SIF Alpha Round 3 Project Registration

Date of Submission

Dec 2024

Project Reference Number

10129418

Initial Project Details

Project Title

Network Security in a Quantum Future - Alpha

Project Contact

Konstantinos Polychroniadis

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

01/10/2024

Project Duration (Months)

6

Lead Funding Licensee

NESO - National Energy System Operator

Funding Mechanism

SIF Alpha - Round 3

Collaborating Networks

National Energy System Operator

Technology Areas

Cyber Security

Digital Network

Project Summary

As part of the UK's critical national infrastructure, the energy system must be secure against malicious cyberattacks. The nature of emerging quantum computing technologies will enable attackers to break encryption that is currently highly secure and open significant new attack vectors.

To ensure resilience, energy networks must therefore consider the quantum threat in their cybersecurity strategies. However, understanding quantum impact highly requires specialist knowledge. This project addresses this by creating an innovative risk management tool to assess the quantum threat to the energy network, mapping it to a diverse range of energy system assets, and enabling prioritisation of appropriate mitigations.

Add Preceding Project(s)

10103996 (2) - Network Security in a Quantum Future

Add Third Party Collaborator(s)

Cambridge Consultants (CC)

University of Edinburgh (UoE)

Project Budget

£553,628.00

SIF Funding

£498,264.00

Project Approaches and Desired Outcomes

Animal testing (not scored)

- ○ Yes
- ◉ No

Problem statement

Quantum computers offer many benefits, but in the wrong hands can introduce new cybersecurity attack vectors. Malicious actors could use quantum to undermine the energy sector's ability to reliably provide energy to customers.

The complexity of quantum computing technology means that making sensible choices about what needs to be done, and when, is extremely challenging. The energy sector's response to any cyberthreat must be appropriate and proportionate, ensuring that systems are upgraded before threats can be realised, but also doing this in a planned way that prevents expensive, reactive 'rip-and-replace' strategies.

Key challenges:

The difficulty of turning fast-moving, cutting-edge quantum computing research into meaningful information for security experts.

The complexity, scale, and distributed nature of the energy network, which means 'off-the-shelf' responses to the quantum threat could be expensive to roll-out retroactively, and could potentially introduce new risks.

Project evolution

Discovery identified that:

Quantum computing technologies will pose a legitimate risk to a subset of cybersecurity controls employed by the energy sector.

The timeline for quantum technology being available to malicious actors ("time-to-attack") is currently ~10years (therefore within the lifetime of energy sector assets being deployed today) so there are opportunities to make cost-effective security decisions now about quantum-defence to enhance energy system resilience.

Rapid evolution of quantum technology is reducing both time-to-attack, and time-of-attack (the time it takes an attacker to launch and deploy a quantum-enabled cyberattack); keeping abreast of technology changes will be key to ensuring accurate risk estimates and keeping the network secure.

Post-quantum risk management tooling must be able to integrate into current cybersecurity processes, without security specialists having to develop expertise in quantum.

Quantum risks must be prioritised against other types of cybersecurity risks, to ensure optimal use of security teams' resources, and maximise risk reduction achieved with the available level of investment. Our understanding of approach and metrics from Discovery will feed into designing tool outputs that can integrate quantum risk assessment/management into BAU.

There is generalised guidance available about mitigating quantum cybersecurity risks; however, a tool that addresses the complexity, scale, and distributed nature of the energy network and determines appropriate mitigations for protection of energy assets, would be the first of its kind.

Link to Primary Innovation Challenge aim/theme

The Network Security in a Quantum Future (NSiaQF) Alpha addresses the challenge aim/theme by developing a tool to convert the latest quantum computing research into actionable intelligence, supporting continuing resilience of the energy sector to cybersecurity threats. The development will focus on a process workflow and supporting software demonstrator tool (the Quantum-Aware Risk Management tool, supported by a Quantum Threat Tracker module) that combines quantum computing research and energy system modelling. The tool will support energy network security teams in identifying, characterising, measuring and ultimately mitigating the risks posed to the energy sector by quantum computers.

