

## NIA Project Registration and PEA Document

### Date of Submission

Sep 2026

### Project Reference Number

NIA\_SPEN\_0143

## Project Registration

### Project Title

Native Cyber-Resilience Instrumentation for Digital Substations

### Project Reference Number

NIA\_SPEN\_0143

### Project Licensee(s)

SP Energy Networks Transmission

### Project Start

October 2026

### Project Duration

1 year and 7 months

### Nominated Project Contact(s)

Lara Cardoso

### Project Budget

£250,000.00

## Summary

Digital substations increasingly depend on converged IT/OT communications, creating cyber risks that conventional controls may not detect. This 18-month research project will define the architecture, requirements and deployment roadmap for programmable cyber-resilience instrumentation embedded within substation networks. It will utilise deep packet inspection and programmable data-plane functions for cyber-resilience in Digital Substations. Through stakeholder engagement, operational behaviour profiling, threat modelling and comparative hardware feasibility analysis, the project will identify suitable insertion points, device classes and monitoring approaches for future deployment. Outputs will include an architectural requirements specification, threat and behaviour analysis, programmable networking review, and a Phase-2 proposal for pilot demonstration and wider SPEN rollout.

## Third Party Collaborators

University of Glasgow

### Nominated Contact Email Address(es)

innovate@spenergynetworks.co.uk

## Problem Being Solved

Electrical substations are increasingly being digitalised through the integration of intelligent IoT devices and control systems, remote management capabilities and standards-based communications such as IEC 61850. This transition is leading to greater convergence between Information Technology and Operational Technology.

Although digitalisation can improve network visibility, automation and operational efficiency, it also increases the cyber-attack surface of substations. A malicious or compromised device may communicate through trusted internal channels, exploit weaknesses in

proprietary or legacy equipment, or generate traffic that is not detected by conventional perimeter firewalls. A successful attack could affect the availability, integrity or safe operation of protection, control and monitoring systems.

Current cyber-security arrangements are principally based on perimeter protection, fixed security appliances and central monitoring. These controls may have limited ability to inspect operational traffic deeply, recognise previously unseen behaviour or apply dynamically updated policies within the substation network. Retrofitting additional security equipment can also be difficult because substations differ in age, architecture, communication protocols, space, power availability and operational constraints.

This project would facilitate SPEN in understanding mechanisms and approaches for native cyber-resilience provisioning of future digital substations. This requires evidence on where programmable monitoring and filtering functions could be introduced, which technologies and hardware classes are suitable, how operational behaviour can be characterised, and how such functions could be scaled without adversely affecting time-critical protection and control communications.

## Method(s)

The project will use a research and technical feasibility methodology comprising five linked work packages.

### 1. Stakeholder and substation instrumentation feasibility:

SPEN stakeholders and relevant domain experts will be engaged to identify operational constraints, existing and future substation configurations, permissible equipment classes and feasible physical and logical insertion points for programmable cyber-resilience functions.

### 2. Architecture and requirements alignment:

The project will review digital substation standards, protocols and communication patterns, including IEC 61850 and GOOSE etc, sampled values and relevant legacy OT protocols.

### 3. Operational behaviour profiling and threat modelling:

Normal substation communication behaviour will be characterised using applicable standards, current research and SPEN operational expertise. Relevant cyber-threat scenarios will be reviewed, and suitable statistical or machine-learning techniques for identifying anomalous behaviour will be assessed.

### 4. Programmable network techniques review:

Deep packet inspection, programmable data-plane technologies, user-plane functions and service function chaining will be assessed for their ability to provide traffic visibility, filtering and policy enforcement with minimal latency. Candidate implementation platforms, ranging from IoT-class devices to embedded routers would be analysed.

### 5. Future exploration and phase-2 proposal development:

The findings will be consolidated into a deployment roadmap and follow-on project proposal covering laboratory demonstration, field validation, central monitoring, data aggregation and potential wider rollout.

