected benefits the Solution

The financial penalties for a potential cyber-attack are expected to be very high, the CPT developed within this project will improve both threat detection and cyber response with a cost-effective solution. There is also expected to be safety benefits, as cyber-attacks can affect monitoring sensors and lead to injuries should someone operate the electrical system.

Please provide an estimate of how replicable the Method is across GB

There is no indication of any issues with other Networks developing similar cyber physical testbeds.

Please provide an outline of the costs of rolling out the Method across GB.

The current cost of the project is £176,000. It is reasonable to assume costs for other Networks' cyber physical testbeds would be similar.

Requirement 3 / 1

Involve Research, Development or Demonstration

A RIIO-1 NIA Project must have the potential to have a Direct Impact on a Network Licensee's network or the operations of the System Operator and involve the Research, Development, or Demonstration of at least one of the following (please tick which applies):

☐ A specific piece of new (i.e. unproven in GB, or where a method has been trialled outside GB the Network Licensee must justify repeating it as part of a project) equipment (including control and communications system software).

☐ A specific novel arrangement or application of existing licensee equipment (including control and/or communications systems and/or software)

☐ A specific novel operational practice directly related to the operation of the Network Licensees system

☐ A specific novel commercial arrangement

RIIO-2 Projects

☐ A specific piece of new equipment (including monitoring, control and communications systems and software)

☑ A specific piece of new technology (including analysis and modelling systems or software), in relation to which the Method is unproven

☐ A new methodology (including the identification of specific new procedures or techniques used to identify, select, process, and analyse information)

☐ A specific novel arrangement or application of existing gas transportation, electricity transmission or electricity distribution equipment, technology or methodology

☐ A specific novel operational practice directly related to the operation of the GB Gas Transportation System, electricity transmission or electricity distribution

☐ A specific novel commercial arrangement

Specific Requirements 4 / 2a

Please explain how the learning that will be generated could be used by the relevant Network Licensees

The threat of cyber-attacks is increasing for all DNOs; therefore, the success of this project can help inform the development of other CPT's. The findings will be disseminated and ensure the replication of the solution for other Network Licenses.

Or, please describe what specific challenge identified in the Network Licensee's innovation strategy that is being addressed by the project (RIIO-1 only)

N/A

Is the default IPR position being applied?

☑ Yes

Project Eligibility Assessment Part 2

Not lead to unnecessary duplication

A Project must not lead to unnecessary duplication of any other Project, including but not limited to IFI, LCNF, NIA, NIC or SIF projects already registered, being carried out or completed.

Please demonstrate below that no unnecessary duplication will occur as a result of the Project.

There have been no similar Cyber physical-testbeds developed for any UK network licensees therefore there will be no duplication.

If applicable, justify why you are undertaking a Project similar to those being carried out by any other Network Licensees.

N/A

Additional Governance And Document Upload

Please identify why the project is innovative and has not been tried before

N/A

Relevant Foreground IPR

Project expected to generate a new methodology for training employees to deal with cyber-attacks.

Data Access Details

The SP Energy Networks Data Sharing policy can be found here.

Please identify why the Network Licensees will not fund the project as apart of it's business and usual activities

The project involves the development of an innovative solution with a low TRL to improve SPENs response to Cyber risks. Exploratory activites are not typically funded under business-as-usual activities. The solution needs to be better understood before taking it to BaU to ensure the benefits are maximised.

Please identify why the project can only be undertaken with the support of the NIA, including reference to the specific risks(e.g. commercial, technical, operational or regulatory) associated with the project

The development of a CPT for DNOs needs to be better understood to allow for a strong business justification. The capabilities of such a system must be explored to determine what the benefits would be from implementation. There is a risk that the CPT would become outdated after its implementation, therefore GCU will provide documentation and support to update the platform. Additionally, there is potential that the CPT does not match the fidelity of Smart Grid.

This project has been approved by a senior member of staff

☑ Yes