national gas transmission

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 2018

Project Reference Number

NIA_NGGT0138

Project Registration

Project Title

Secure AGI – Intrusion Detection System (IDS)

Project Reference Number

NIA_NGGT0138

Project Licensee(s)

National Gas Transmission PLC

Project Start

October 2018

Project Duration

1 year and 8 months

Nominated Project Contact(s)

Jeremy Hunns

Project Budget

£1,215,000.00

Summary

To develop a compact and low cost hard cyber module for AGI's. Will provide an open source (s/w) solution to ensure future proofing of the cyber protection of the NTS SCADA assets.

Nominated Contact Email Address(es)

Box.GT.Innovation@nationalgrid.com

Problem Being Solved

The Network and Information Systems (NIS) Directive 2016 (as transposed into UK law by way of the Network and Information Systems Regulations 2018) places a legal requirement on operators of essential services (OES) requiring them to "...take appropriate and proportionate technical and organisational measures to manage risks posed to the security of the network and information systems on which their essential service relies."

Currently there are a number of large IT Intruder Detection Systems (IDS) in the market, however these solutions are designed predominantly to service large scale IT networks, rather than smaller distributed OT networks used in the ICS space. These systems cost in excess of £100k per unit, making them uneconomical for smaller remote sites including Above Ground Installations (AGIs).

This project will seek to design a vendor agnostic IDS solution with remote telemetry unit (RTU) technology that has the capacity to offer standardised control and protection functionality and can be retrofitted into existing AGIs to allow early notification of cyber-attack incidents.

Method(s)

The project will develop and deliver the following key outputs:

- Research and develop an open source modular platform which can be used to host an IDS on AGI sites as an alternative to the existing large-scale IT solutions.

- Develop an IDS which can be operated on low-cost, commercial off the shelf (COTS) hardware.
- Create a process-specific ruleset and establish trigger points based on the status of the plant within the trial AGI.
- Vendor-neutral IDS solution, ensuring independence between the open source IDS software and hardware.
- A standardised solution which can be used on all AGI sites.
- Centrally managed and coordinated system which can be maintained and updated remotely from the National Grid Security Operations Centre (NG-SOC).
- Alignment with National Grid cyber security strategy.
- The solution will create a significantly lower number of false alarms than traditional IT IDS solutions, therefore allowing the NG-SOC to focus on the significant events only.
- The inclusion of telemetry functionality to allow for future system replacements at a significantly lower cost than existing Remote Telemetry Units (RTU).
- The inclusion of control and protection capability.
- Ownership of the solution will be retained by National Grid, therefore ensuring that the architecture is deployed on any new site installations.

The Secure AGI programme has been structured to be delivered in two parts with a stage-gate in-between with an aim to ring fence sanction exposure in the event of any technological difficulties.
Part 1: Design, build and trial a vendor agnostic IDS solution which uses network and real-time process data and which can be retrofitted into existing AGI's to allow early notification of cyber-attack incidents.

- Scope and Specification.
- Design of solution and development of the rulesets.
- Deployment and data analysis including validation and refinement.
- STAGE GATE

Part 2: Integration of the RTU requirements within the IDS to allow for single device to remotely monitor, control and protect (with standard logic) the installation in accordance with IEC-61131.

- Design of solution and development of RTU technology.
- Design of solution and development of Control and Protection functionality.
- Deployment and data analysis including validation and refinement.

Scope

Cyber security is becoming an ever-increasing challenge for operators of critical network infrastructure assets. The industrial control systems (ICS) utilised in them play a crucial role in managing and operating the gas transmission system as part of the critical national infrastructure across the UK.

ICS has evolved over several decades, utilising technology borrowed from business computing and communications, standard computer software programming languages and techniques. This has resulted in the systems being hosted on existing aging and vulnerable communication technology in the operational technology (OT) space, such as Modbus RTU, satellite uplinks, PSTN and ISDN. As well as upgrading these assets, there is significant pressure to find a way to secure these new and legacy technologies against cyber-attacks in a cost-effective manner offering the least impact on site operations.

Whilst the enterprise IT industry has developed robust methodology and systems to counter emerging threats within their sector, the rate of development for cyber resilience by manufacturers of ICS has not kept pace. This is mainly a result of early cyber threats being focused on the enterprise IT rather than OT systems.