## Scope

The project will define the foundations for programmable cyber-resilience instrumentation within SPEN digital substations. It will cover:

- Current and anticipated digital substation architectures;
- Interfaces between digital communications, control and monitoring systems;
- Operational constraints and feasible instrumentation locations;
- IEC 61850, GOOSE, MMS, sampled values and relevant legacy protocols;
- Deep packet inspection, programmable networking and service function chaining;
- Normal operational behaviour profiling and cyber-threat modelling;
- Options for central monitoring and multi-substation orchestration;
- The technical and organisational roadmap for the subsequent stage.

The project is expected to benefit consumers by reducing the risk and potential consequences of cyber-related disruption, supporting the secure digitalisation of the network and enabling future monitoring and mitigation capabilities to be developed more efficiently. It may also reduce future duplication of design, integration and procurement effort by providing SPEN with a common architectural blueprint and evidence-based technology requirements.

While this is a low TRL research project that will advise on but not deploy any production solutions, financial benefits will stem from establishing evidence needed to quantify avoided outage exposure, reduced incident investigation effort, reduced bespoke engineering, and more efficient deployment during the follow-up demonstration Phase-2.

## Objective(s)

- Define the architectural requirements for a programmable cyber-resilient network node for digital substation environments

- Assess state-of-the-art approaches for real-time deep packet inspection and anomaly filtering at the edge
- Identify feasible physical and logical instrumentation points across SPEN substation architecture(s).
- Evaluate feasibility of low-footprint implementation, e.g., IoT-class hardware, through comparative analysis of candidate hardware platforms.
- Produce a technical and strategic roadmap for a Phase-2 NIA proposal for laboratory and operational demonstration.

## Consumer Vulnerability Impact Assessment

An assessment of distributional impacts (technical, financial and wellbeing related) for this project has been carried out using a bespoke assessment tool, which assesses the project as having a positive, negative or neutral effect on consumers in vulnerable situations. To help inform the assessment, this tool considers the categories of consumers identified in the Priority Services Register. This project has been assessed as having a neutral impact on customers in vulnerable situations.

The project will not interact directly with consumers and is not expected to create any adverse distributional, financial or wellbeing impact for consumers in vulnerable situations.

Its benefits arise from improving the resilience posture of the electricity distribution infrastructure. Consumers who are medically dependent on electricity, have limited ability to respond to interruptions, live in remote locations or have reduced financial resilience can be disproportionately affected by prolonged or widespread loss of supply. Research that supports earlier detection and containment of cyber incidents may therefore contribute to reducing the likelihood or duration of interruptions affecting these groups.

No consumer data will be collected, processed or used. The project will also avoid changes to live operational systems during this phase, so it will not introduce additional reliability or service risks to consumers.

A more detailed assessment of impacts on consumers in vulnerable situations will be undertaken during any Phase-2 field demonstrator, particularly where automated mitigation or operational decision-making is proposed.

## Success Criteria

The project will be considered successful where:

1. Relevant SPEN stakeholders have been engaged and their operational constraints, priorities and deployment requirements are documented.
2. A stakeholder-informed instrumentation framework is devised to identify credible physical and logical insertion points across representative digital, legacy and mixed-architecture substations.
3. A complete architectural requirements specification is produced for a future programmable cyber-resilience node.
4. Normal substation communication characteristics, relevant cyber-threat scenarios and appropriate anomaly-profiling techniques are documented.
5. Deep packet inspection, programmable data-plane and service function chaining options are assessed against substation requirements, including latency, reliability, interoperability and maintainability.
6. Key technical, data, safety, security, integration and organisational gaps for a Phase-2 development and demonstrator are identified.
7. A credible roadmap for central monitoring and wider deployment is produced.
8. A Phase-2 proposal and associated problem statement are prepared.