By providing an accurate model of both the time-to-attack and the time-of-attack, which evolve in line with quantum computing technology developments, quantum computing risks can be assessed alongside other cybersecurity risks to the energy sector, and appropriately prioritised and mitigated in a cost-effective, pre-emptive way.

Potential users

The project outputs will consider the needs of the whole energy industry, consulting the Energy Sector Cyber Security Group and other key stakeholders.

Primary users:

Energy network security teams. Supported by the proposed methodology and tooling to manage risks from quantum computing.

Secondary users:

Quantum computing researchers. Use their domain knowledge to update the tool's model of quantum threats.

Policymakers. Use the tool to identify areas of greatest potential quantum impact on energy network security.

Prior funding - Discovery phase.

Innovation justification

The below Innovations will support resilience of the energy sector to emerging quantum-enabled cyberthreats:

- Making quantum intelligence actionable: Quantum research will be captured, analysed, and converted to parameters that can be used to update risk models on a regular basis, translating highly technical, cutting-edge research into usable threat intelligence for energy sector security teams.
- Embedding quantum computing risk management into BAU: The proposed tool and workflow will map into standardised risk management processes familiar to energy sector security professionals, allowing quantum risks to be prioritised against traditional cyber risks, and enabling informed trade-offs about where to invest in mitigations. Consumers will benefit from reduced costs achieved through better-targeted mitigations.
- Characterising quantum risks: Our novel methodology will produce evidence-based estimates of quantum risk, blending analysis of time-to-attack (time until quantum computing resources become available to attackers), with time-of-attack (time required for an attacker to initiate and execute a quantum attack). The risks posed by quantum computers to energy sector assets will be characterised to a level of detail not previously achieved, adding significant value for security teams.
- Modelling energy network assets: We will identify an asset modelling approach that is detailed enough to be useful but lean enough to support the need for the quantum risk tool to be scalable and feasibly applied to the full range of energy system assets.

Developing Discovery research

- We will expand on Discovery's analysis of types of quantum-enabled attacks and post-quantum mitigations, covering more energy system test cases, asset types, and ranges of tactics, techniques and procedures (TTPs) that attackers will use.
- Discovery's literature review highlighted ongoing research likely to shorten both time-to-attack and time-of-attack for quantum-enabled cyberattacks. In Alpha we will begin developing the tool to incorporate quantum experts' updated estimates of these parameters, enabling security specialists to make decisions based on timely data.
- Discovery highlighted gaps in the literature about quantum attack prediction; specifically, much literature focused on time-to-attack. Our Discovery work focused on time-of-attack. Alpha will merge these approaches to build a complete picture of risk, based on both factors (and others that could impact quantum risk).
- Discovery created a list of potential mitigations for quantum-enabled attacks but was not comprehensive and did not include advice on when to employ which mitigation; Alpha will develop clearer guidance on this.

Readiness Levels (Now->Alpha)

- TRL2->TRL4 (limited scope demonstrator in a working environment).
- IRL2->IRL3 (compatibility between technologies).
- CRL2->CRL3 (technology application).

Stakeholder validation

To ensure that tool outputs are relevant and appropriate for the energy sector, we will continue to leverage knowledge from the NESO and engage with the UK Cyber Security Task Group. We will target embedding the toolset into Business-As-Usual (BAU),

defining a roadmap from Proof-of-Concept (PoC) to BAU.

Need for SIF Funding

The quantum cybersecurity threat is an industry-wide challenge of national importance.

The complexity of distilling quantum computing knowledge into actionable intelligence takes this process outside the scope of normal energy network strategic planning, and other network funding routes. The SIF phased structure will facilitate an informed and engaged approach, involving development of a process, then of a tool, utilising an iterative process, working first with the NESO security team, and then with the broader energy ecosystem.