One mitigation measure that has been deployed in large IT enterprise scenarios are intruder detection systems (IDS). Currently there are a number of large IT vendor IDS platforms in the marketplace, however their solutions are based on large scale central IT networks, rather than smaller scale and more specialised OT networks used in the ICS space. These systems are expensive, making them uneconomical for remote sites such as AGI's.

The proposed approach requires significant knowledge of ICS network and system behaviour and of the general characteristics that a malicious intrusion might exhibit. This type of proactive monitoring or threat discovery would typically involve:

- Designing bespoke alerts or trip-wires, using experience or reasoning based on the engineering / domain knowledge, of what an intrusion might do with the physical assets to disrupt the asset owner's business, rather than specifically around what past attacks have done
- A good understanding of normal system behaviour through the OT design engineering expertise. For example; what software is authorised and how it would normally behave, how technical and operational individuals normally access network resources or how network components connect to each other and transfer data
- A good understanding of the ways that different types of anomalies might signify a malicious intrusion, based on a comprehensive and advanced understanding of the OT attack surface and threat intelligence.

The project also aligns to corporate strategy in the areas of:

- Safety – addressing cyber security challenges within process safety.
- Security – increasing the robustness of the cyber security strategy, to comply with NISD legislation.
- Efficiency – retaining control of proprietary systems to reduce lifecycle costs.

Objective(s)

To engineer a fit-for-purpose ICS intruder detection system solution, with inbuilt RTU, control and protection functionality, which will be tailor-made for use in a live AGI environment.

Consumer Vulnerability Impact Assessment (RIIO-2 Projects Only)

n/a

Success Criteria

This innovative project seeks to design and develop a standard ICS intruder detection system using open source technology that removes the complexities and demonstrates reduced TOTEX costs currently associated with traditional IT-focused IDS solutions. The finalised solution will:

- Detect and prevent cyber security attacks on remote operated assets
- Have little impact on the total cost of ownership of the current ICS systems
- Provide a low cost and scalable solution
- Require no or little additional physical space on site
- Provide cyber security threat information to National Grid's CSOC (Cyber Security Operational Centre)
- Ensure that an intruder detection solution can be designed with similar detection capabilities of that which is currently used in the IT enterprise solution.
- Provide successful RTU functionality.
- Provide successful control and protection functionality.

In addition to the solution meeting each of the objectives listed above, the following measures of success shall be applied to the project:

- Smart detection of intrusion on an AGI using the OT design documentation and real-time process conditions in combination with the ICS network traffic.
- Cost effectiveness: achieved through COTS and open source technology.
- That the solution is vendor agnostic: achieved through COTS and open source technology.
- The system ownership and retained control over the system via an open source solution can be maintained by National Grid.

Change Control - February 2020:

- The project was initially due to be trialled at one NG location and was due to finish end of 2019.
- Hardware was procured, site design activities and system development for original location commenced and was close to being finalised.
- It became apparent late last year that the original site location was no longer a viable option for project trial site.
- A project decision was taken to re-deploy the trial to an alternate site, subject to survey and risk assessment.
- New site requires additional development work to include the Profibus Technology Protocol (to make everything communicate correctly).

Further engineering and system development undertaken/in flight to allow for the late change in trial site and ensure successful delivery of the project.

This change control will:
Increase the project external costs to £62k to cover the additional work involved; therefore, increase the total project budget to a new total of £1,215,000.

Extend project date until 31st March 2020.

- Considers the additional development work and time for the final technical report to be received and reviewed by NG.

Project Partners and External Funding

Project Partner – Lagoni Engineering Ltd.

External Funding – (nil)

Potential for New Learning

The project will provide a genuine insight into the use of open source technologies and low-cost hardware in the fields of cyber security and remote telemetry. The fundamental basis of the programme will inform the debate as to the suitability of this approach for all other National Grid above ground infrastructure (AGI) infrastructure and adoption by the distribution network operators.

Scale of Project

The project will develop the IDS platform with additional functionalities on a nominated National Grid Gas Transmission above ground installation site.

