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

May 2020

Project Reference Number

NIA_NGTO054

Project Registration

Project Title

Cyber Security Solutions for Legacy Equipment

Project Reference Number

NIA_NGTO054

Project Licensee(s)

National Grid Electricity Transmission

Project Start

September 2020

Project Duration

0 years and 8 months

Nominated Project Contact(s)

Thomas Charton

Project Budget

£92,000.00

Summary

While it is well recognised that IEC61850 based fully digital substation technologies can deliver great benefits to power utilities and their customers, the existing legacy equipment will continue to play a crucial role to support the critical power infrastructure for the remainder of its service lifetime, especially substation protection and control systems. Since legacy equipment was originally designed for use on dedicated or closed networks and therefore contains little or no cyber security features.

Even though they perform critical functions managing power grid and communication networks, most are lacking crucial features for access control and device hardening. Many of these devices cannot be easily updated with new firmware to include security and replacing them with new secure versions will take years. Hence a risk assessment and detailed review of options for improved cyber security for legacy equipment to stop any cyber-attack are urgently required. In this context, we consider legacy equipment all assets that have been delivered prior to the implementation of our architecture for secondary substation systems.

Nominated Contact Email Address(es)

box.NG.ETInnovation@nationalgrid.com

Problem Being Solved

While it is well recognised that IEC61850 based fully digital substation technologies can deliver great benefits to power utilities and their customers, the existing legacy equipment will continue to play a crucial role to support the critical power infrastructure for the remainder of its service lifetime, especially substation protection and control systems. Since legacy equipment was originally designed for use on dedicated or closed networks and therefore contains little or no cyber security features.

Even though they perform critical functions managing power grid and communication networks, most are lacking crucial features for access control and device hardening. Many of these devices cannot be easily updated with new firmware to include security and replacing them with new secure versions will take years. Hence a risk assessment and detailed review of options for improved cyber security for legacy equipment to stop any cyber-attack are urgently required. In this context, we consider legacy equipment all assets that have been delivered prior to the implementation of our architecture for secondary substation systems.

Whilst significant progress is made both in terms of research but also development and commercial availability of enhanced cyber security for operational technology, the existing asset base is typically a mix of old and new equipment at any one time. Protection, automation and control equipment has a typical service life time of 15 to 20 years and in particular older devices, whilst providing network, USB or other interfaces do not have the same level of cyber security features we are now rolling out with new equipment.

Managing the overall cyber security risk our networks are exposed to will depend to some extent on how well we are able to improve the security of existing legacy equipment.

Method(s)

In order to address the challenge of securing legacy protection, automation and control equipment we will carry out a desktop based investigation into cyber security risk and risk assessment methodologies. The study will particularly consider the different vintages of equipment and investigate new ways of establishing a risk assessment framework as well as options for overall risk mitigation and management.

Some laboratory based testing and validation of risk mitigation methods may be included if the opportunity arises. This would require access restrictions to lab space to be lifted and some collaboration from our supply chain partners.

Scope

Deliverables:

Review and report on literature dealing with cyber security, including cyber security issues and the existing potential cyber solutions for legacy equipment, including assessment of commercially available products in the field, and experience of deployment by other utilities.

· Review of current population of Protection, Automation and Control (PAC) solutions and relevant technologies used in NGET, and develop and carry out risk assessment for current legacy equipment,

· Develop methods, including options of using off-the-shelf products as well as novel ideas in terms of technology, processes and configurations to address cyber security issues for legacy equipment, considering in particular the implementation of IEC62351 and 62443 and providing implementation guidance

· Option assessment and ranking considering residual risks, asset lifecycle and cost benefit,
Main report on project, including sub-reports, presentations and dissemination of results (as far as appropriate) delivered during the project.

Objective(s)

The aim of this project is to

· investigate and develop methodologies for cyber risk assessment

· assess risk levels for P&C equipment, in particular legacy equipment

· understand the currently available options to improve security and develop new ideas and concepts capable of improving security for legacy equipment in a cost-effective way.

