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

Jan 2022

Project Reference Number

NIA2_NGET0014

Project Registration

Project Title

Secure Edge Platform

Project Reference Number

NIA2_NGET0014

Project Licensee(s)

National Grid Electricity Transmission

Project Start

May 2022

Project Duration

1 year and 4 months

Nominated Project Contact(s)

Ibukunolu Oladunjoye
(Box.NG.ETInnovation@nationalgrid.com)

Project Budget

£295,000.00

Summary

The energy network transition will require more agile, flexible and interconnected networks. Digitalisation of assets and processes will play a key part in the preparation of a net-zero capable network. Whilst the IEC61850 suite of standards has been widely adopted for SCADA systems, enhanced system and asset awareness will be required and will be based on IoT technology in many cases. Correlating both data sets and interfacing to common business applications will be a key enabler and value lever for the energy transition. Remote data collection from SCADA and IoT sensors will also require appropriate security solutions that can guarantee the integrity of each of the separate security zones. This project will investigate new solutions for operational data collection and reporting, edge computing and security.

Nominated Contact Email Address(es)

box.NG.ETInnovation@nationalgrid.com

Problem Being Solved

The energy system transition to net zero will require increased system and asset awareness to ensure that asset health and system conditions are understood and operational systems can be optimised. This will require a step change in the amount of data that is collected and reported, as well as the associated cyber security measures that will enable remote connectivity to critical assets. Future system operating tools, situational awareness, wide area monitoring, protection, automation and control, online network modelling as well as digital twin based asset management will all depend on system and asset data. Current reporting architectures are fragmented and no common reference architecture is available. Additionally, a wide variety of data formats and protocols is in use and do not provide the required flexibility. Whilst these data streams and remote access create value, they also introduce cyber security risks which need to be addressed to ensure that the benefits can be delivered without compromising our security.

Method(s)

To address the above problem this project will carry out research into hardware and software architectures and technologies that will enable secure reporting of SCADA data, system monitoring data and asset health data from IoT sensors using a common gateway. The project will aim to virtualise the required functions and provide an edge platform that can offer secure reporting as well as edge processing. The project will develop a laboratory-based test platform for research and development concerning the required software solutions that will be hosted on a virtualisation platform and interact with SCADA, IoT sensors, system monitoring and business systems hosted in the cloud.

A number of use cases for IoT based data reporting, remote configuration, and Machine Learning based edge computing applications will be developed and demonstrated in the supplier laboratory as part of the first phase of the project. During the second phase the test facility will be migrated onto an open NGET virtualisation platform in a substation environment which is part of NGET's cyber security research environment. Remote management of the functions, reporting and edge-computing based use cases will be demonstrated and their security and viability will be evaluated as an end to end process.

Data Quality Statement (DQS):

- The project will be delivered under the NIA framework in line with OFGEM, ENA and NGET internal policy. Data produced as part of this project will be subject to quality assurance to ensure that the information produced with each deliverable is accurate to the best of our knowledge and sources of information are appropriately documented. All deliverables and project outputs will be stored on our internal Sharepoint platform ensuring access control, backup and version management. Relevant project documentation and reports will also be made available on the ENA Smarter Networks Portal and dissemination material will be shared with the relevant stakeholders.

Measurement Quality Statement (MQS):

- The methodology used in this project will be subject to our supplier's own quality assurance regime which is ISO 9001 certified. Quality assurance processes and the source of data, measurement processes and equipment as well as data processing will be clearly documented and verifiable. The measurements, designs and economic assessments will also be clearly documented in the relevant deliverables and final project report and will be made available for review.

In line with the ENA's ENIP document, the risk rating is scored 5 = low.

TRL Steps = 1 (2 TRL steps)

Cost = 1 (<£500k)

Suppliers = 1 (1 supplier)

Data Assumption = 2 (assumptions known but will be defined within the project)

Scope

The scope of the project covers 2 phases. The first phase consists of research and development activities and the design, engineering and development activities carried out in the supplier's laboratory. The work has been structured as 7 work packages that will be delivered by a dedicated team as a "sprint", each addressing a given set of use cases.

Work package 1 will research and develop a proof of concept for a remotely deployable data consuming virtualised application that can be delivered to an existing industrial edge gateway. The application will provide an open interface to data sources including system monitoring, SCADA and IoT sensors that may be using a range of different protocols. The data will be stored locally and made available securely as read-only information to cloud based business applications (see WP3). The design and design choices will be documented and test results will be recorded confirming the extent to which the required performance in terms of security and capability could be demonstrated.

