SIF Round 3 Project Registration

Date of Submission

Mar 2024

Project Reference Number

10103996 (2)

Initial Project Details

Project Title

Network Security in a Quantum Future

Project Contact

Simon Lambe

Challenge Area

Novel technical, process and market approaches to deliver an equitable and secure net zero power system

Strategy Theme

Data and digitalisation

Lead Sector

Electricity Transmission

Project Start Date

01/03/2024

Project Duration (Months)

2

Lead Funding Licensee

National Grid Electricity System Operator

Funding Licensee(s)

National Grid Electricity System Operator

Funding Mechanism

SIF Discovery - Round 3

Collaborating Networks

National Grid Electricity System Operator

Technology Areas

Cyber Security

Project Summary

The energy system is key to UK critical infrastructure. It must be secure against state actors, organised crime, and other potential threats. Emerging quantum computing technology will open significant new attack vectors against existing cybersecurity. This project will investigate the quantum threat to the energy system's cybersecurity, developing a novel assessment framework and a prioritised mitigation approach. The aim is to ensure that critical energy infrastructure remains secure in a post-quantum era, applying expertise in quantum and cybersecurity to cut through the hype, helping the industry to understand the actual threat and timelines, and enabling mitigation strategies to be developed.

Project Budget

£169,857.00

SIF Funding

£149,621.00

Project Approaches and Desired Outcomes

Problem statement

Identified Problem:

Ongoing energy system security is a key concern for the UK. The potential application of emerging quantum computing technologies to overcome existing cybersecurity systems and cryptography poses a significant threat. The extended lifespan of energy network assets means this is of particular concern. Characterising the quantum threat, and delivering a mitigation strategy, are key to national security. This project will design a new framework to evaluate the quantum threat and methodology to generate timescale estimates and readiness indicators, enabling appropriate mitigation strategies and supporting resilience across the energy industry.

Primary Innovation Challenge:

Key challenges for the industry are:

understanding the nature, impact, and timeline for the quantum threat
using this knowledge to mitigate appropriately considering the lifetime of energy network assets and operational information.
Addressing these challenges requires an innovative approach. There is significant hype around quantum, and little clarity on the scale or timing of impact. This project will cut through the hype, delivering an unbiased, robust, and actionable assessment of the energy industry's security challenge, identifying the requirements for cryptographic relevance, and creating a novel framework for generating timescale estimates and readiness indicators.

The framework will incorporate the concepts of both asset and information lifetime, ensuring threat assessment and mitigation strategies can be prioritised effectively. Energy networks have an unusually large range of system lifespan timescales. A one-size-fits-all security threat mitigation approach is both ineffectual and non-cost-effective.

The project approach starts from the principle that information has a lifetime over which it needs to be protected, impacting the relevance of the quantum threat. The threat from quantum to operational information with a lifespan of minutes (substantially lower than quantum capabilities) is low, but the threat to assets and information with long operational lifespans is significant. Understanding these timescales and how they impact the quantum threat will enable effective, value-for-money cybersecurity planning.

Potential users:

In a future where quantum computing is commonplace, users of the innovation will be all network's operational teams, who would use the project outputs to better understand the quantum threat and plan their response in an ongoing and cost-effective manner for consumers. The development will consider the needs of the whole energy industry, utilising input from the Energy Sector Cyber Security Group (E3CC) and will be the first of its kind for the energy industry.

Video Description

https://www.youtube.com/watch?v=eoEqAXnWTME

Innovation justification

How does your Project demonstrate novel and ambitious innovation in the energy networks?
Innovation:

This project brings an understanding of the quantum threat to energy systems and development of associated mitigations. The novelty lies in the assessment of the timescales of information and asset lifespans across the current and future energy network, the consequential threat, and mitigating actions --incorporating this into a usable (and scalable) framework for the industry. The project will deliver an understanding of the specific threats, and enable development of an improved cybersecurity approach. It will protect consumer value by helping to prevent future cybersecurity vulnerabilities, and resultant cost from actual attacks.

Advancing Previous Research:

This project brings insight from the project partners' current research on methods for assessing cybersecurity threats. Quantum computing is a nascent and developing technology, leading to hype and a cloudy understanding of its applications, potential threats and timescales.

