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

Nov 2016

Project Reference Number

NIA_NGET0189

Project Registration

Project Title

Security Assessment of Industrial Control Systems (ICS)

Project Reference Number

NIA_NGET0189

Project Licensee(s)

National Grid Electricity Transmission

Project Start

June 2016

Project Duration

1 year and 4 months

Nominated Project Contact(s)

Stuart Mann

Project Budget

£342,000.00

Summary

This project will develop a systematic process specifically targeting devices utilised for the Electricity Transmission System ICS. To identify potential results of cyber-attacks designed to exploit vulnerabilities in the devices and systems deployed in electricity substations. The process and tools utilised in cyber-attacks are likely to evolve expressly from those currently employed in the business IT world.

A significant amount of technology used in ICS is based on common worldwide open industry standards. It is envisaged that the processes and tools produced by this project will be relevant to other Critical National Industries participating in a wider SCEPTICS (A SystematiC Evaluation Process for Threats to Industrial Control Systems) programme of work with EPSRC, and will form a foundation that can be developed further by industry peers around the world.

As vulnerabilities, exploits, threat actors and outcomes are understood within this study, this information will be used to develop and implement actions formulated specifically for the GB electricity transmission system to provide effective defences or resolution to issues.

The project shall undertake the following tasks:

- Utilise intelligence, cyber testing techniques and methodologies available in the public domain to identify vulnerabilities that are present in and exposed by equipment or systems in use on the GB Electricity Transmission Network.
- Determine how vulnerabilities may be exploited and used to compromise the integrity of the Electricity Transmission System.
- Identify the potential impact that exploits may have on the reliability or stability of the Electricity Transmission System.
- Use the output from the project to determine who could take advantage of these vulnerabilities, why they may be exploited and the method used to undertake these actions.
- Provide a framework and methodology to facilitate repeatable risk assessments to be periodically undertaken.

Nominated Contact Email Address(es)

box.NG.ETInnovation@nationalgrid.com

Problem Being Solved

The Industrial Control Systems (ICS) utilised by National Grid play a crucial role in managing and operating the electricity transmission system as part of the Critical National Infrastructure across Great Britain, balancing supply with demand on a minute by minute basis while ensuring that the network is operated safely, reliably and cost efficiently.

ICS has evolved over several decades. Utilising technology borrowed from business computing and communications, standard computer software programming languages and techniques. As well as published open worldwide standards for communications technology and protocols as part of an industrial and electrical environment hardened electronic device package. Because of this technology overlap, ICS systems are increasingly cyber physical.

Whilst the business IT industry have developed robust methodology and systems to counter emerging threats within their sector, the rate of development for cyber resilience by manufacturers of ICS have not kept pace. The result is that ICS, and the businesses that use them, are increasingly vulnerable to cyber-threats and exploit techniques which initially evolved from those developed and found within the business IT industry.

Despite the availability of some well-founded knowledge and experience, there remains a significant lack of comprehensive understanding of the vulnerabilities and exploits that exist on ICS, the consequences of exploitation, and therefore the resolutions or mitigations that need to be implemented. Industry partners across Great Britain recognise that the resilience of technology, design and implementation practice associated with products in current use may be insufficient. There is, therefore, a relevant need for research that will bridge this gap of understanding, particularly as it relates to the use of ICS on power grids.

Method(s)

Industrial Control Systems typically comprise of a selected combination of a significant number of available devices and systems from a large variety of suppliers. A basic summary of devices available include wide area Supervisory Control And Data Acquisition (SCADA) systems, local area Distributed Control Systems (DCS), and a range of embedded devices such as Programmable Logic Controllers (PLC). Large ICS are characterised by their complexity. Including a wide range of control devices, sensors and network configurations, many of which are now legacy technology. For National Grid, these include the addition of devices to protect, supervise and manage the high voltage equipment that comprises the GB Electricity Transmission System (ETS), and to protect connected customers from system or natural events like equipment failures or lightning strikes. The management frameworks for these systems can often be equally complex. Vulnerabilities in ICS can be a result of this complexity combined with the use of legacy systems.

Because the capability exists to find and potentially exploit vulnerabilities of the ICS, it is relevant that National Grid undertake analysis of threats and understanding of any consequences resulting from exploitation. This method of research must take into account the physical properties of the Electricity Transmission System as well as the physical consequences of exploitation. Limited measures have been implemented and are periodically reviewed. However, in light of current understanding of, and the continuing advancements in technology, it is judicious to investigate and fully understand the vulnerability of ICS to ensure appropriate measures are taken in order to mitigate and counter the risk of cyber-attacks. In undertaking this research, National Grid hopes to achieve a greater understanding that will ultimately lead to a common and adaptable process for ongoing identification mitigation and resolution of these issues.