Counterfactual solutions

The alternatives to this project, which we believe are either too risky or too costly to be viable, are to:

1. Adopt a purely reactive response strategy, relying on cybersecurity suppliers to implement solutions.
2. Rip-and-replace' all assets with systems that support post-quantum cryptography as they appear.

The Appendix provides a comparison of the counterfactuals to the Network Security in a Quantum Future (NSiaQF) strategy.

Impact and benefits (not scored)

Financial - future reductions in the cost of operating the network

Impacts and benefits description

Primary Benefit: Future reductions in cost of operating the network

Current Situation

Discovery showed that quantum computers will enable cybersecurity threats against the energy sector by breaking current public key cryptography, enabling potentially catastrophic attacks such as network shutdown by malware or market manipulation through message tampering. If network operators do not prepare, this will increase the likelihood of a successful attack.

Financial and social costs of cyberattacks on critical infrastructure are significant. In December 2015 a Russian cyberattack on Ukraine left 1.4M homes without power. Logistics provider Maersk estimated a successful cyberattack on their systems cost $300M to fix.

The UK National Risk Register 2023 estimates the cost of a cyberattack against UK critical infrastructure could run to “hundreds of millions of pounds”, causing 81-400 casualties and 41-200 fatalities.

Alpha WP4 (Impact analysis) will define and quantify the increased risk and likely impact of quantum-enabled attacks, with input from the NESO"s cybersecurity team and other industry stakeholders.

Further, WP1 will develop an asset model for the energy network, highlighting the size and scope of potential vulnerabilities and inform the quantification of potential benefits.

Quantification of Benefits

Option 1: Develop and deploy Q-ARM tool (proposed project)

Alpha's cost-benefit analysis will quantify the expected reduction in future energy network operating costs, primarily from using the Q-ARM tool to support cost avoidance through minimising risk of a successful quantum-enabled cyber-attack. Potential successful attacks could start by 2029, increasing year-on-year through 2033. We have estimated the lifetime net present value (NPV) as £878,455,958. This figure will be refined during Alpha.

Further reductions in operating costs would come from minimising the costs for implementation of mitigation strategies within energy networks by ensuring mitigations are targeted and appropriate to quantum-enabled threats. The proposed Q-ARM tool will evaluate the criticality of energy network assets and recommend cost-effective mitigation strategies. This will also facilitate planning for long-term asset investment.

Baseline/BAU (Reactive Strategy):

Up-front cost would be lowest in this option, as no Q-ARM tool would be developed. However, the likelihood of successful quantum-enabled cyberattacks would increase significantly, with negative impacts on consumers, security of supply and the UK economy.

Option 2: Rip-and-Replace Strategy

In this option (not yet modelled), network operators undertake an accelerated asset replacement program, targeting all hard-to-upgrade assets (those unable to change cryptographic standard). This would be done without the Q-ARM tool to identify and prioritise specific vulnerabilities, and thus would mean bringing major cross-network investment requirements forward by many years. We will develop the analysis for this in Alpha; however, as a benchmark, in 2022 the UK invested £13billion in the energy industry, mainly for asset replacement. Assuming a significant proportion (20%) of this replacement will need to be accelerated over the coming years to maintain network security against the quantum threat, this would lead to extra cost of £350-£450million annually.

Metrics

In Alpha's cost-benefit analysis, we will develop a methodology and associated metrics to clearly quantify the above benefits but will include:

- Level of cyber-risk from a quantum attack.
- Expected impact on the wider UK economy.
- Reduction in accelerated asset replacement costs due to cyber-risk.

Other benefits: De-risking cybersecurity of energy network assets and systems in the post-quantum world

Qualitative Benefit:

Discovery highlighted the real, significant threat quantum computing will pose, with threats initially coming from nation states in as early as 5 years but then from other threat actors. The risk reduction enabled by developing the Q-ARM tool will ensure future energy network resilience, security of supply for consumers. This is key for social and economic benefit, continued security of supply and protection of Critical National Infrastructure.

