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

Mar 2024

Project Reference Number

NIA_SPEN_0090

Project Registration

Project Title

Cyber Risk Impact Assessment (Cyber-RIAST)

Project Reference Number

NIA_SPEN_0090

Project Licensee(s)

SP Energy Networks Distribution

Project Start

May 2024

Project Duration

2 years and 6 months

Nominated Project Contact(s)

Lara Cardoso

Project Budget

£600,000.00

Summary

The main objective is to develop a fully responsive cyber risk impact awareness tool, Cyber RIAST, that proactively scans the status of the cyber-physical energy system, providing a detailed picture of threat risk metrics and performing impact analysis on the physical energy system resilience. The purpose of this solution is to intervene cyber-attacks from their infancy and avoid the impact of cascading the cyber threats.

The key outcomes are:

- The development of a cyber-physical system risk impact awareness tool through the holistic approach.
- The development of a cyber intelligent system using sophisticated modelling, Machine Learning and Artificial Intelligence methodologies.
- The determination of cyber-physical system risk impact assessment criteria under various risk impact scenarios through both offline and hardware in loop testing.

Nominated Contact Email Address(es)

innovate@spenergynetworks.co.uk

Problem Being Solved

The smart grid is rapidly evolving and merging with digital and information communication technologies (ICT) systems, resulting in an interconnected cyber-physical energy system. Cyber-attacks have become a great threat to the energy system, and according to a recent IBM security report, the UK is one of the top three most attacked countries in Europe, along with Germany and Italy in 2021[1]. During this period, the UK energy system suffered from 24% of the overall cyber-attacks - higher than the manufacturing and financial sectors combined. Cyber-attacks on power grid infrastructure can result in complete shutdowns, leading to economic, financial, and

environmental damage, as well as potential fatalities. Thus, cyber security for both current and future energy systems must be treated as an urgent matter. Since cyber-attacks are highly unpredictable and unforeseen attacks occur regularly, current reactive cyber-physical risk assessment methodologies are no longer effective and need to be updated.

[1] IBM Security Report., “Energy sector becomes UK’s top target for cyberattacks as adversaries take aim at nation’s critical industries”, 23 February 2022, https://uk.newsroom.ibm.com/2022-02-23-IBM-Security-Report-Energy-Sector-Becomes-UKs-Top-Target-for-Cyberattacks-as-Adversaries-Take-Aim-at-Nations-Critical-Industrie

Method(s)

The vision is that a future smart energy system must be capable of a dynamic, standardised, and proactive risk impact assessment for cyber-physical energy systems so that cyber asset investment for defensive efforts can be better targeted. The ambition is to create a holistic approach to physical security risk impact awareness by developing a tool capable of scanning the risk status of cyber-physical systems. This tool will predict and dynamically discover the severity of cyber incidents and assess their impact on the resilience of the cyber-physical energy system. By identifying the weakest areas in terms of cyber security vulnerability and physical energy systems, power grid operators can effectively address high-impact cyber security issues in a timely and cost-effective manner. Furthermore, the tool will help power grid security teams identify optimal cybersecurity investments and allocate key resources to prevent the escalation of cyber incidents from their early stages through early intervention.

The novelty of this work is summarised below:

- The development of a cyber-physical system risk impact awareness tool through the holistic approach of (i) proactively assessing cyber system vulnerability, (ii) dynamically scanning and determining the severity of adversary efforts, and (iii) cyber risk impact analysis of the actual loss of physical components on the power system.
- The development of a cyber intelligent system using sophisticated modelling, Machine Learning and Artificial Intelligence to carry out the anatomy analysis of adversary efforts, identifying each cyber-attack severity for different possible attack actions.
- The determination of cyber-physical system risk impact assessment criteria under various risk impact scenarios through both offline and hardware in loop testing.

