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

Jul 2024

Project Reference Number

NIA2_NGET0065

Project Registration

Project Title

High Security Control and Protection System

Project Reference Number

NIA2_NGET0065

Project Licensee(s)

National Grid Electricity Transmission

Project Start

July 2024

Project Duration

1 year and 7 months

Nominated Project Contact(s)

Ibukunolu Oladunjoye

Project Budget

£1,100,000.00

Summary

To ensure energy systems of the future continue to be resilient to evolving threats, it is important we develop increasingly secure control systems. Working with vendors, the goal is to innovate and develop efficient, deliverable, and secure protection and control systems capable of mitigating advanced cyber threats using secure by design practices. Lessons learned from this innovation project will enable National Grid to make decisions on the proportionality and appropriateness of security controls for both new and existing sites. This must be achieved while still maintaining the current user experience and meeting control/protection functionality specifications, all in a system designed to match the lifecycle of current systems of approximately 20 years.

Nominated Contact Email Address(es)

box.NG.ETInnovation@nationalgrid.com

Problem Being Solved

National Grid faces a variety of threats in operating Critical National Infrastructure. To ensure energy systems of the future continue to be resilient to these evolving threats, it is important we develop increasingly secure substation control systems leveraging best practice standards.

Designing, building, and implementing control systems can take years. For this reason, to date, National Grid has opted to incrementally improve security specifications once specific capabilities are proven.

As National Grid works with Original Equipment Manufacturers (OEMs) to develop products capable of meeting these requirements there will be challenges in both design and implementation. Introducing security controls to even greenfield implementations can cause unforeseen issues in designing, implementing, operating, and maintaining control systems. Introducing new security control increases new complexity and thought must be given to both time-saving automation and effective support models. Any changes need careful consideration to determine their proportionality and ensure minimal impact on the safety, resilience, and cost of our energy networks.

Method(s)

Work Pack 1 (part of this project):
National Grid will provide a Conceptual Cybersecurity Requirements Specification to support design works. The selection process will include submissions detailing bills of material, conceptual cyber security design specifications including conceptual system architecture, budgetary cost and schedule estimates, relevant certifications and how vendors propose to meet each of the National Grid specified controls with evidence of previous implementations and current and future cost implications.

Scope

Key deliverables for the project are:

- Producing a refined view of National Grid defined controls, including proposed vendor design, implementation approach, proposed costs, support model and previous examples. Noting where implementations conflict with existing Transmission Standards or exceptions must be made against security requirements. In achieving this, there will be enhanced confidence in the robustness and adherence to standards of the control systems being developed, ensuring the systems are designed and implemented with consideration for industry best practices, minimising the risk of vulnerabilities and potential disruptions to services.
- Developing a Functional Design Specification which should additionally include highlighting the impact of implementing the security controls on the control system's operational functionality. The Functional Design Specification will ensure the implementation of security controls do not compromise the operational functionality of the control system. This means that consumers can continue to rely on the system's performance and functionality while enjoying the added protection and security measures in place.

Objective(s)

- Inform proportionate decision making on the specification and assurance of new control systems and their lifecycle.
- Enhance OEM product offerings by providing higher security alternatives.
- Gain a better understanding of the risk and threat environment facing National Grid's substation control systems. Risk scenarios will be tested during the commissioning of the control systems to demonstrate resilience and make iterative improvements.
- Determine the complexities of implementing a high security control system and challenges in scaling to the wider estate. If organisational change is required, we will be able to uncover this and begin the process of closing those gaps.
- Develop National Grid's internal skills and capabilities to build increasingly secure control systems.
- Collaborate with partners to modify existing policies and standards.
- Gain wider recognition as an industry-leading Security function in the energy sector.
- Protecting the confidentiality, integrity, and availability of control systems, reducing the risk of costly security breaches and downtime.
- Enhancing incident response and incident recovery processes by testing forensics tools and developing comprehensive documentation.

Consumer Vulnerability Impact Assessment (RIIO-2 Projects Only)

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.

Success Criteria

1. Decision makers will have access to comprehensive and up-to-date information on control system specifications and assurance, enabling them to make informed decisions that align with National Grid's objectives and risk appetite.
2. OEMs offer improved and more secure product options that meet National Grid's requirements, resulting in increased security and reduced vulnerabilities in control systems.
3. National Grid has a comprehensive risk driven design.
4. National Grid identifies complexities and challenges associated with implementing a high-security control system and scaling it across the wider estate. This understanding allows National Grid to address changes, close any identified gaps, and ensure successful implementation.
5. National Grid's workforce identifies the necessary skills and capabilities to design, develop, and implement increasingly secure control systems, resulting in improved security measures and reduced vulnerabilities.
6. National Grid collaborates effectively with partners to modify existing policies and standards, ensuring alignment with industry best practices and enhancing the overall security posture of control systems.
7. National Grid's Security function continues to be widely recognised as an industry leader in the energy sector, demonstrating expertise in control system security and contributing to the advancement of security practices in the industry.
8. Substation control systems are effectively protected, ensuring the confidentiality, integrity, and availability of critical assets. This results in a reduced risk of security breaches and costly downtime.
9. Incident response and recovery processes are improved through testing and refinement of forensics tools, as well as the

development of comprehensive documentation. This leads to more efficient and effective incident management and recovery.
10. National Grid successfully continues to meet regulatory compliance requirements, including those outlined in the Network & Information Systems Regulation.