Work package 2 consists of an application that will provide data enrichment. Events recorded by any of the data sources will be correlated to other data sources providing it with additional meta information not contained within the original event record. The application will also enable remote deployment of standardised data models based on the CIM standards (IEC61970).

Work package 3 consists of the development of a cloud publisher application that can securely deliver the locally stored, enriched or otherwise processed data to the relevant business applications in the cloud. Penetration testing will be carried out as part of the work to evaluate the level of security of edge to cloud data communication where the identity of the edge device can be managed from the cloud. Information will be encrypted and the application will be remotely configurable.

Work package 4 will investigate the concept of a remotely deployable rules engine that analysis incoming data and triggers predefined actions depending on the information provided by the data sources. Secure remote configuration, visual programming of rules and analysis functions as well as the interface with the cloud publisher (WP3) will be the main focus of the WP. This application provides an opportunity for easy deployment of rule-based automation and protection schemes as well as enhanced asset management.

Work package 5 aims at proving the concept of remotely deployable machine learning algorithms for detailed analysis of asset health, risks, diagnostics and root cause analysis. Remote deployment to the edge platform will enable large raw datasets to be analysed at each substation site and feed into reporting, monitoring, planning and automation schemes.

Work package 6 investigates a proof of concept for secure and reliable edge to edge messaging. This will facilitate the remote deployment of applications that require data from multiple substations. These applications include rule based or ML based algorithms as investigated in WP 4 and 5.

Design and engineering information for all of these work packages will be produced as well as test schedules and results. Work package 7 will also provide a detailed assessment of the overall architecture in terms of performance and cyber security as well as the second phase of the project which includes an end to end demonstration of the developments carried out in WP1 to 6 in an operational environment at our cyber security research environment based in one of our substations.

There are multiple applications and value levers in terms of optimised asset management, operational and system data reporting. This work has also got the potential to enable remote deployment of new and enhanced automation schemes. The virtualisation of reporting and diagnostic functions will also reduce the number of hardware platforms required when rolling out SCADA systems and enable remote management of some of the configurations. The reduced hardware requirements will provide a saving of £320k over the life of the assets (10 years in this case) and reduced cost for change management due to remote configurability will save approximately £370k. Maintenance costs will also be reduced by £7.5k and overall the net benefit in terms of Net Present Value (NPV) is estimated as £371k based on £295k project spend. This is based on a 10 year assessment following a 2 year development period, required for the development of a solution that can be rolled out. The technology is expected to deliver significantly greater benefits from optimised asset management of primary and secondary assets which are however currently not quantified at this stage. Follow up projects for digital twin applications, system awareness and analysis tools as well as enhanced system integrity protection and remedial action schemes are among those applications that this technology plays a key role in and their benefits will be quantified in future projects.

Objective(s)

The objective of this project is to investigate and validate a global architecture and solution for the reporting of system, asset and operational data from substations to cloud based business applications and potentially operational systems that avoids the current fragmented architecture and delivers enhanced capabilities and opportunities for asset monitoring and management, operational data reporting and system management. The project aims to demonstrate a secure virtualised substation edge computing platform that can deliver:

- Secure reporting of SCADA, monitoring and IoT sensor data
- Data enrichment and standardisation in line with CIM (IEC61970 etc.)
- A secure communication channel from substation to cloud applications
- Edge computing capabilities for rule-based and ML based edge applications
- Secure edge to edge communications for wide area applications
- Detailed cyber security assessment and an end to end demonstration in an operational environment

Consumer Vulnerability Impact Assessment (RIIO-2 Projects Only)

Financial distributional impact: The project is expected to support energy networks to deliver and manage substation equipment more efficiently and at lower cost through virtualisation and digitalisation, levering the value of asset and system data. If these savings are achieved, the financial distributional impact of this project aligns with the simplest case discussed in OFGEM's Assessing the impact of economic regulation report. The report confirms that the savings as a percentage of household income are more significant for lower income deciles and therefore the achieved benefits will be particularly valuable to vulnerable consumers. The pricing structure for energy transmission will not be impacted, e.g. benefits delivered as part of this project can be passed on to all consumers including households using a prepayment meter.