Scope

- WP1 **Network modelling and resilience studies**: carry out Physical network modelling and resilience index calculation. The simulated physical network model consists of a large number of power plant and system components (i.e. generations, transformers, circuit breakers, cables/overhead lines, loads and etc) that are connected to substations. With inputs from network operators that are supporting the project, this part will carry out power network modelling with the consideration of key grid components, such as traditional and future generations and low-carbon technologies, and develop benchmark models for the assessment of the physical network resilience indices under various loss of physical components in the context of cyber-attack scenarios, including loss of some generation and load connections as well as loss of entire substations under N-1 and N-2 scenarios.
- WP2 **Creation of Cyber System Vulnerability Models**: This work package will establish cyber system vulnerability models based on the inputs of the existing cybersecurity protection compliances to UK NCSC recommendations in NGET or SPT networks. Results will be communicated and verified within the consortium. Ant Data will coordinate the software interface formats between WP1 and WP2
- WP3 **Development of cyber intelligent System**: The aim of this WP is to develop new techniques using sophisticated analysis modelling, Machine Learning and Artificial intelligence to carry out the anatomy analysis of adversary efforts, identify attack paths, and discover the severity of cyber incidents. This WP will enable Cyber RIAST to detect and discover attack incidents in real-time. Ant Data will design and develop data-driven processing architecture in the big data environment and develop a big data analysis method to facilitate the real-time data collection, processing, and integrity checking, so as to provide a real-time data process platform for Cyber RIAST.
- WP4 Determination of cyber risk impact assessment criteria: Stage 4 will formulate equations with the inputs from the calculated the impact network resilience index results from WP1 and the cyber system risk vulnerability index results from WP2 and WP3 to obtain the cyber-physical system risk-impact awareness metrics. This work package will also determine cyber physical stem risk impact assessment criteria through lab tests under various testing scenarios.
- WP5 **Workshops, Industry Consortia Forums and Knowledge Dissemination:** within each stage and final report

Objective(s)

UoM

Stage 1/WP1: Network modelling and resilience studies:

- The scope and requirements for the delivery of this project: Agreed on the scope at the Project Kick-off meeting
- Literature and research preparation work
  - Report 1:

- State-of-the-art and evolving technologies in the literature relating to power system resilience studies.
- Identify suitable power systems simulation tools for power system resilient studies, such as Power Factory – DIG SILENT power system analysis software.
- Familiarize the simulation tools and carry out power system resilient studies for typical UK transmission and distribution networks.

- Network modelling and Establish Network Resilience Indices
  - Report 2:
- Benchmark network models: Modelling of typical transmission and distribution networks, including the cyber-physical system models within substations and SCADA systems within the control centres, the control of various types of generation and low carbon loads by the cyber systems.
- Calculation of network resilience indices: identify suitable power system simulation tools to carry out network load flow studies under N-1, N-2 or N-k scenarios. This will calculate the impact of the loss of physical components on network resilience indices and should lead to a review the ranking of each physical component's importance within the network.

Stage 2/WP2: Creation of Cyber System Vulnerability Models

- Implements a data interface between power system simulation network data and the cyber system Vulnerability Models
  - Report 3:
- Establish a software interface between the power system simulation model and cyber-physical risk resilience models.

Stage 3 / WP3: Development of cyber intelligent System

- Evaluation and verification of the proposed cyber intelligent System algorithms
  - Report 4:
- Develop new techniques using sophisticated analysis modelling, Machine Learning and Artificial intelligence to evaluate and analyse the cyber adversary efforts, identify attack paths, and discover the severity of cyber incidents.

Stage 4 / WP4: Determination of cyber risk impact assessment criteria

- Performance evaluation of Cyber-RIAST solutions
  - Report 5:
- Development of physical lab supporting infrastructure, including virtual substation communications, SCADA system for the developed methods to be tested and validated.
- Formulation to calculate the cyber-physical system risk impact metrics based on the results of the impact of physical system resilience indices based on the inputs of physical network impact indices from WP1 and the cyber system risk indices status from WP2 (cyber system vulnerability model) and WP3 (online discovery attack severity).
- Development of a real-time cyber-physical system by modifying the available Virtual Site Acceptance Testing & Training (VSATT) platform and SCADA system in Manchester's Real Time Digital Simulator (RTDS) lab, and determination of the cyber-physical system risk impact assessment criteria through the lab tests and verifications, so to achieve the said Cyber-RIAST solution.
- Development of a visualisation dashboard to show the status of the cyber risk impact metrics and use different display colours to represent the different risk-impact assessment criteria.
- Design specification report of WP4

Stage 5: Improvement, Workshops, Industry Consortia Forums and Knowledge Dissemination

- Publications and Final Report
  - Organising UK wide workshop in collaboration with CIGRE to maximize the visibility of the project achievements.
  - Annual attendance and representation by the Collaborator at relevant conferences.
  - Summary of Publications and Presentation slides: on ongoing training & workshop sessions delivered in 2024.

