nationalgrid

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

Jun 2016

Project Reference

NIA_NGET0190

Project Registration

Project Title

EPRI Research Collaboration on Cyber Security 2016 (P183)

Project Reference

NIA_NGET0190

Project Licensee(s)

National Grid Electricity Transmission

Project Start

June 2016

Project Duration

0 years and 11 months

Nominated Project Contact(s)

Mukund Ravipaty

Project Budget

£2,123,819.00

Summary

Several projects form the overall EPRI P183 work package, which are delivered in tandem:

1. Deliverable P183A: Industry Collaboration & Technology Transfer - the landscape of cyber security activities in the UK electricity sector involves numerous industry, government, and regulatory groups. Although tracking these groups can be a daunting effort, it is critical for utilities to be up-to-date on key industry activities. This deliverable provides members with an up-to-date view of industry activities and supports technical contribution to these groups.

2. Deliverable P183B: Security Technologies - this deliverable will address several security technology challenges facing UK power-delivery and control systems, such as developing protective measures and managing cyber threats.

3. Deliverable P183D: Information Assurance - this deliverable focuses on security challenges that affect multiple operations domains, such as designing security into products, creating security metrics for the UK electricity sector, and developing technical solutions for meeting security compliance requirements.

The work packages have deliverables that span across multiple years to complete, therefore not all of them will be completed at the end of 2016. Among the key expected areas of progress in 2016 are:

- Active participation by National Grid Digital Risk & Security in reviewing resulting deliverables and applying them internally to key processes, technological improvements supporting the Critical National Infrastructure for the UK as applicable. In addition there will be a societal benefit of EPRI informing the UK industry of electricity utility perspectives and needs for cyber security.

- Threat Management - guidelines for a coordinated view of all aspects of an organisation's security posture to provide an integrated

security operations center (ISOC). These will bring together the many isolated monitoring and response functions into a unified framework that would benefit National Grid and our customers.

- Security Architecture - integration of new security architectures to help sustain high levels of electricity quality and reliability.

- Security Metrics - monitor the control guidance based on useful cyber security metrics that result in benefit and improvement of National Grid's cyber security programme. Such metrics could also be used to support decisions about investments in cyber security in areas such as hardware, software, and personnel resources.

- Cyber security compliance - further understanding and ability to apply new cyber security requirements for critical infrastructure, including guidance such as the Policy on Critical Information Infrastructure Protection (CIIP) and the Network and Information Security (NIS) Directive of the European Commission.

Nominated Contact Email Address(es)

box.NG.ETInnovation@nationalgrid.com

Problem Being Solved

Cyber security threats are of significant concern to key industries in GB, including the utility sector. There is significant attention being given to the issue in Government and in the press. Managing cyber security across an organisation like National Grid with a global reach is a challenging and complex process that must be managed alongside the rapid evolution of the cyber threat landscape, with attacks becoming more prevalent and sophisticated.

Cyber and physical security is a critical priority for National Grid, the UK electricity sector, and the communities we serve. The sector is increasingly dependent on information technology and telecommunication infrastructure to ensure the reliability and security of the Electricity Transmission Network. Specifically for National Grid, measures to ensure cyber security must be designed and implemented to protect the Electricity Transmission Network in England and Wales from attacks by terrorists and hackers, to strengthen grid resilience against natural disasters and inadvertent threats such as equipment failures and user errors.

Method(s)

The rapid pace of change in the electricity sector creates a challenging and changing environment for asset owners and operators to monitor the cyber security activities, develop an understanding of how new technologies affect security, and maintain the right knowldege and skills in place to assess those technologies.

The Electric Power Research Institute (EPRI) employs a team of experts with comprehensive backgrounds in cyber security within the electricity sector. Their team of experts address these challenges by providing insight and analysis of various security tools, architectures, guidelines, and results of testing to programme participants and organisations. This research programme would help National Grid with our efforts to focus on developing security requirements, creating and utilizing new security technologies, and performing laboratory assessments of existing, relevant technologies to help enhance the current cyber security posture and increase the security of systems that are deployed in the future to better protect our customers and the communities we serve.

Scope

Several projects form the overall EPRI P183 work package, which are delivered in tandem:

1. Deliverable P183A: Industry Collaboration & Technology Transfer - the landscape of cyber security activities in the UK electricity sector involves numerous industry, government, and regulatory groups. Although tracking these groups can be a daunting effort, it is critical for utilities to be up-to-date on key industry activities. This deliverable provides members with an up-to-date view of industry activities and supports technical contribution to these groups.
2. Deliverable P183B: Security Technologies - this deliverable will address several security technology challenges facing UK power-delivery and control systems, such as developing protective measures and managing cyber threats.
3. Deliverable P183D: Information Assurance - this deliverable focuses on security challenges that affect multiple operations domains, such as designing security into products, creating security metrics for the UK electricity sector, and developing technical solutions for meeting security compliance requirements.