Technical and wellbeing impact: The consumer impact of any of the methods or solutions developed in this project is not dependent on any of the following factors:

- Dwelling and location (potentially including tenure)

- Readiness for digital technology
- Personal and social factors (for example, households with disabilities and medical conditions, or which speak English as a foreign language)

Energy technology and usage profiles:

The results of this work can be applied regardless of energy technology and will not differentiate between consumer usage profiles.

Success Criteria

The success of this project can be measured based on the extent to which the objectives have been achieved, i.e. the successful delivery of reports, designs, specifications a laboratory demonstration as well as a demonstration at a NGET site. The project will provide essential learning to the industry on secure publication of operational data, remote deployment of edge computing services, IoT data reporting and the use of artificial intelligence and machine learning in a substation operational and asset management context.

Project Partners and External Funding

Not applicable

Potential for New Learning

This project has the potential to deliver significant new learning in the field of cyber security, SCADA, protection, automation, control, virtualisation and asset management. The growing need for enhanced asset management, system monitoring, asset health monitoring, device management and centralised role based access management is calling for more connectivity between business applications and operational assets. Security requirements and policies however prevent this unless solutions are secure by design and can not be compromised. If successful, this project will provide a secure means of publishing data to business applications via a secure edge platform that can accommodate all potential substation data sources.

This will act as a key enabler for a large number of applications including ML driven asset management tools including digital twins, System Integrity Protection schemes and many mother applications.

The learning will be disseminated through the publication of the final project report and depending on opportunity through publication and presentation of research papers at conferences and through the ENA and CIGRE.

Scale of Project

The scale of the project includes a desktop study, the development of a laboratory-based proof of concept system and demonstration of key features in a substation environment.

Whilst the technologies used in this research have been applied in different contexts, their application on a common, virtualised platform for SCADA, IoT and system monitoring requires investigation. The assessment of security, architecture and performance is best evaluated using a laboratory based minimum viable demonstrator. End to end tests from site equipment to cloud application also require validation which is why a site implementation of the developed solution is also included in the scope.

Technology Readiness at Start

TRL4 Bench Scale Research

Technology Readiness at End

TRL6 Large Scale

Geographical Area

The project will be partly desktop based and partly consist of laboratory trials. The work will be carried out at the relevant supplier's premises and the demonstrator will be transferred to a NGET substation for testing of the end to end process in an operational environment.

Revenue Allowed for the RIIO Settlement

Not Applicable

Indicative Total NIA Project Expenditure

Total NIA expenditure: £265,500

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:

The project supports the energy system transition through three mechanisms relating to enhanced asset management, system monitoring data and cyber security:

- The energy system transition will require more efficient use of existing infrastructure. Providing an efficient means to collect asset health data securely will provide the foundation for advanced asset management applications and digital twin asset modelling.
- Enhanced deployment of system monitoring and associated situational awareness as well as simplified deployment of System Integrity Protection Schemes (SIPS) are also key technologies required for the energy system transition which will be facilitated by the Secure Edge Platform. These schemes are required in the context of reduced system inertia and fault levels to ensure that appropriate contingencies are defined and network stability can be guaranteed.
- Due to increasing criticality of electricity supplies, improved cyber security will also be an important factor for a successful energy system transition which will be underpinned by digitalisation.

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

Not applicable

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)

Not applicable

Please provide a calculation of the expected benefits the Solution

The secure edge platform will deliver benefits via three value levers. It will reduce the cost of the current baseline solution for collection of operational data from substations by reducing the number of physical devices needed for implementation. The SEP will be a virtualised device, i.e. a software application that can be deployed on already existing hardware. As a secondary benefit this will reduce the support and maintenance cost. The SEP will also enable more remote management and therefore reduce the cost of some configuration changes that can be delivered remotely. Assuming that a solution can be developed and will be ready for deployment in the next two years, an assessment of benefits over the next 10 years would deliver the following outcomes: Based on the NGET business plan the volume of control system replacements and refurbishments would enable a saving of £320k due to virtualisation. The reduction of maintenance cost is estimated as £7.5k and the contribution from reduced cost for changes and updates is £370k. The underlying assumption for this is that 15% of changes can be deployed remotely with a saving of £5k per remote deployment. Considering the anticipated project cost of £295k the net present value of this project is a benefit of £371k.