Technology Readiness at Start

TRL6 Large Scale

Technology Readiness at End

TRL8 Active Commissioning

Geographical Area

All work will be conducted in the UK and only involve Gas Transmission assets.

Revenue Allowed for the RIIO Settlement

None

Indicative Total NIA Project Expenditure

£1,215,000.00

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)

£19.35m - £26.35m

Please provide a calculation of the expected benefits the Solution

National Grid Gas Transmission has 180 critical AGIs where, during RIIO-T2, it is likely that an Intruder Detection System (IDS) solution will be deployed.

The current large-scale IT IDS systems which are available would cost between £100k and £150k per site following site-specific amendments being made. The proposed solution aims to reduce the cost of hardware and installation for this system to between £10k and £25k per site, allowing for the potential future requirement for RTU and standardised control and protection functionality.

Currently Available Solutions:
£125,000/site

£125,000 x 180 sites = £22.50m

Proposed Solution:
£17,500/site

£17500 x 180 sites = £3.15m

Base – Method:
£22.5m – £3.15m = 19.35m

Total saving = £19.35m

Should the decision be made in the future to utilise the RTU / Control and protection functionality on all 180 AGIs, a further £9.0m CAPEX saving is available, as the proposed IDS solution has been future proofed for this inbuilt capability.

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

In addition to the 180 critical NGGT AGI sites, there are a significant number of distribution sites that could also potentially benefit from this solution.

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

To roll the solution out on all NGGT AGIs, the indicative costs are in the range of £2.65m - £6.63m

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 offer an Intruder Detection System solution which is suitable for deployment on AGI sites within the transmission and distribution networks.

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

The project aligns with NGGT's Data & Cyber Innovation Strategy objective and cyber deployment reducing challenges posed by the use of legacy RTU technology.

☑ 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.

The current NIA portfolio of other gas distribution networks does not indicate similar type of programme. All networks will be fully informed of the progress of the current initiative.

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 innovation for this project is the adoption of open source SCADA technology for the basis of a cyber intrusion detection system utilising commercially available off the shelf hardware, as opposed to OEM equipment, which is a concept that has never been developed for gas transmission or distribution assets before. The provision of a tailor-made IDS solution for use on AGI sites, with the added benefit of RTU, control and protection functionality, offers considerable benefits not only to NGGT, but to DNOs also. The creation of a customised process-specific ruleset will remove the significant number of false alarms which would be generated by the adoption of a large-scale, generic IT solution. This solution will ensure that the latest defences against cyber security attacks can be used to protect these critical assets.

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 NIA funding offers the most expedient route for NGGT to evaluate the technology with a carefully controlled and ring fenced programme. Only this approach will enable NGGT to develop and test the IDS system without it being compromised by the needs of business as usual programmes which require tested and proven business ready solutions at the time of installation.

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 Network and Information Systems (NIS) Directive 2016 (as transposed into UK law by way of the Network and Information Systems Regulations 2018) places a legal requirement on operators of essential services (OES) requiring them to “...take appropriate and proportionate technical and organisational measures to manage risks posed to the security of the network and information systems on which their essential service relies.” The latest advancements of open source technology potentially offer considerable benefits to NGGT and other network operators if their capabilities are proven and would help NGGT to comply with the NIS Directive 2016, hence meeting technical, operational and regulatory requirements. The open source solutions to be utilised in this project are widely used in the cyber security community and are chosen for this innovation project to demonstrate that they provide a fit for-purpose solution in the operational technology (OT) space, which can be proven to be cost effective and leverage benefits of non-OEM tied solutions. The risks of not carrying out this programme into the potential application of this open-source cyber security technology are that the government may change their stance on current legislation and impose stricter cyber security targets that National Grid may not be able to react quick enough to. A full capability assessment requires a dedicated programme of evaluation by the relevant technical experts. Innovation funding provides a robust framework that enables these assessments to be undertaken and ensures that all the necessary updating of procedures and standards are captured and approved, decreasing the business implementation time. Innovation funding ensures the dissemination of the generic findings are communicated to all networks which improves efficiency and ensures that relevant proven commercially available off the shelf equipment is considered to enhance cyber security as opposed to OEM based solutions.

This project has been approved by a senior member of staff

- [x] Yes