The project will review current developments to design a framework that delivers clarity on the relevant threats, tailored to the energy system.

It will then explore novel approaches to making decisions about the energy system's mitigating actions to the quantum threats, informing a comprehensive framework for selecting the most appropriate mitigation.

This project delivers a step change in risk assessment and mitigation, moving significantly beyond current approaches by:

taking a holistic approach to understanding the quantum cybersecurity threat;
considering lifespans of information and assets;
enabling development of tailored mitigations.
The Discovery phase will raise maturity level of the project's technologies, integration, and commercial readiness from:

TRL1- \> TRL3 (Proof of principle)
IRL1- \> IRL2 (Characterised concept)
CRL1 -\> CRL2 (Initial market analysis)
The project team is exceptionally qualified to address this innovation challenge, combining expertise and experience on quantum computing, cybersecurity, and the energy systems.

Need for SIF Funding:

The quantum cybersecurity threat is an industry-wide challenge of national importance. The uncertain timing, nature, scale, and impact means it falls outside the scope of normal strategic planning. This project enables collaboration across energy networks, industry, and academia to create new methodologies and solutions, appropriate to the whole energy industry. The SIF phased structure will facilitate exploring beyond business-as-usual, to deliver cross-industry impact.

Counterfactual Solutions:

Most current research is insufficiently specialised to the energy industry, providing a snapshot of the current state of cybersecurity threats, and implementing blanket "one-size-fits all" mitigation strategies. This is not appropriate for energy systems, given their wide variability in infrastructure and assets; nor efficient, as it results in ineffective or over-specified mitigations.

Impacts and benefits selection (not scored)

Financial - future reductions in the cost of operating the network

Financial - cost savings per annum for users of network services

Revenues - creation of new revenue streams

New to market – processes

New to market - services

Others that are not SIF specific

Impacts and benefits description

Future Reductions in the Cost of Operating the Network:

Significant savings can be realised by identifying the correct mitigation for the quantum cybersecurity threat, providing means to evaluate criticality of assets to the network and assessment of the most cost-effective mitigation strategies. This will help avoid over-specification of low-priority assets, and under-specification of critical assets, as relating to cybersecurity threats, enabling effective forward planning for long-term asset investment. This will help reduce the vulnerabilities to cyberattack, limit the severity

of detrimental impacts to the system, and reduce long-term costs from remedying unexpected issues. Logistics provider Maersk estimated a recent cyberattack cost $300m to fix.

Cost-Savings per Annum for End Users of the Network Services:

In December 2015, the Russian cyberattack on Ukraine left 1.4m homes without power. By reducing the risk of significant cyberattacks, this project also reduces the associated ongoing cost of defending (and insuring) against cyberattacks. This saving can be measured, and estimates made of how much may be passed on to end consumers. Lowering the risk of attack reduces the attendant cost to consumers of dealing with consequences of a successful attack; such costs will be estimated in Discovery. Furthermore, those who suffer the most from system outages are vulnerable customers, for whom energy is vital to support their essential needs, or who lack resources that would otherwise allow them to mitigate the impact of an outage.

New to Market Processes and Services and Creation of New Revenue Streams:

The framework generated by the project will be a novel quantum cybersecurity risk assessment and mitigation approach, incorporating the encryption lifecycle of operational data related to systems or assets. This process can be operationalised and embedded in future analysis by the energy networks. The approach developed through Discovery (and subsequent phases) could be offered to other infrastructure-heavy industries (e.g., transport, water), or to other countries whose critical infrastructure faces the same challenge. Initial estimates (tbc) indicate an opportunity to target 0.5%-1% of the cybersecurity market, valued annually at £10.1bn in the UK and £40.8bn globally.

Others:

The key benefit realised by this innovation, not explicitly captured by other SIF metrics, is the de-risking of the cybersecurity of the energy network assets and systems in the post-quantum world. This reduction in risk will ensure energy network resilience in the future when quantum computing is available, securing the continuous secure operation of services for consumers.

Teams and resources

This project builds a partnership between National Grid ESO, Cambridge Consultants, University of Warwick, and University of Edinburgh, (no subcontractors).