· assess options and make recommendations based on a CBA

The investigation will refer to and build on the ongoing work in the CREST project (NGTO020) and in particular the cyber security requirements and implementation guidance for IEC standards 62351 and 62443. The project will provide guidance on how to apply these standards to the relevant vintages of P&C equipment.

Consumer Vulnerability Impact Assessment (RIIO-2 Projects Only)

n/a

Success Criteria

If successful, this project will deliver the following key outcomes:

§ A framework for cyber security risk assessment, in particular considering legacy equipment and technologies.

§ Risk assessment and categorisation of cyber assets

§ Option assessment and ranking for cyber security related asset interventions including CBA

§ Implementation guidance considering relevant standards

Project Partners and External Funding

n/a

Potential for New Learning

The project will generate new learning for utilities with guidance on how to secure older assets that can not be cyber hardened in the same way as new equipment. The types of existing legacy equipment managed by network licensees is to a large extent similar and the learning will be transferrable to other networks.

Scale of Project

The project will be a desktop study with some laboratory trials where the opportunity arises. This is appropriate for this type of project. It is very likely that the learning will lead to a wider rollout of the cyber security measures identified in this project across GB networks. This is likely to be handled separately, outside the NIA framework.

Technology Readiness at Start

TRL2 Invention and Research

Technology Readiness at End

TRL3 Proof of Concept

Geographical Area

The work will desk based research with potentially some laboratory trials.

Revenue Allowed for the RIIO Settlement

None

Indicative Total NIA Project Expenditure

£92,000

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:

n/a

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)

A widely-recognised framework for monetised risk for cyber security has not been developed yet for our industry. This project will develop a risk model and framework that can contribute to a robust methodology for CBA for cyber security. The risk of compromised cyber security can range up to a country-wide blackout which would cost potentially several days of GDP. Mitigating this huge risk will deliver large benefits to consumers.

Please provide a calculation of the expected benefits the Solution

N/A - Research Project

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

The learning from this project will provide Network Licensees across GB with guidance of how to mitigate the residual cyber security risk posed by legacy protection automation and control equipment. It is estimated that this type of equipment can be found in approximately >80% of substations.

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

The costs of a wider rollout depend on the measures identified in this research. A CBA will be developed to score and rank the options. At this stage it is not possible to quantify the cost for any potential measures yet.

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

☐ 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 outcomes from the project will be available to the general public via the ENA portal and it will be presented during dissemination meetings or events such as conferences or journal publications. The learning from this project is relevant to all GB licensees due to commonalities in equipment types and a common need to deliver enhanced cyber security.

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

This project fits within the Managing Assets value area of the Electricity Innovation Strategy.
☑ Has the Potential to Develop Learning That Can be Applied by all Relevant Network Licensees

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.

To the best of our knowledge, this work has not been conducted before. This review has included the ENA smart portal, and supply base (including Universities and EPRI)

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

The project will evaluate innovative solutions to mitigate cyber security risks which could avoid early replacement of cyber assets. The industry focus within the supply chain as well as research has been on new features and equipment however legacy equipment is likely to pose the greater risk.

Relevant Foreground IPR

n/a

Data Access Details

n/a

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

activities

The nature of a research programme means it inherently carries a risk that the research may be unsuccessful or identify unforeseen challenges/costs to implementation. The NIA funding offers the most appropriate route for the National Grid Electricity Transmission (NGET) to assess the cyber risk of legacy protection automation and control equipment and the learning can be applied to all Network Licensees.

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 inherent risk of the project is detailed above and the learning from the project will be directly relevant to all Network Licensees. For this reason, NGET believes this project is appropriately funded through NIA, and material from the project will be available to the general public via the ENA portal.

This project has been approved by a senior member of staff

- [x] Yes