Teams and resources

This project continues a partnership between NESO, Cambridge Consultants, and the University of Edinburgh. No new partners are envisaged; however additional third-party stakeholders will be engaged to provide supporting input and feedback, with possible consideration for inclusion as partners in Beta.

There will be no subcontractors.

No additional resources, equipment or facilities will be required for Alpha.

NESO

NESO, the project lead, is the electricity system operator for Great Britain, ensuring continuous, reliable and secure system operation across the UK. The move to National Energy System Operator will soon expand NESO's role to cover the whole-energy system. The NESO will use their expert knowledge of Critical National Infrastructure (CNI) and system operation to steer the project to produce useful outcomes for the NESO and the wider energy industry. The NESO's Chief Information Security Officer (CISO), Simon Lambe, and his team, including members of the E3CC, will identify and test relevant use cases, and develop user stories, to ensure robust outputs. Alongside overall project management, the NESO will also be responsible for project governance and wider industry stakeholder engagement.

Cambridge Consultants (CC)

CC is a deep-tech engineering consultancy working across multiple industry sectors, with departments specialising in both cybersecurity and quantum computing. CC will provide the interface between the major workstreams, drawing on their broad team, which includes specialists with experience of the NESO's cybersecurity threat/cost assessments. Furthermore, CC is part of the UK quantum industry body UKQuantum, with members on the steering committee. CC has 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. The project will also leverage CC's statistics expertise and insights into decision-making under uncertainty, both of which will be important in developing the relevant methodologies within this project.

CC will continue to be a key delivery partner during the Alpha phase, focusing on the design and implementation of the Quantum-Aware Risk Management demonstrator tool.

University of Edinburgh (UoE)

UoE is a leading research university with specialisms in quantum computing and power systems. UoE hosts the Quantum Software Lab, a research centre focused on exploiting quantum computers to solve problems beyond the reach of classical machines. UoE will use their experience in cryptographic quantum computing to provide input to the project on methodologies for understanding and assessing the quantum threat. The UoE team will also leverage their power systems expertise to focus on ensuring clear mapping of the specific challenges quantum poses to energy networks.

New external parties

Several key parties have been identified to provide additional guidance and input, to ensure the developed PoC is appropriate and usable across the UK energy network and will be considered for a closer role in Beta:

- UK Cyber Security Task Group (E3CC): Will be involved in providing stakeholder review and feedback as a potential user of the Quantum-Aware Risk Management tool (Q-ARM). The group includes 24 energy system operating companies from across the UK market, and members of UK government bodies and regulators including the National Cyber Security Centre (NCSC). We will seek their input to ensure the operational value and usability of Q-ARM as target end-users. This involvement will provide engagement over a wide stakeholder group, ensuring the project's applicability beyond a single generator.
- National Gas Transmission (NGT): Will be involved in providing stakeholder review and feedback as a potential user of Q-ARM. This will help the consortium to extend the scope of the tool's relevance to a broader range of energy vectors.

Project Plans and Milestones

Project management and delivery

Delivery and approach

The project is split into five parallel work packages each utilising a waterfall approach, sharing project resources, research and governance.

WP1: Quantum--Aware Risk Management (Q-ARM) Modelling tool (CC lead)

Aim:

- Development and demonstration of a Proof-of-Concept (PoC) tool for identifying and prioritising mitigation strategies against quantum risks to energy networks.

Tasks:

- Capture overall tool requirements through stakeholder workshops, create detailed process workflow (identify asset groupings/characteristics, assess quantum threat, and identify risks and possible countermeasures). Develop this into a PoC demonstration tool, and test on two test cases (WP3).