National Grid ESO (NGESO):

NGESO, project lead, is the electricity system operator for Great Britain, ensuring continuous reliable and secure system operation across the UK. The move to Future Systems Operator will soon expand NG ESO's role to cover whole-energy system. NGESO will use their expert knowledge of critical national infrastructure and system operation to steer the project to produce useful outcomes for the NGESO and wider energy industry. The Chief Information Security Officer and his team, including members of the E3CC, will identify and test relevant use cases to ensure robustness of Discovery outputs. Alongside overall project management, NGESO will be responsible for robust innovation project governance processes, using experience from their role as a regulated network.

Cambridge Consultants (CC):

CC is a deep-tech engineering consultancy working across industry sectors, with departments specialising in both cybersecurity and quantum computing. CC will provide the interface between the major workstreams, drawing upon their broad team, including specialists with experience of the NGESO's cybersecurity threat / cost assessments. Furthermore, CC are part of the UK quantum industry body, UKQuantum, with members on the steering committee. CC have in-house photonics facilities which have been used to work on Quantum key distribution, and, through their parent company Capgemini, have access to quantum hardware as part of the IBM Quantum network.

University of Warwick (UoW):

UoW is a leading research university with specialisms in cybersecurity and statistics. This project will utilise their expertise to direct the work on impact of the quantum threat and potential mitigations. UoW's statistics group brings knowledge and insight into decision making under uncertainty, which plays an important role in developing the relevant methodologies within this project. UoW host a NCSC-EPSRC Academic Centre of Excellence in Cyber Security Research, which will enable this project to further connect into the cybersecurity community and access cutting-edge research.

University of Edinburgh (UoE):

UoE is a leading research university with specialisms in quantum computing and power systems. UoE will use their experience in cryptographic quantum computing to understand and assess the quantum threat. Their expertise in power systems will enable the project to focus on the specific challenges to the energy industry. UoE hosts the Quantum Software Lab, a research centre focused on exploiting quantum computers to solve problems beyond the reach of classical machines.

Project Plans and Milestones

Project management and delivery

The project is split into three work packages running in parallel and sharing project resources, research, and project governance:

WP1: Quantum threat analysis
WP2: Information model design (framework)
WP3: Project management and communications
WP1 will produce the assessment of the quantum threat to the cybersecurity of the NGESO. This commences with a workshop and literature review to identify the threats posed by quantum, followed by a gap analysis to cross examine against the energy systems. This work culminates in an outline methodology, for development in the Alpha phase, to identify the opportunities and threats from quantum computing, estimate timescales, and identify readiness indicators.

WP2 focusses on designing an information model (framework), based on understanding the security requirements for the energy network, assessing potential vulnerabilities identified in WP1 as they are generated. This will result in a framework considering the security lifespan of the various assets and systems and an adaptation methodology for implementation.

The robustness of the information model will be assessed using a test case based on one of NGESO's existing systems, ensuring the developed methodology is relevant to the energy network's requirements and threats. It will be used throughout the project to inform example asset and data points, and to identify any opportunities for improvement of the output not visible without industry specific knowledge.

The project's parallel work packages follow a waterfall structure, with regular milestones and deliverables to enable collaboration across activities and partners. The first two milestones are the kick-off and mid-phase workshops, providing opportunity for all partners to disseminate background knowledge of the energy network, cybersecurity, and quantum computing. The final milestone is the creation of comprehensive reports, summarising the learnings from the Discovery phase, vision for further developments, and their potential impact on energy network security.

Project Management:

The project will be led by NGESO, who will assign a dedicated project manager and will be responsible for project coordination, governance, and dissemination. Three regular steering meetings will be held to review progress, alignment of output, and review risks. The project will adopt a rigorous risk management process to identify, manage, mitigate, monitor, and communicate project risks throughout Delivery. Risks are defined in the PM Template and will be reviewed and updated at steering meetings.

Interruptions and Interactions with Customers:

There are no foreseen supply interruptions to customers, nor policy / regulatory challenges within the Discovery, or subsequent phases.

