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

Project Reference Number

NIA_SPEN_0064

Project Registration

Project Title

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

Project Reference Number

NIA_SPEN_0064

Project Licensee(s)

SP Energy Networks Distribution

Project Start

May 2022

Project Duration

4 years and 0 months

Nominated Project Contact(s)

Ross Davison

Project Budget

£650,000.00

Summary

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 networks PAC, WAMS and SCADA systems against advanced cyber-attacks. Cyber-SAFEN uniquely focuses on a combined intrusion detection (IDS) and intrusion response system (IRS) powered by advanced AI and machine learning technologies to build a dual defence system against advanced cyber threats.

Third Party Collaborators

Energy Innovation Centre

Nominated Contact Email Address(es)

innovate@spenergynetworks.co.uk

Problem Being Solved

The electricity network serves as the interface between distributed generation, active demand, and local flexibility market. To accelerate the digital transformation of power systems, digital substations are key enablers for the network power flow to be controlled and directed safely and securely from generation to demand. This, however, makes the digital substation a highly attractive target for cyber-attackers aimed at disrupting operations. There is no evidence to show that the existing cyber security technologies or tools could be able to provide sufficient cyber intrusion prevention and defences against advanced cyber threats for power system PAC and SCADA systems so a system is needed to protect our networks from cyber attacks.

Method(s)

This project aims to research, build and demonstrate an integrated cyber defence (ICD) platform to provide essential cyber safe and resilient functions for electricity networks PAC, WAMS and SCADA systems against advanced cyber-attacks.

The intended method to solve the problem will be a technical solution. Through studies we will identify and assess the capability of existing cyber security platforms and products that could be used to build the intrusion defense system.

Scope

Develop the cost benefit analysis and technical feasibility of creating a cyber defence platform at device and system level. Engage and select suitable vendor(s) equipment to utilise

Implement a trial network to test the cyber defence platform. Use advanced data analysis and modelling for identification of normal and abnormal power system operation conditions as well as cyber threats.

Integrated Intrusion detection system: Develop an integrated Intrusion detection System (IDS) based on vendor engagement

Intrusion Response/Defence System: AI based collaborative control of distributed multi-devices strategy to build resilience for PAC, WAMS and SCADA systems against malicious attack actions.

Validate the cyber defence solution on the trial network.

The benefits to customers and the network will come from:

- Reduced risk of outages and damage caused by cyber attacks
- Enable increased digitalisation and automation across the network
- Ensuring a secure and resilient platform on which to rollout further applications

Objective(s)

Cyber-SAFEN will research and develop a Cyber Intrusion Response/defence System (IRS) platform to provide essential cyber security functions to protect control systems, such as PAC, WAMS and SCADA, in electricity networks.

The objectives of the project are as follows:

- Quantify the cost benefit and enabling capability to the GB energy networks,
- Identify the core technologies and applications,
- Engage with the supply chain and identify suitable vendors
- Determine the data sources required for the response capability.
- Develop combined cyber defence solution
- Lab based trail of solution

Generate IPR and disseminate through UK energy industry

Consumer Vulnerability Impact Assessment (RIIO-2 Projects Only)

Details of the expected effects of the Method(s) and Solution(s) upon consumers in vulnerable situations. This must include an assessment of distributional impacts (technical, financial and wellbeing-related). For RIIO-1 projects please add "Not Applicable

Success Criteria

Details of how the Funding Licensee will evaluate whether the Project has been successful. This cannot be changed once registered.

This project will be viewed as a success if it can:

Identify and document the current and future intrusion detection and response requirements for SPEN and NGESO

Deploy and demonstrate a cyber security defence solution in a lab environment and simulated network trial.

Generate IP and disseminate knowledge throughout the UK energy networks.

Project Partners and External Funding

This project will run as a partnership with University of Manchester who will be carrying out the studies and development on behalf of SP Energy Networks and National Grid TO. After the initial technology appraisal the chosen vendor(s) will be selected to develop the solution.

Potential for New Learning

The project will generate new ways to implement a combined cyber defence platform that could be utilised by Energy network operators. The opportunity for demonstrating the cyber-SAFEN solution in the laboratory setup would be used for training and dissemination throughout SPEN and other interested parties. The dissemination of the IP will foster greater competition within the market and encourage multiple vendors to create interoperable commercial solutions and facilitate future investment opportunities.

Scale of Project

The scale of this project is will focus on a trial network. A successful outcome can be scaled across UK energy network operators.

Technology Readiness at Start

TRL2 Invention and Research

Technology Readiness at End

TRL4 Bench Scale Research

Geographical Area

The project will take place within SP Transmission. All work will be conducted in the UK at our project partners laboratories.