Milestones/Deliverables:

- PoC Q-ARM tool
- Supporting documentation
- Test case performance Report

Success:

- Tool can interpret the quantum threat and possible countermeasures for the test cases.

WP2: Quantum Threat Tracker (QTT) (CC lead))

Aim:

- Produce PoC tool to enable tracking of quantum threat, to feed into Q-ARM tool (WP1).

Tasks:

- Capture overall tool requirements and outputs to Q-ARM tool, specifically a dynamic estimate for time-to-attack (length of time to development of a cryptographically-relevant quantum computer) and time-of-attack (time to initiate and deploy a quantum-enabled attack when this becomes possible). Initial configuration will analyse impact of two specific recent quantum computing developments. PoC tool output will be a scenario configuration file for ingestion into the Q-ARM to enable decision making.

Milestones/Deliverables:

- PoC QTT tool
- Architecture and guidance documentations

Success: tool is able to create configuration files for different quantum threats.

WP3: Energy system specification and product ownership (NESO lead)

Aim:

- Develop relevant test cases for PoC tools, focussing on energy systems requirements.

Tasks:

- Starting with a requirement workshop to define scope boundaries, generate two energy system test cases to test performance of Q-ARM tool (WP1). This will ensure relevance of the project to the energy network, without compromising sensitive Critical National Infrastructure (CNI) data.

Milestones/Deliverables:

· Two test cases for use in the Q-ARM

Success:

- Satisfactory comparison of generated test cases to scope defined in workshop.

WP4: Impact/Benefit Analysis and Roadmap (CC lead)

Aim:

- Create roadmap for further development of tools through Beta into BAU and analyse benefits of the solution.

Tasks:

- Leveraging the planned stakeholder engagement, produce a detailed report on development and deployment roadmap, including updated comprehensive cost/benefit analysis.

Milestones/Deliverables:

- Roadmap to BAU
- Updated cost/benefit analysis

Success:

- Demonstrate benefit and structure suitable Beta phase.

WP5: Project Management, Governance, and Stakeholder Engagement (NESO lead)

Aim:

- Project Governance and Stakeholder Engagement.

The project will be led by the NESO, who will assign a dedicated project manager, responsible for project coordination, governance and dissemination. Regular steering meetings will be held to review progress, alignment of output and review risks.

Key Tools:

- SharePoint; NESO PMO Framework.

Milestones/Deliverables:

- Kick-off/Progress/Monitoring meetings
- Stakeholder Engagement Plan
- Project Completion

Success:

- Completion on-time and within budget.

Risk Management

Risk Management will be a continuous process, monitored and actively maintained by the PM using an Identify, Assess, Control, Record approach. Risks will be a standing item at the regular progress meetings. Mitigation activities, owner assignment and progress will be discussed. Escalation to senior management will be utilised as required.

Key risks

- Project test cases may involve CNI and commercially sensitive data.
- Progress delays due to sharing sensitive information between partners quickly.
- Getting access to/contribution from key stakeholders.

(Detailed risk table in PMT).

Supply Interruptions & Access to Energy Services

The project itself will not impact access to energy services nor require any direct or indirect supply interruptions, as it will not involve direct interaction with the energy network. However, it is designed to develop tools to help ensure that consumers have access to the energy services and connections they require, through the effective use of risk mitigation for Quantum threats.

Key outputs and dissemination

Achievements

At the end of the Alpha phase, this project will have built a set of Proof-of-Concept (PoC) software tools and frameworks demonstrating the future development pathway. These will be validated on two relevant energy network test cases. Key achievements will be:

- Quantum-Aware Risk Management Tool (WP1): This work package will develop and refine both the process for carrying out a quantum-aware risk management assessment, and a supporting demonstrator software tool (the Q-ARM tool). The Q-ARM tool will take the complex information generated by the Quantum Threat Tracker (see below), provide actionable insight for a given asset or piece of infrastructure, and identify where this should be integrated into current cybersecurity operations. To facilitate this, we will develop (or identify) an asset register, quantum-enabled Tactics, Techniques and Procedures (TTPs), and potential mitigation strategies.
- Quantum Threat Tracker (WP2): We will develop and document an architecture for a Quantum Threat Tracker (QTT) module, which will feed quantum technology information into the Q-ARM tool. The QTT will allow users to update the quantum threats, explore potential future scenarios and query the tool about sensitivities. The architecture will clearly highlight how future quantum computing developments can be updated and integrated. The initial PoC implementation will focus on two relevant recent developments in quantum computing: Chevignard's improvement to Shor's algorithm and quantum Low Density Parity Check (LDPC) codes. It will demonstrate the benefit of a modular approach and provide up-to-date estimates (time-to-attack and time-for-attack) for use with the Q-ARM tool.
- Impact/Benefit Analysis and Roadmap (WP4): We will quantify the benefit of this approach for the energy industry, building on the initial business case presented in the CBA submitted with this application. We will also provide a comprehensive roadmap detailing the path to uptake across the energy sector, within BAU cybersecurity processes.

Alpha outputs

The following will be used to disseminate learnings to the wider community:

- PoC demonstration software (delivered by CC and UoE).
- Several demonstration workshops (delivered by the NESO and CC) where the software can be trialled by appropriate stakeholders.
- Supporting deck for the workshops (produced by the NESO) detailing a roadmap to BAU integration and the pathway to widespread adoption . This will enable conversations/planning around future cybersecurity integration.
- A report (compiled by CC) detailing findings from the task of generating the inputs for the Q-ARM tool, including the asset registry, quantum-enabled TTPs and the associated mitigation strategies.
- A report (compiled by CC) detailing the designed process/ workflow for the Q-ARM tool and the PoC demonstration, for two energy network test cases. This will outline the methodology, and how to implement the workflow. It will include a detailed description of future implementation considerations for Beta, and potential integration pathways for BAU.
- A report (compiled by UoE) detailing the modular architecture for the QTT module, describing how future quantum computing developments can be incorporated on an ongoing basis. This report will detail the latest estimates of the 'time-to-attack' and 'time-of-attack' based on the PoC.

Dissemination

- Reports shared on the ENA Smarter Networks Portal.
- Presentations at relevant forums including Energy Emergencies Executive Committee (E3CC) and the Electricity and Gas Networks Forum.
- Two sector-wide workshops to be arranged in conjunction with E3CC. The first will be for mid-project review to enable wider stakeholder engagement; the second will be detailed dissemination of developments and BAU integration plans .
- A poster and briefing material for Innovation events attended by the NESO.

Project outputs will also be disseminated across the public domain in accordance with SIF governance requirements (including the end-of-phase show-and-tell), ensuring that key knowledge gained in the Alpha phase will not undermine development of competitive markets.

Commercials

Intellectual property rights, procurement and contracting (not scored)

The Proof-of-Concept demonstrator will not be ready for direct commercial exploitation at the end of the Alpha phase. As such, it will not require ongoing software maintenance or licencing. However, the demonstrator will provide the basis for a software tool to be deployed in the Beta phase.

The ownership of IPR generated shall obey the terms and conditions of Chapter 9 of the SIF Governance Document. The mechanism for recording and assigning any IP created during the Alpha phase will be agreed between project partners alongside the project contract.

Procurement and Contracting

As noted, while not required for Alpha, it is not yet known whether any hosting or other services will be required for Beta or into BAU. This will be assessed and reviewed as part of Work Package 4 (Impact/Benefit Analysis and Roadmap).

Commercialisation, route to market and business as usual

Path to Business-As-Usual (BAU)

Post-Beta, the proposed Quantum-Aware Risk Management (Q-ARM) tool and Quantum Threat Tracker (QTT) will serve as part of energy network operators' BAU cybersecurity planning toolkits. The tool will provide decision support for risk management.