## Project Partners and External Funding

This project will be run with the University of Glasgow

## Potential for New Learning

The project is expected to generate new learning in the following areas:

- How programmable network-security functions can be incorporated within digital substations without major reconfiguration of existing architectures;
- Where monitoring and filtering nodes can be positioned in legacy, IEC 61850 and mixed-technology substations;
- The functional and non-functional requirements for processing time-critical substation communications;
- The suitability and limitations of deep packet inspection for GOOSE, MMS, sampled values and legacy protocols;
- The applicability of programmable data-plane and user-plane-style processing to electricity distribution OT environments;
- How service function chaining can support adaptive security policy enforcement;
- Methods for profiling normal substation traffic where access to high-resolution live data is constrained;

Learning will be disseminated through project reports, internal/SPEN knowledge-sharing sessions, technical workshops, academic

publications and conference presentations where appropriate. Sensitive details relating to substation architecture, vulnerabilities or defensive configurations will be sanitised or withheld in accordance with SPEN security requirements.

Scale of Project

The proposed scale is proportionate to the technical breadth and importance of the research problem. Digital substations combine protection, control, telecommunications, cyber-security and operational safety requirements. A credible assessment therefore requires expertise in programmable networking, cyber-security, power systems, substation communications and operational technology.

The 18-month duration allows the project to conduct meaningful stakeholder engagement, examine variations across representative substation architectures, review a range of technologies and protocols, undertake comparative feasibility work, and consolidate the results into a usable Phase-2 roadmap.

A smaller project would risk producing only a high-level literature review without sufficient SPEN-specific operational input, protocol analysis, hardware comparison or deployment planning. It would also limit the project's ability to examine the interaction between architecture, modelling, traffic behaviour, performance and operational constraints.

The proposed investment is modest relative to the potential cost of cyber-related disruption, widespread redesign or unsuitable technology deployment. The study will derisk and reduce uncertainty before SPEN commits to a more costly laboratory or field demonstration.

Technology Readiness at Start

TRL2 Invention and Research

Technology Readiness at End

TRL3 Proof of Concept

Geographical Area

The project will be carried out in the SPT licence area

The research will principally be undertaken at the University of Glasgow and through engagement with SPEN. The study will consider requirements applicable to SPEN electricity distribution substations. No installation or active testing in a live substation is proposed during this project phase. Where site-specific information is needed, representative SPEN substations or architecture types will be considered, subject to operational access, cyber-security controls and information-governance requirements.

Revenue Allowed for the RIIO Settlement

0

Indicative Total NIA Project Expenditure

£ 249,999.62 subject to final confirmation

# Project Eligibility Assessment Part 1

## Requirement 1

Facilitate the energy system transition and/or benefit consumers in vulnerable situations

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

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

The energy system transition requires increasing levels of automation, monitoring, decentralised energy integration and remote operation. These capabilities depend on secure and reliable digital communications within substations.

Cyber-security concerns can delay digitalisation or require costly, bespoke controls. By establishing how cyber-resilience can be designed into substation networks, the project will reduce uncertainty associated with deploying future digital protection, control, monitoring and flexibility solutions.

The project will identify architectural and technical requirements for adaptable monitoring and filtering functions that can respond to new threat behaviours without repeatedly redesigning the physical substation environment. This may support safer and more scalable adoption of digital substations, active network management, distributed energy sources and other capabilities needed for a low-carbon electricity system.

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

The project may benefit consumers in vulnerable situations by supporting greater resilience of the electricity distribution infrastructure.

Consumers who rely on electrically powered medical equipment, have mobility or communication difficulties, live in isolated areas or have limited financial means can experience disproportionate harm from prolonged interruptions. Improved detection, analysis and containment of cyber incidents could reduce the probability, scale or duration of interruptions caused by malicious activity.

The project will not use consumer data and will not change live operational systems. Consequently, no direct adverse impact on consumers in vulnerable situations is expected over the course of this project.