Project Partners and External Funding

None

Potential for New Learning

Recognising the security risk this project poses if certain outputs are shared, a filtered version will be disseminated.

Scale of Project

The scale of this project involves the following:

Data collection and processing
Presentation and documentation
Development of the 'secure by design' design specifications
Running a tendering exercise for interested parties to produce a control system meeting the specifications of the design requirements.

The project scope and actions can be classed as a desktop exercise.

Technology Readiness at Start

TRL4 Bench Scale Research

Technology Readiness at End

TRL7 Inactive Commissioning

Geographical Area

Work Pack 1 is a desktop exercise.

Revenue Allowed for the RIIO Settlement

N/A

Indicative Total NIA Project Expenditure

£990,000

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:

This proposal facilitates energy system transition by acting to protect digitalised assets on the network, which are a major factor in decarbonising the transmission system.

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

Introduce new and emerging security capabilities within our substation protection and control systems and leverage these solutions in our designs to increase the resilience of our energy networks and protect our customers and vulnerable consumers from outages caused by cyber attacks.

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 benefit duration has been assumed to be 10 years given the control system lifecycle is 15 years. We would expect to need to explore refreshing some controls at this stage which may impact the full lifespan of the benefits. NPV Baseline cost is before any innovation cost is calculated from the CBA innovation spreadsheet. The risk cost is £2.8m per year and for a span of 10 years results to £26.3m (considering the future value – as per NPV value – cash in flow and out flows over a period of time.)
NPV cost if the innovation is implemented is £14.5m which includes the £3.1m innovation project cost.
Based on our cost benefit analysis, the estimated benefits of the project by 2032 in NPV (Net Present Value) will be around £11.8m if the project is successful.

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

National Grid has about 350+ substations and deployment of a High Security Control System can be implemented across all sites in time.

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

At this early stage, the costs of deploying the new control system would be an estimated additional 5% upfront and 2.5% increased running costs (post-delivery support etc). The actual cost will be known as the project develops and more learning is captured on the new systems being proposed.

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

Lessons learned and requirements can be applied by other Network Licenses to help inform secure by design decisions on their own control system deployments.

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

Please demonstrate how the learning from the project can be successfully disseminated to Network Licensees and other interested parties.

Virtual closed workshops, i.e virtual only-invite workshops
Redacted paper (e.g white paper) made available on request from licences

Please describe how many potential constraints or costs caused, or resulting from the imposed IPR arrangements.<

There are no constraints or additional costs

Please justify why the proposed IPR arrangements provide value for money for customers.

This project aims to determine a proportionate set of security controls for our energy network in order to provide customers value for money. Making National Grid specific design IP available publicly to vendor customers around the world could pose a risk to the security of the UK energy networks.

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 is no awareness of any similar project that uses a ‘secure by design’ design philosophy to develop a High Security Control System as described in the scope of this project.

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

Role based access control (RBAC) is a common technology in IT systems. However, it is not widely used in electric utilities Operational Technology (OT) spaces because it requires additional communications and standardization. The standard for that application (IEC 62351-8) was initially released in 2020.

Even though it relies on common technologies, devices have begun to adhere to the new specifications recently and therefore an early investigation into how the technology can be applied to Electricity Transmission substations needs to be conducted to ensure the right choices are made.

The project aims to introduce innovation by applying new concepts, design philosophies, and testing activities to control and protection systems. The primary goal is to implement a High Security Control System. While some of these technologies may already be in use, we propose integrating a suite of new and untested functions and technologies into a single holistic solution. This approach may involve the introduction of new hardware and software solutions. Any changes made must be carefully considered to ensure minimal impact on the safety, resilience, and cost of our energy networks.

Relevant Foreground IPR

The following IPR will be generated by this project:

- Updated National Grid Specifications
- Generated Requirements Documentation
- A forecast predicted state for substations
- A report which articulates the pros and cons, and lessons learned
- Risk modelled architectures

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

Due to the nature of this project the outputs will need to be de-sensitised to avoid introducing a security risk.

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

Design changes may put at risk in-flight projects that are essential for meeting the changing energy requirements. Due to these challenges, National Grid has chosen to enhance security specifications gradually once specific capabilities have been validated. The objective of this project is to develop a state-of-the-art control system, designed with security in mind, as a test platform. The purpose is to identify which controls can be successfully implemented in the BAU systems.

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 project involves considerable research, development, and proof of concept, making it fit well as an innovation project.

This project has been approved by a senior member of staff

- [x] Yes