The Alpha demonstrator will be developed based on existing energy sector cybersecurity frameworks and workflows, enabling energy network operator cybersecurity teams to incorporate quantum threat intelligence.

Specifically, it will enable them to evaluate and mitigate for quantum-enabled threats to different energy network asset classes, via specific types of attacks, and to prioritise these based on 'time-of-attack' (the time when a cryptographically-relevant quantum computer becomes available), and 'time-to-attack' (the amount of time that a cryptographically-relevant quantum computer needs to break a specific encryption scheme).

Integration with existing processes will be achieved through cyberattack Tactics, Techniques and Procedures (TTP) scenarios for attacks enabled or enhanced by quantum computers. TTPs are already regularly used within energy network security workflows. The MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) Framework that models TTPs is already used by energy sector stakeholders. This approach will therefore ensure compatibility with existing processes.

Collaboration with the UK Energy Emergencies Executive Cyber Security Task Group (E3CC) will give the consortium insights into how the sector incorporates threat intelligence into architecture, future planning and business processes. These insights will ensure reduced uncertainty and cost-effective interventions to manage quantum threat risk.

Commercial Model

The commercial model for adoption will be fully detailed and explored in Alpha. The intent is for the tool to be widely used to benefit the entire sector. Network operators could, for example:

- Pay a nominal licensing fee to have access to the Q-ARM tool and/or QTT.
- Gain access to the tool(s) in exchange for contributing data or scenarios, e.g., asset class grouping information, TTPs.
- Join a 'post-quantum energy cybersecurity' consortium where members gain access to the tool as part of membership.
- Gain access to the tool via an existing industry cybersecurity association such as E3CC.

Commercial partnership agreements may be needed for future post-Beta adoption of the tool. It may be necessary for one party (e.g., NESO) to host the Q-ARM tool and QTT module. Key will be clearly assigning responsibility for tool maintenance, updating, adaptation/expansion and refinement/error correction. This will be explored in Alpha and eventually Beta, with findings forming part of Alpha WP4 output.

Partner readiness and scaling

BAU adoption and scaling requirements will include, but are not limited to:

- Ongoing programme to maintain and update Q-ARM tool.
- Representation of all relevant energy network asset classes within the tool.
- Creation of representative quantum-enabled attack TTPs, with regular review and updating.
- Regular updating of QTT to reflect impact of latest quantum developments.
- User feedback capture process.
- Process for corrections and improvements in the tool and supporting documentation.
- Dissemination and training for energy sector end users, to enable successful adoption and integration into ongoing cybersecurity processes, mitigation planning and investment planning.
- Resources to host the tool, and to manage users and data in a compliant manner.

The project will therefore engage with the NESO's DD&T (IT) team. Initial exploratory discussions with partners and other potential stakeholders and the requirements for any supporting partner resources will be outlined in Alpha WP4. NESO will utilise its newly formed Innovation Incubator team to ensure outcomes are successfully delivered and integrated into BAU.

Senior sponsorship

The business sponsor is Simon Lambe, NESO Chief Information Security Officer (CISO). Simon has been guiding the design and ensuring it addresses business needs. Simon will own the vision and direction for the project and is responsible for successful implementation.

Policy, standards and regulations (not scored)

We do not believe that the proposed work presents any barriers to meeting the requirements of regulations, policy or standards, in the Alpha or Beta phases.

The output will be a decision-making support tool to guide Post-Quantum Cybersecurity (PQC) decision-making for energy network cybersecurity and IT teams. There are no currently applicable standards to be considered other than commonly applied cryptographic standards that could be subject to quantum-enabled cyberattacks, which will be fully taken into consideration in the work.