The work packages have deliverables that span across multiple years to complete, therefore not all of them will be completed at the end of 2016. Among the key expected areas of progress in 2016 are:

- Active participation by National Grid Digital Risk & Security in reviewing resulting deliverables and applying them internally to key processes, technological improvements supporting the Critical National Infrastructure for the UK as applicable. In addition there will be a societal benefit of EPRI informing the UK industry of electricity utility perspectives and needs for cyber security.

- Threat Management - guidelines for a coordinated view of all aspects of an organisation's security posture to provide an integrated security operations center (ISOC). These will bring together the many isolated monitoring and response functions into a unified

framework that would benefit National Grid and our customers.

- Security Architecture - integration of new security architectures to help sustain high levels of electricity quality and reliability.
- Security Metrics - monitor the control guidance based on useful cyber security metrics that result in benefit and improvement of National Grid's cyber security programme. Such metrics could also be used to support decisions about investments in cyber security in areas such as hardware, software, and personnel resources.
- Cyber security compliance - further understanding and ability to apply new cyber security requirements for critical infrastructure, including guidance such as the Policy on Critical Information Infrastructure Protection (CIIP) and the Network and Information Security (NIS) Directive of the European Commission.

Objective(s)

National Grid's participation in the EPRI Cyber programme 183 is focused on efforts to improve the industry's ability to defend against an ever changing cyber security threat landscape. This will ensure the safe and reliable operation of the electricity transmission network. Objectives include:

- Track industry and government activities and provide technical contributions to key working groups;
- Develop a security management foundation for UK transmission and distribution systems;
- Improve the UK electricity sector's ability to detect, respond, and recover from cyber incidents;
- Continue technical development of the Integrated Security Operations Center (ISOC);
- Extend the security architecture for the Integrated Grid to include new domains;
- Develop security metrics for the UK electricity sector; and
- Address the technical challenges of cyber security compliance.

Consumer Vulnerability Impact Assessment (RIIO-2 Projects Only)

n/a

Success Criteria

The overall the EPRI Research Programme 183 comprises multiple deliverables with varying degrees of progress expected on each deliverable during 2016/2017. The project team will be positioned to leverage the knowledge gained within that time frame to further National Grid's understanding and development of security requirements. This will include the generation and utilisation of information regarding new security technologies, in order to better protect the electricity transmission network and our customers.

Project Partners and External Funding

n/a

Potential for New Learning

n/a

Scale of Project

The rapid pace of change in the electricity sector creates a challenging environment for National Grid to monitor the cyber security activities of industry groups, develop an understanding of how new technologies affect security, and maintain the right knowledge and skills for assessing those technologies. The scope of work is required to help focus on addressing the emerging threats to the UK electricity sector through multidisciplinary, collaborative research on cyber security technologies, standards, and business processes.

Technology Readiness at Start

TRL3 Proof of Concept

Technology Readiness at End

TRL4 Bench Scale Research

Geographical Area

The programme is predominantly laboratory and desk based, located in the EPRI laboratories.

Revenue Allowed for the RIIO Settlement

None

Indicative Total NIA Project Expenditure

The total indicative NIA expenditure is £200,000

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)

Each programme and deliverable will have different financial savings based on the outcomes and potential benefits gained. Each EPRI programme that National Grid joins has been through two stages of review that consider the potential to deliver financial benefits. In the first instance, within EPRI's governance, the Research Advisory Committee provides guidance on policies and issues that impact the power industry to inform the content of the research programmes.

Within National Grid, the Technical Leader for each aspect of the GB Transmission Network undertakes a review of the proposed EPRI programme relevant to their technical expertise and responsibilities and evaluates which provide potential value from a GB perspective as part of an annual review of which programmes to participate in.

The Cyber Security programme is expected to generate valuable learning in regards to industry landscape, cyber security technologies and information assurance which may improve and maintain the reliability of the system.

Please provide a calculation of the expected benefits the Solution

Not required for research projects

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

Each EPRI programme will have different financial savings based on the outcomes and potential benefits gained. Each EPRI programme that National Grid joins has been through two stages of review that consider the potential to deliver financial benefits. In the first instance, within EPRI's governance, the Research Advisory Committee provides guidance on policies and issues that impact the power industry to inform the content of the research programmes. Within National Grid, the Technical Leader for each aspect of the GB Transmission Network undertakes a review of the proposed EPRI programme relevant to their technical expertise and responsibilities and evaluates which provide potential value from a GB perspective as part of an annual review of which programmes to participate in.

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

The direct cost of making the relevant improvements to our cyber security infrastructure will depend on what the various identified cyber threats are, the complexity of the change and its implications. The wider cost implications arising from such changes will be dependent on the specific outcomes generated from the deliverables and typically will be subject to further stages of demonstration prior to roll

out.

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

In addition to the publication of research outcomes and summary reports described above, every year EPRI organises a European Information, Communication and Cyber Security summit to disseminate results and share research priorities. The summit is open to all Transmission Operators and Distribution Network Operators, irrespective of their involvement in the programme. Public information from each project is made available to all relevant parties to ensure an open environment for learning to be shared.

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 value area of the ElectricityTransmission 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

☑ Yes