Key outputs and dissemination

Achievements:

At the end of the Discovery phase, this project will have completed three interconnected activities which will be used as the foundation for later stages of the project:

Review (WP1): a review of the current understanding of the quantum threat and analysis of the gaps that need to be addressed to apply this understanding to the cyber threat to power systems. This understanding will used to direct work on the threat side in later stages.
Framework (WP2): initial development of a methodology for assessing the cybersecurity requirements of assets to deliver a secure energy system within a quantum future. This will include building understanding and providing transparency on how the methodology is developed. In the later (Alpha and Beta) stages this methodology will be further refined and operationalised, and novel mitigations will be developed, incorporated, and tested.
Testing (WP2): The final piece of work is to test the framework on an initial case study (i.e. family of assets) to both demonstrate the intended use and the value that the methodology delivers.

Outputs:

Three reports will be generated, one associated to each activity, to disseminate the learnings to the wider community:

A report detailing the current understanding of the quantum threat to cryptographic standards relevant to the energy industry and key areas for future work to bring further clarity and understanding. CC will be responsible for this report.
A report detailing the designed methodology for assessing security requirements. This will outline how the methodology was achieved and how to implement it. Included will be a description of potential refinements for consideration in Alpha and plans for incorporating mitigations. CC will be responsible for this report.
A report detailing the completed case study. This will incorporate details of the use case architecture and the application of the methodology to that architecture. NGESO will be responsible for this report.
Dissemination:

Outputs and learnings will be shared on the ENA Smarter Networks Portal, which publicises projects across the energy industry, via relevant forums such as Energy Emergencies Executive Committee (E3C) and the Electricity and Gas Networks Forum, and through show and tell sessions hosted by NGESO with input from all the project partners. Outputs from the project will be disseminated across the public domain in accordance with SIF governance requirements, ensuring that key knowledge gained by the Discovery phase will not undermine the development of competitive markets.

Commercials

Intellectual Property Rights (IPR) (not scored)

All Project Partners will treat Intellectual property in accordance with Chapter 9 of the SIF Governance Document. It is noted that foreground IPR is unlikely to be developed in the Discovery phase. If further details are required on each partner's compliance with Chapter 9 when IP is developed at later project stages, this would be supplied to the Project Monitoring Officer at the relevant point.

Value for money

Total Project Cost:

The overall cost of the Discovery phase is £169,857, split across the four partners (£36,554 for NGESO, £102,926 for CC, £15,403 for UoW, and £14,974 for UoE), with no subcontractors.

SIF Funding and Contributions:

The total amount of SIF funding requested is £149,621, the remaining 11.9% contributed by the project partners from private funds. CC, UoW and UoE will contribute 10% from internal funds to offset all labour and expenses costs incurred in the delivery of the project, providing assurance that the costs compare favourably to normal industry rates (£10,293 by CC, £1,543 by UoW, and £1,500 by UoE). Furthermore, NGESO will contribute £6,900 (equivalent to 18.8% contribution) from internal funds relating to time required to provide expertise and ensuring coordination and successful delivery of the project. There will be no additional innovation funding.

Value to the Consumer:

The project enables collaboration between leading organisations across energy systems, cybersecurity and quantum computing, as well as dissemination in a public forum. The result is an output which benefits from cross-disciplinary experience, at favourable cost compared to normal industry advisory and development rates, and significantly less than the alternative development approaches (independent, siloed and parallel investigations across the energy systems and wider industry).

Path to Business As Usual:

The Discovery phase will create a design for an information model and methodology for assessment and mitigation of the quantum threat. At full maturity, both the information model and the assessment and mitigation tool can be embedded directly into business as usual in NGESO, and across the wider energy industry, utilised as part of the standard assessment for cybersecurity threat (with particular value in the specification and procurement of new and upgraded assets and systems).

The tools and methodology for assessing quantum computing performance indicators will have direct use across industry. Using the links to E3CC, the Alan Turing Institute and CC's quantum technologies team, the methodologies can be used to directly influence the adoption and development around quantum computing - many of the subroutines used in cryptography have similarities to uses within chemistry. The project's objectives have already gathered positive feedback in sharing with wider industry.

Furthermore, the developed approach to assessing not only potential risk but also lifespan of critical information in Discovery could be adopted and tailored for industry-relevant challenges across other infrastructure-heavy industries (e.g., transport, water), when upgrading and replacing assets and systems with significant lifespan.

Supporting documents

File Upload

No documents uploaded

Documents uploaded where applicable?

☑