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

Oct 2021

Project Reference Number

NIA2_SGN0004

Project Registration

Project Title

Phoenix IIoT Demonstrator

Project Reference Number

NIA2_SGN0004

Project Licensee(s)

SGN

Project Start

October 2021

Project Duration

1 year and 1 month

Nominated Project Contact(s)

stuart.sherlock@sgn.co.uk

Project Budget

£423,978.00

Summary

At present the industry uses traditional standalone industrial control system from a mix of companies, making good data quality very challenging. Attempts have been made to overlay IoT solutions, which creates more complexity and management of the digital asset and often leads to cyber security issues or makes the asset more vulnerable.

The project centres on an experimental concept and use trusted technologies which combines advanced real-time control, with cloud technology. The solution will be developed to allow a full sensor to cloud approach, reducing the human operator oversight at each facility.

This demonstrator project will help to ensure the future safety and resilience of our network as it is today, by investing in our infrastructure to keep our assets safe from cyber-attacks, whilst maintaining supply of gas and reducing consumer vulnerability across the network.

Third Party Collaborators

Deltaflare

Nominated Contact Email Address(es)

sgn.innovation@sgn.co.uk

Problem Being Solved

With the aging UK energy industry there is a requirement to modernise these systems to improve efficiency and longevity of our infrastructure, which is critical in meeting our net-zero targets.

With the adoption of smart technology to support the Energy System Transition there is an increased risk of cyber-attacks, therefore it

is essential that we implement a solution that provides maximum security of our infrastructure and for our customers.

Cyber threats can vary in size and impact and can result in site shutdowns and loss of supply to customers, we are also seeing high-profile cases across the world that are causing significant disruptions. The threats are also getting more technically complex to mitigate against due to the use of AI and ML technologies. In the event of a cyber-attack vulnerable consumers would be significantly impacted, therefore providing security and the appropriate resilience at an affordable price will be an integral part of the energy system transition and the future protection of our customers.

Method(s)

At present the industry uses traditional standalone industrial control system from a mix of companies, making good data quality very challenging. Attempts have been made to overlay IoT solutions, which creates more complexity and management of the digital asset and often leads to cyber security issues or makes the asset more vulnerable.

The project centres on an experimental concept and use trusted technologies which combines advanced real-time control, with cloud technology. The solution will be developed to allow a full sensor to cloud approach, reducing the human operator oversight at each facility.

This demonstrator project will help to ensure the future safety and resilience of our network as it is today, by investing in our infrastructure to keep our assets safe from cyber-attacks, whilst maintaining supply of gas and reducing consumer vulnerability across the network.

Scope

The project will run over 12 months and will include the demonstration and validation of the combined software solution in a test environment, followed by deploying two further physical demonstrators at SGN facilities to provide data, evidence and learning in support of the IUK DEFGID project that aligns to Network Information System Directive (NISD) compliance.

The project aims to deliver operational capabilities which facilitate the following productivity increases across the Network:

- Reduction in manual intervention (travel and on-site time)
- Improvement in process optimisation delivering energy efficiency
- Data driven, preventative to predictive maintenance
- Lower replacement costs RTU/ Process control
- Reduced overheads for testing, commissioning, maintenance, and asset management
- Bespoke software on devices will not become obsolete once replaced or upgraded
- Lower power requirements for operation
- Smaller site footprints
- Cyber Security Resilience through Unified cyber security protocols
- Ability to progress away vendor lock-ins
- NISD Compliance

Objective(s)

Key objectives for the demonstrator are as follows:

- Establishing industry-specific Sensor to Cloud connectivity within SGN facilities
- Delivering CNI-grade secure communication on a public/ untrusted WAN
- Achieving software-defined functionality which can be centralised onto a single scalable ‘hub’/hardware platform, rather than on individual devices.
- Reducing the electrical power consumption and footprint of edge gateway

Following outcome will be targeted:

- Lower replacement costs
- Reduced overheads for testing, commissioning, maintenance, and asset management
- Unified cyber security protocols
- Mitigation against obsolescence of bespoke software on devices
- Vendor-independence of entire edge to cloud stack
- Lower power requirements for operation

- Smaller site footprints
- Lower carbon footprint

Consumer Vulnerability Impact Assessment (RIIO-2 Projects Only)

Cyber threats can vary in size and impact and can result in site shutdowns and loss of supply to customers, we are also seeing high-profile cases across the world that are causing significant disruptions. The threats are also getting more technically complex to mitigate against due to the use of AI and ML technologies. In the event of a cyber-attack vulnerable consumers would be significantly impacted, therefore providing security and the appropriate resilience at an affordable price will be an integral part of the energy system transition and the future protection of our customers.

Success Criteria

The following success criteria for the project include the completion of:

- Successfully establishing industry-specific Sensor to Cloud connectivity within SGN facilities
- Deliver CNI-grade secure communication on a public/ untrusted WAN
- Achieving software-defined functionality which can be centralised onto a single scalable 'hub'/ hardware platform, rather than on individual devices.
- Reduction in electrical power consumption and footprint of edge gateway

Project Partners and External Funding

Deltaflare

Potential for New Learning

The project aims to further enhance cyber security within the utility sector and to improve efficiency and longevity of our infrastructure

The project is expected to deliver the demonstration and validation of the combined software solution in a test environment, followed by testing of two further physical demonstrators at two SGN AGI sites.

Scale of Project

The project involves carrying out inhouse testing to prove the physical and software concepts. This will be followed by live trials to demonstrate the technique and gain feedback during the trial.

Technology Readiness at Start

TRL3 Proof of Concept

Technology Readiness at End

TRL8 Active Commissioning

Geographical Area

Trials to be carried out at one site in Scotland and one in Southern on SGN Network.

Revenue Allowed for the RIIO Settlement

N/A

Indicative Total NIA Project Expenditure

The total project expenditure is £381,580, 90[EK1] % (£318,063) of which will be recovered via the NIA funding mechanism in line with the funding conditions. Total project value is £423,978.

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:

N/A

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

This demonstrator project will help to ensure the future safety and resilience of our network as it is today, by investing in our infrastructure to keep our assets safe from cyber-attacks, whilst maintaining supply of gas and reducing consumer vulnerability across the network.

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 need for a secure and robust cyber infrastructure throughout the energy and water utility industries is critical, where the cost associated of cyber-attack can be well over £1m.

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

SGN Network and asserts are similar across the UK, therefore this project is applicable to all Gas Networks.

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

Cost for full testing and demonstration would be determined upon completion of 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

Currently the SGN Network is similar to the other GDNs and Utility Networks with regards to how we manage our Assets with remote monitoring etc. being sent back to the control room.

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.

The project scope has been reviewed against all existing projects and no areas of duplication have been identified.

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

Cyber security is forever changing and requires innovative technology to tackle these issues.

Relevant Foreground IPR

N/A

Data Access Details

Data and project information can be obtained by contacting the project manager.

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

The NIA framework offers a robust, open framework to support this work and ensures the results are disseminated to all licenses. The project will address the viability of the site, identify risks and provide necessary mitigations.

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

This project involves developing a new cyber security which requires development and field trials. The project will address the viability of the site, identify risks and provide necessary mitigations.

This project has been approved by a senior member of staff

☑ Yes