Subcontractor

Stage 1: Network modelling and resilience studies

- Software interface proposal and specification
  - Sub Report 1:
- Establish cyber-physical risk resilience fragility curves.
- Establish and develop Cyber-RISAT database,
- Development of a software interface to allow the results from the load flow studies (by UoM) to be loaded into the Cyber-RIAST database automatically.

Stage 2: Creation of Cyber System Vulnerability Models

- Creation of Cyber System Vulnerability Models

- Sub Report 2:
  - The creation of cyber system vulnerability models. As a first attempt, a fragility curve model is suggested to obtain the probability of cyber vulnerability curves for each cyber system based on the current cybersecurity measures/protections/compliances. For example, implementing physical network access control methods, e.g. fence, locker, alarm, security camera, or cybersecurity role-based access control protocol, such as passwords, different levels of authenticity keys, etc. It is expected that the more security measures in place, the cyber less vulnerable the system becomes. The created cyber vulnerability models should accurately represent the above-mentioned principle.
  - The development of methodology and specification to allow the representative vulnerability model as a function of the different levels of the severity of cyber-attack incidents. Coordinate efforts to verify the cyber system vulnerability models with the inputs of the SPT and NGET cyber security team and operators.

Stage 3 / WP3: Development of cyber intelligent System

- Cyber intelligence system specifications and development
- Sub-Report 3:
  - Technical specifications on data process architecture, data engineering and data integrity analysis. The data proceeding system will consider the ability to connect health data points to establish prevention /defence against false data injection and deliver secure and reliable data to the Cyber-RIAST
  - Software implementation of data-driven cyber intrusion detection system using sophisticated decision processing modelling, ML and AI. This will enable the development of a cyber intelligent system to carry out the anatomy analysis of adversary efforts, discover attack paths and predict the severity of any associated attacks.
  - Calculation of cyber system risk indices: By comparing the established vulnerability fragility curve from WP2 and the predicted attack severity from WP3, the status of the cyber system risk vulnerability index will be calculated as input to WP4.
  - Data engineering specifications and report of WP3.

Stage 4 Determination of cyber risk impact assessment criteria

- Validation of the design Performance
- Sub Report 4:
  - Data analysis and design evaluation based on the obtained testing results

Stage 5: Improvement, Workshops, Industry Consortia Forums and Knowledge Dissemination

- Support the final project report
- Participate workshops and knowledge dissemination events
- Provide all necessary data, results and summary of publications and Presentation slides.

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

Minimum success criteria (Must and should)

- Should produce SPT and NGET requirements specification for cyber component vulnerability models and physical component impact indices analysis on power system resilient. Measure: Requirements specification document(s)
- Determination of the cyber-physical risk impact indices assessment criteria should have the inputs from SPT and NGET cyber team according to their networks cyber risk analysis requirements. Measure: Market analysis of current cyber-physical risk analysis tools
- Must share knowledge and disseminate findings at regular energy system events. Measure: Presentations and published reports at industry events

Must demonstrate and validate cyber-physical risk impact assessment at lab environment. Measure: Lab testing to meet required success criteria

Desirable criteria (Could)

- Identify suitable proactive cyber-physical risk assessment methods or strategies for digital substation and SCADA systems. Measure: The outcome of this investigation will be included within report 5.

Project Partners and External Funding

Project Partners:

- SPT
- NGET
- UoM
- EIC

Potential for New Learning

The development of cyber impact awareness system and its application to smart energy system will enhance the network security for future smart, flexible and decarbonised energy system, a sector representing more than £13bn of Gross Value Added between now and 2050. It will support British Energy Security Strategy aims for secure, clean and affordable British energy for the long term. The outputs of this project will support and meet UK government net zero and resilient objectives, specifically support the UK power utilities focus area 'preparing systems to withstand extreme events. The opportunity for demonstrating the cyber-physical risk impact assessment and Cyber-RIAST solution in the laboratory setup would be used for training and dissemination throughout SPT, NGET, and by other interested parties. The dissemination of the IP will foster greater competition within the market and encourage multiple vendors to create interoperable commercial solutions and facilitate future investment opportunities.