The National Cyber Security Centre Cyber Assessment Framework (NCSC CAF) contains mandatory cybersecurity goals for the operators of all Critical National Infrastructure (CNI) in the UK. The current version (v3.2) contains several actions that are related to this work. For example, within CAF objective A "Managing security risk", subsection A2.a "Risk management process", there is an objective which states "Your organisational process ensures that security risks to network and information systems relevant to essential function(s) are identified, analysed, prioritised, and managed." This project clearly contributes to the integration of quantum-enabled security risks into that process. Throughout the programme, the CAF will be monitored to ensure that all project's outputs support its objectives. There is little risk of accidental non-compliance for this programme, as the CAF is largely process-agnostic, focussing on outcomes rather than methodologies. In addition, the latest revision was issued in April 2024, and it is typically updated at approximately 3-year intervals, so an update is not expected within the Alpha phase but is possible within the Beta phase.

Whilst not a standard, current guidance from the NCSC contains two relevant pieces of guidance:

- Firstly, the NCSC cautions against the early adoption of PQC before it has been officially endorsed by the National Institute of Standards and Technology (US). The decision support tool we will develop shall repeat this advice to users by adding a note to any PQC mitigations.
- Secondly, the NCSC position on quantum-key distribution (a technology with the potential to overcome a subset of the challenges posed by quantum computers) is that, not only should it not be used at the current level of technological readiness, but also that its use may not be used as evidence of compliance to the CAF data in transit security principle. We shall continue to respect this guidance and not offer quantum key distribution as a potential mitigation for this threat.

In summary, the team will pay close attention to relevant security laws when proposing mitigations for potential cybersecurity threats. Overall, however, the goal of the work is to enable better delivery/enforcement of policy and regulation around data security and energy network cyber resilience.

Derogation

Owing to the nature of the project, the NESO do not anticipate the need for a derogation.

Value for money

- Total project cost: £553,628
- Funding requested: £498,264 (90%)
- Total contribution: £55,364 (10%)

Balance of costs:

NESO (Lead Partner)

- Total cost: £119,789 (22% of total)
- Contribution: £11,979 (10%)
- Funding requested: £107,810 (90%)

CC (Partner 1)

- Total cost: £336,451 (61% of total)
- Contribution: £33,646 (10%)
- Funding requested: £302,805 (90%)

UoE (Partner 2)

- Total cost: £97,388 (17% of total)
- Contribution: £9,739 (10%)
- Funding requested: £87,649 (90%)

There will be no subcontractors utilised in the delivery of NSiaQF Alpha.

Contributions

All partners are making a 10% contribution. These contributions will be funded by:

- NESO through their network innovation budget.
- CC by discounting commercial rates.
- UoE by discounting Full Economic Cost (FEC) rates

The costs compare favourably to normal industry rates. As a Commercial Partner, CC's rates are competitive with other innovative businesses and UoE partners are utilising FEC rates that represent a significant reduction on commercial rates for innovation work. NESO have benchmarked pay approved by Ofgem.

Value-for-money for 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).

In addition, there is a significant benefit to the energy sector as well as to energy end-users, through more effective and efficient defence of the UK energy network against cyberattacks. This was discussed in more detail in the supporting CBA document, which estimates a Net-Present Value (NPV) of £878,455,958.

Discovery showed that quantum computers will enable cybersecurity threats against the energy sector by breaking current public key cryptography, enabling potentially catastrophic attacks such as network shutdown by malware or market manipulation through message tampering.

The UK National Risk Register 2023 estimates the cost of a cyberattack against UK critical infrastructure could run to “hundreds of millions of pounds”, causing 81-400 casualties and 41-200 fatalities.

Additional Funding

No additional funding from other innovation funds has been sought.

Existing Assets

No pre-existing assets will be utilised in the delivery. Knowledge of existing approaches and cybersecurity processes will be made available as required from the NESO Subject Matter Experts.

Associated Innovation Projects

- (•) Yes (Please remember to upload all required documentation)
- ( ) No (please upload your approved ANIP form as an appendix)

Supporting documents

File Upload

No documents uploaded

Documents uploaded where applicable?

☑