Revenue Allowed for the RIIO Settlement

£650,000

Indicative Total NIA Project Expenditure

SPEN £126,605

NG £75,721

University of Manchester £448,653.85

Total £651,000 SPEN £125,000 NG £76,000 University of Manchester £450,000 The supplier costs will be shared between SPEN and NGET, each contributing 50% as the shared funding for supplier costs table below: Partner 2022-2023 2023-2024 2024-2025 Total SPEN £ 60,000 £ 107,500 £ 57,500 NGET £ 60,000 £ 107,500 £ 57,500 Total £ 120,000 £ 215,000 £ 115,000 £ 450,000

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:

Cyber security is a key enabler for the rollout of digital technologies. Having a secure infrastructure acts as an insurance policy and reduces the likelihood of successful attack and reduction in harm caused by a successful attack. The key benefits realised by undertaking this project include:

- Reduced risk of outages and damage caused by cyber attacks
- Enable increased digitalisation and automation across the network
- Builds a secure and resilient platform on which to rollout further applications

Power system digitisations play a key role and provide essential functions to keep the increasingly decarbonised and decentralised energy system running in a reliable, sustainable, and cost-effective manner. Digital substations become enablers for the network power flow to be controlled and directed safely and securely from generation to demand. The digital transformation of the power network, in particular, digital substations, becomes prone to cyber-attacks aimed at disrupting the network operations.

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

This is a research-based project. Benefits will be quantified throughout the project.

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

The research, methods and technical solution will be shared and diseminated throughout the project. The study and trials will have input from multiple license holders to bring the greatest benefit and be replicable for all GB license holders.

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

This is a research-based project. Roll out costs will be quantified throughout the project.

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 project will generate learning that can be disseminated to all relevant network licensees in the area of cyber security. This learning will be shared with the GB licensees via conferences and best practice.

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.

Following projects have been identified on the smarter networks portal that have relevance to the proposed project:

1. NIA_NGET0190 EPRI Research Collaboration on Cyber Security 2016 (P183)

This project provided guidelines for IDS/IPS solutions on the network. CyberSAFEN looks to build on these guidelines, testing and developing a deployment ready solution – powered by AI and machine learning – to protect the network.

2. NIA_NGTO020 IEC 61850 Cyber Resilient Electric Substation Technologies

This project successfully developed a substation IDS. CyberSAFEN looks to take this to the next level by developing an integrated Intrusion Detection and Intrusion Response System.

3. NIA_NGGT0138 Secure AGI – Intrusion Detection System (IDS)

This project developed an intrusion detection system solution tailored for use in a live AGI environment. While learnings will be useful, CyberSAFEN will be large scale and adaptable to many parts of the energy network as well as implementing intrusion response systems.

4. NIA_NGET0189 Security Assessment of Industrial Control Systems (ICS)

This project considered responses to cyber attacks on the network. CyberSAFEN will use AI and machine learning to develop responses to cyber attacks.

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

To date there is no evidence to show that the existing cyber security technologies or tools would provide sufficient cyber intrusion prevention against advanced cyber threats to power system PAC, WAMS and SCADA systems. Protection and control systems studies at Manchester reveal that it is easy to deploy a self-learned GOOSE device with malware software to shut down a digital substation entirely. There is limited research conducted for Intrusion response system at device and system level.

Cyber-SAFEN aims to research and implement suitable defence strategies for the countermeasures to mitigate any malicious attack risk to PAC systems in substations, and WAMS and SCADA systems in control centre. The novelty of Cyber-SAFEN is to harness advanced AI and ML technologies to build a dual defence system against advanced cyber threats. This would act as an enabler and reduce the risk and impact of a successful cyber attack and accelerate future technology and platform rollout.

This project builds on the learnings from the following innovation projects that have received over £12million funding:

- Architecture of Substation Secondary System (AS3)
- Virtual Substation Acceptance Test and Training (VSATT)
- Future Intelligent Transmission NEtwork SubStation (FITNESS)
- IEC61850 Cyber Resilient Electric Substation Technologies (CREST)
- Cyber Security Solutions for Legacy Equipment (CSLE)

National Grid, University of Manchester and SP Energy Networks teams have been working together under the above prior innovation projects to uplift the TRL (Technology Readiness Level). This project is leveraging the resources and outcomes from them, striking the right balance of innovation and investment certainty.

Relevant Foreground IPR

Development will bring together existing open standards, vendor platforms and new data processing and cyber security techniques, this will maximise the interoperability of the platform. We will seek to use existing platforms where possible and identify and partner with the platform which aligns best with our goals. We would expect that the vendor(s) would then act to supply the intrusion defense platfom. We will ensure that the specifications, learning and identified gaps between different vendor platforms are made clear to enable interoperability and a competitive market that the platform can be procured from; in addition, we will ensure the relevant foreground IP is disseminated to facilitate this market.

Data Access Details

Access to data must be requested by contacting SPInnovation@spenergynetworks.com or the project contact.

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 apart of it's business and usual activities

Conventionally such products would be developed by one or two international suppliers. The innovation funding is sought to enable the energy industry to provide leadership in the future product development. With the IP output from the project this will enable commercialisation and competition in the market.

No integrated cyber security defence solution exists in the market for the energy network and therefore SPEN will not fund the project as a part of our business as usual activities.

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

Without NIA funding the commercial and technical risk associated with the development and trial could not be borne by the business. This is the reason for the required support of the NIA fund.

This project has been approved by a senior member of staff

☑ Yes