The project will also facilitate the:

• Transfer of knowledge from various industry sectors developing Cyber-physical impact awareness solutions,

• Development of innovative solutions which lead to benefits for consumers.

Scale of Project

This project will be carried on a lab network in University of Manchester. A successful outcome can be scaled across UK energy network operators.

Technology Readiness at Start

TRL2 Invention and Research

Technology Readiness at End

TRL5 Pilot Scale

Geographical Area

All work will be conducted in the UK at our project partners laboratories, in Manchester, UK.

Revenue Allowed for the RIIO Settlement

0

Indicative Total NIA Project Expenditure

- SPT - £225k
- NGET - £225k

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:

With the implementation of Cyber-RIAST the energy network will become more secure as it highlights weaknesses in the network and allows us to proactively respond to incidents. With a network more secure from cyber-attacks the transition to net-zero will become easier as there will be not only capital savings but it will also allow us to focus on transitioning to net zero.

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)

N/A

Please provide a calculation of the expected benefits the Solution

It is out of scope of this project to investigate quantifiable benefits of rolling out the solution. Expected benefits of solution are:

- Establishment and standardising of cyber system vulnerability models,
- Development of online detection method enabling anatomy analysis of adversary efforts to predict each attack severity
- Determination of cyber-physical risk assessment criteria through lab hardware in loop tests and verification

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

BaU method should be fairly replicable across GB, specially considering 2/3 of GB's TOs are involved in it. It is important to note that current methods are at a TRL of 2, through the project we expect to uplift to a TRL of 5.

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

It is out of scope for this project to investigate costs of rolling out the solution across GB.

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 development of cyber impact awareness system and its application to smart energy system will enhance the network security for future smart, flexible and decarbonised energy system, a sector representing more than £13bn of Gross Value Added between now and 2050. It will support British Energy Security Strategy aims for secure, clean and affordable British energy for the long term. The outputs of this project will support and meet UK government net zero and resilient objectives, specifically support the UK power utilities focus area 'preparing systems to withstand extreme events. The opportunity for demonstrating the cyber-physical risk impact assessment and Cyber-RIAST solution in the laboratory setup would be used for training and dissemination throughout SPT, NGET, and by other interested parties. The dissemination of the IP will foster greater competition within the market and encourage multiple vendors to create interoperable commercial solutions and facilitate future investment opportunities.

The project will also facilitate the:

- Transfer of knowledge from various industry sectors developing Cyber-physical impact awareness solutions,
- Development of innovative solutions which lead to benefits for consumers.

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

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.

It has been confirmed no project registered on the SNP being carried out or completed will have similar outcomes as Cyber-RIAST, as this is an unproven method in GB's energy industry.

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 novelty of this work is summarised below:

- The development of a cyber-physical system risk impact awareness tool through the holistic approach of (i) proactively assessing cyber system vulnerability, (ii) dynamically scanning and determining the severity of adversary efforts, and (iii) cyber risk impact analysis of the actual loss of physical components on the power system.
- The development of a cyber intelligent system using sophisticated modelling, Machine Learning and Artificial Intelligence to carry out the anatomy analysis of adversary efforts, identifying each cyber-attack severity for different possible attack actions.
- The determination of cyber-physical system risk impact assessment criteria under various risk impact scenarios through both offline and hardware in loop testing.

Relevant Foreground IPR

Project expected to generate new methodology of proactively evaluating risks and impacts of attacks on the energy network.

Data Access Details

Access to data must be requested by contacting spinnovation@spenergynetworks.com or the project contact.

Please provide the following information in your request:

- Affiliation, position and contact details of requesting party
- Relevant project and type of data required
- Reasons for requesting this data and evidence that this data will be used in the interest of the UK network electricity customers
- How data will be shared internally and externally by the requesting party

Any data request deemed unsuitable for sharing will be highlighted to the appropriate requesting party. After receiving the request, we will provide the estimated date for completing the data provision based on other requests and our team workload at that time. All requested data remains the property of SP Energy Networks. Further information found here: Data Sharing Policy - SP Energy Networks

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

This is an unproven technology, which requires significant testing and assessment to minimise risk of operation on the Network.

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

There are significant technical and operational risks to the solution if it were to be implemented directly into BaU.

This project has been approved by a senior member of staff

☑ Yes