Additional benefits, which are not currently monetised, will be delivered from enhanced asset management, i.e. reduced cost for maintenance, delayed replacement or refurbishment for assets that are healthy for longer, based on better monitoring data, etc. Further benefits will also arise from applications based on system monitoring data enriched with other operational data.

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

The concept of a secure edge platform and the technologies used to develop, deploy and secure it will be described in detail in the project reports. Network licensees will be able to use the learning and replicate the concept which is applicable to all licensees.

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

PC based control and monitoring systems tend to have a shorter lifetime than IEDs and will typically be replaced or refurbished every 10 years. The rollout methodology for a secure edge platform would be a deployment together with a control system refurbishment or replacement scheme. Replacing existing operational data reporting and monitoring solutions with this virtualised platform will deliver a saving for each implementation and provide advanced features as described in the project scope above.

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 learning from this project, as documented in the project deliverables, will benefit all network licensees. The results of the research will be documented in the project deliverables and the learning will be made available to all network licensees. Based on the outcomes, other networks can implement these technologies and integrate them into their own solutions.

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

Not applicable

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.

A review of ongoing and previous projects has not shown any duplication with regards to this work. Some cyber security aspects have previously been investigated as part of the CREST project (NIA_NGTO020) and the i40 project (NIA_NGGT0165), however the focus in these projects was on the network architecture and cyber security features. The SEP project will build on the learning from these projects and develop the edge processing infrastructure as well as a proof of concept for edge computing applications for data reporting, enrichment and modelling (CIM), Machine Learning (ML)-based algorithms and remote deployment and management of these applications.

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

Not applicable

Additional Governance And Document Upload

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

Operational data handled by SCADA systems and IoT based asset monitoring systems as well as system monitoring are typically configured as separate security zones and report to separate business systems. Enriching operational data with other sensor data and reporting to subscribing business applications has not been routinely implemented and the cyber security of potential implementations has not yet been assessed in depth. The same applies to remote deployment of automation functions, ML based local or wide area PAC, configuration and device management. Further details about feasibility and cyber security will be required prior to wider rollout.

Relevant Foreground IPR

The foreground IPR created in this project will be embedded in the project deliverables, i.e. the reports, design documentation, requirements specifications, test results, software and demonstrator configuration. The supplier will bring their own background IPR to the project with regards to SCADA, IoT, Machine Learning, data processing, networking, cyber security and substation equipment design. The learning from this project can be used by other licensees without access to the background IPR.

Data Access Details

Data for this project and all other projects funded under the Network Innovation Allowance (NIA), Network Innovation Competition (NIC) or the new Strategic Innovation Fund (SIF) can be found or requested in a number of ways:

- A request for information via the Smarter Networks Portal at https://smarter.energynetworks.org, to contact select a project and click ‘Contact Lead Network’. National Grid already publishes much of the data arising from our innovation projects here so you may wish to check this website before making an application.
- Via our Innovation website at https://www.nationalgrid.com/uk/electricity-transmission/innovation
- Via our managed mailbox box.NG.ETInnovation@nationalgrid.com

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

Operational data handled by SCADA systems and IoT based asset monitoring systems as well as system monitoring are typically configured as separate security zones and report to separate business systems. Enriching operational data with other sensor data and reporting to subscribing business applications has not been routinely implemented and the cyber security of potential implementations has not yet been assessed in depth. The same applies to remote deployment of automation functions, ML based local or wide area PAC, configuration and device management. Further details about feasibility and cyber security will be required prior to wider rollout.

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

Technical risks:

Whilst IoT technologies and ML as well as cyber security technologies have made significant progress in recent years the application to CNI SCADA systems, the integration into current engineering processes and required cyber security measures have not been assessed in detail. Some work on secure remote access has been carried out previously but this area is evolving and requires a more detailed investigation on the risk associated with communication gateways and how this impacts commercial viability. There is also some risk associated with feasibility of efficient remote deployment of ML and rule-based edge processing algorithms that enhance system security and support asset management.

Commercial risks:

The above technical risks contribute to significant uncertainty regarding the effort required to develop and secure more connectivity and leverage the value of enriched data sets, ML enabled edge computing and advanced asset management. This initial proof of concept is aimed at reducing the technical risk and the resulting commercial risk in order to enable further development of BaU innovation solutions for optimised system management and asset management.

This project has been approved by a senior member of staff

- [x] Yes