Scope

This project will develop a systematic process specifically targeting devices utilised for the Electricity Transmission System ICS. To identify potential results of cyber-attacks designed to exploit vulnerabilities in the devices and systems deployed in electricity substations. The process and tools utilised in cyber-attacks are likely to evolve expressly from those currently employed in the business IT world.

A significant amount of technology used in ICS is based on common worldwide open industry standards. It is envisaged that the processes and tools produced by this project will be relevant to other Critical National Industries participating in a wider SCEPTICS (A SystematiC Evaluation Process for Threats to Industrial Control Systems) programme of work with EPSRC, and will form a foundation that can be developed further by industry peers around the world.

As vulnerabilities, exploits, threat actors and outcomes are understood within this study, this information will be used to develop and implement actions formulated specifically for the GB electricity transmission system to provide effective defences or resolution to issues.

The project shall undertake the following tasks:

- Utilise intelligence, cyber testing techniques and methodologies available in the public domain to identify vulnerabilities that are

present in and exposed by equipment or systems in use on the GB Electricity Transmission Network.

- Determine how vulnerabilities may be exploited and used to compromise the integrity of the Electricity Transmission System.
- Identify the potential impact that exploits may have on the reliability or stability of the Electricity Transmission System.
- Use the output from the project to determine who could take advantage of these vulnerabilities, why they may be exploited and the method used to undertake these actions.
- Provide a framework and methodology to facilitate repeatable risk assessments to be periodically undertaken.

Objective(s)

The objective of this project is gain a more comprehensive understanding of the vulnerabilities and exploits that exist on Industrial Control Systems. This includes the consequences of potential exploitation and the resolutions or mitigations which can be implemented. This research will inform the development of a systematic process that can evaluate the types of ICS devices that monitor, control and protect the GB electricity transmission system and connected customers to identify and understand risks and delivery vectors that these systems are exposed to.

Consumer Vulnerability Impact Assessment (RIIO-2 Projects Only)

n/a

Success Criteria

Learnings gained from the research undertaken in this project will inform National Grid on the following:

- Provide input and influence National Grid strategy, policy and specifications on ICS
- Provide direction to support effective and efficient investment decisions to protect the transmission Network from cyber-threats
- Provide a basis to drive development of international common standards for cyber security of ICS
- To influence change in technology implemented and marketed by equipment manufacturers

Project Partners and External Funding

n/a

Potential for New Learning

n/a

Scale of Project

This is the first time a systematic process for the evaluation of the critical ICS equipment and systems that National Grid use will be undertaken in the UK. The research and development of the process is predominantly laboratory and desk based which will mirror the expected environment when the output is utilised after project completion.

Technology Readiness at Start

TRL3 Proof of Concept

Technology Readiness at End

TRL5 Pilot Scale

Geographical Area

The research and modelling activity will primarily be desktop based, located in the Midlands.

Revenue Allowed for the RIIO Settlement

None

Indicative Total NIA Project Expenditure

The total NIA project expenditure will be £300,000 (this excludes the EPSRC contribution of £42,000)

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)

The outputs of this innovation project will reduce exposure to cyber exploit and provide a more resilient system through the mitigation and removal of exploitable cyber vulnerabilities. Financial benefits are expected to be primarily derived from avoidance of costs, which is estimated at ~£2m annually, associated with the prevention of a cyber-attack.

Please provide a calculation of the expected benefits the Solution

Not applicable – this is primarily a research project.

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

The methods developed as an output of this project will provide industry across GB with a more informed understanding into the specific cyber vulnerabilities and threats targeted at electricity systems. The knowledge gained will inform key strategic and investment decisions in respect to mitigating or resolving the cyber threats to which network licensees are exposed.

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

The systematic process developed within this project will form part of an initial cyber evaluation process. A continuous re-evaluation process to monitor the changing vulnerability and threat landscape will follow, as the outputs will be used to determine the actions that need to be undertaken by National Grid, and whether there is further need to develop, change, and amend mitigation and resolution strategies currently in place.
Roll-out will be undertaken in several stages over a number of years. It is anticipated that the initial evaluation process will cost an estimated £300k, and will including resource training, evaluation of equipment currently on the network to determine vulnerabilities in-line with the SCEPTICS model, implementing controls relative to the systems tested, the procurement of equipment, and data capture of device information on the asset management inventory for future evaluation purposes.

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 learnings developed within this project can be used to support the need for, and drive improvements of the devices and systems provided specifically for the electricity transmission industry in the form of specifications and testing methodologies.

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 corporate responsibility, managing assets value area of the Electricity Transmission Owner 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.

n/a

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

n/a

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

n/a

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

n/a

This project has been approved by a senior member of staff

- [x] Yes