## 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

n/a

### Please provide a calculation and/or description of the expected benefits of the solution

N/A - This is a research innovation project

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

N/A - This is a research innovation project

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

N/A - This is a research innovation project

## Requirement 3 / 1

Involve Research, Development or Demonstration

Projects 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

Involve Research, Development or Demonstration - Please select all that apply

- ☐ 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

Network licensees could use the project learning to:

- Define requirements for future digital substation procurement;
- Identify suitable monitoring and security insertion points;
- Assess the impact of cyber-security processing on time-critical OT traffic;
- Develop representative digital substation threat models;
- Select anomaly-detection approaches appropriate for constrained operational environments;
- Structure future in-house and field trials;
- Develop common specifications rather than site-specific solutions;

Because the outputs will be based on common substation criteria and vendor-neutral specifics, they should be adoptable to other GB distribution and transmission licensees.

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. Networks must explicitly mention similar projects that they have considered and how these differ.

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

The project will not lead to unnecessary duplication of existing or completed innovation projects. A review of relevant NIA, NIC, SIF, IFI and LCNF projects indicates that, while cyber security and digital substations have been addressed in other initiatives, there is no known project that focuses specifically on the programmable monitoring, inspection and policy-enforcement functions, embedded at selected points within the substation's communication network architecture.

**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**

Current substation cyber-security is generally based on network segregation, perimeter controls, fixed monitoring equipment and centralised security systems. These measures remain important but can have limited visibility of malicious activity operating within trusted substation environment.

This project provides an innovative approach that takes into account programmable monitoring, inspection and policy-enforcement functions, embedded at selected points within the substation's communication network architecture. It combines deep packet inspection, programmable data-plane processing, operational behaviour profiling and adaptable policies.

Although these technologies exist in teleco, cloud and enterprise environments, their combined application to time-critical electric distribution substation communications is an ambitious task. The project will address distinctive requirements such as deterministic traffic, low latency, high availability, legacy interoperability, environmental constraints and the risk of interfering with protection and control functions.

The project is therefore not business as usual and involves technical, operational and integration uncertainty.

### **Relevant Foreground IPR**

N/A

### **Data Access Details**

Access to this data must be requested by contacting [innovation@spenergynetworks.co.uk](mailto:innovation@spenergynetworks.co.uk). Please provide the following information in your request:

- Affiliation, position and contact details of requesting party
- Relevant project and type of data required
- Reasons for requesting this data and evidence that this data will be used in the interest of the UK network electricity customers
- How data will be shared internally and externally by the requesting party Any data request deemed unsuitable for sharing will be highlighted to the appropriate requesting party.

After receiving the request we will provide the estimated date for completing the data provision based on other requests and our team workload at that time. All requested data remains the property of SP Energy Networks.

### **Please identify why the Network Licensees will not fund the project as a part of it's business and usual activities**

The appropriate architecture, performance limitations, insertion points, hardware platform, threat models and integration requirements remain uncertain. No proven commercial product has been identified that can be deployed consistently across varied digital, legacy and mixed-architecture substations while meeting operational, safety and cyber-security requirements.

Business-as-usual funding would normally be used to implement a sufficiently mature and implemented solution. This project is required to establish whether the method is feasible and to define the evidence needed for future investment.

### **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**

NIA support is appropriate because the project involves research with an uncertain outcome, generates learning relevant to other network licensees and addresses risks that prevent immediate commercial deployment.

Key risks include:

- **Technical risk:** may not achieve the latency, throughput, or reliability requirements for substation communications.

- **Operational risk:** incorrectly placed or configured functions could interfere with protection and control traffic.
- **Integration risk:** substations vary in age, architecture, vendor equipment and telecommunications design.
- **Cyber-security risk:** detailed monitoring and response functions could themselves create new attack surfaces.
- **Data risk:** representative operational data may be limited or security-sensitive.
- **Commercial risk:** there is no established market price or mature business case for network-wide implementation.
- **Regulatory and assurance risk:** future deployment may require extensive safety, engineering and cyber-security assurance.
- **Adoption risk:** operational teams may not accept a solution that is complex to maintain or insufficiently transparent.

**This project has been approved by a senior member of staff**

☒ Yes