SIF Discovery Round 2 Project Registration

Date of Submission

Apr 2023

Project Reference Number

10061439

Project Registration

Project Title

Looking-Glass

Project Reference Number

10061439

Project Licensee(s)

SGN

Project Start

Apr 2023

Project Duration

2 Months

Nominated Project Contact(s)

stuart.sherlock@sgn.co.uk

Project Budget

£118,557.00

Funding Mechanism

SIF Discovery - Round 2

SIF Funding

£88,007.00

Strategy Theme

Data and digitalisation

Challenge Area

Improving energy system resilience and robustness

Lead Sector

Gas Distribution

Other Related Sectors

Funding Licensees

Lead Funding Licensee

SGN - Southern England (inc South London)

Collaborating Networks

SGN

Technology Areas

Asset Management, Control Systems, Cyber Security, Digital Network, Network Automation, Resilience, System Security

Equality, Diversity And InclusionSurvey

Yes

Project Summary

In response to Aim 4 of Challenge 3, this innovation project focuses on development of a repeatable measure of the effectiveness of active cybersecurity controls. We will use these measures to derive a robustness score.

Additionally, innovation and technological advancement is delivered through developing software applications that will provide this trusted assessment automatically and at scale. These applications will be delivered, across hundreds of geographically distributed assets, as part of the Phoenix ecosystem at the site edge and in the cloud. Phoenix, built and maintained by deltaflare, is a software-defined security platform currently in use within the Critical National Infrastructure.

Enabling a deep understanding of the network robustness will underpin the cybersecurity required for secure digitalisation towards reaching Net Zero.

SGN, the project Energy Network Licensee, is one of the largest utility companies, distributing natural and green gas safely and reliably through our 74,000km of pipes to 5.9 million homes and businesses across Scotland and southern England. SGN's plans to transition to digitalised future networks requires robust and resilient networks.

Deltaflare, the industrial partner, are recognized within the UK utility and cybersecurity domains for their innovative approach and expertise. They support Ofgem on NIS inspections and deliver cybersecurity guidance to the industry through the NCSC. Our founders are elected by the UK gas industry to act as the Competent Design Authority for OT cybersecurity.

SGN has been working with deltaflare and has trialled the use of Phoenix to deliver enhancements to its network resilience and robustness. SGN will provide access to their facilities and resources as required across the life of the project.

The Ministry of Defence (MOD) is a government department led by the Secretary of State for Defence. Nested within Strategic Command and Defence Digital, the Cyber Resilience Programme (CRP) aims to substantially reduce risk, protect critical assets and systems and develop a cyber-aware workforce that will allow MOD to make cybersecurity part of the DNA of its business and operations.

The MOD CRP are a non-funded partner in this project who will provide cross-domain expertise during the Discovery phase of the project and will disseminate the learning during later phases.

This project challenge is shared between all operators of essential services. When successfully exploited, the outcome of this innovation project could be used by all gas and electricity operators to gain live view of their network robustness in their journey to Net Zero.

Project Description

We recognise the UK's energy infrastructure will be undergoing significant changes to facilitate a low carbon future and therefore requires us to understand the importance Cybersecurity will play in ensuring safety supply.

Cybersecurity risks and regulatory obligations (NIS Regulation 2018) have compelled business to invest in cybersecurity safeguards. The real-time effectiveness of these controls in reducing the risk is not currently measured. Therefore, businesses are unable to ascertain their robustness or establish the efficiency of their investments.

As businesses adopt smart technologies and hyperconnectivity to reach Net Zero, they increase their chances of cyberattacks. Lack of robustness and resilience measure in the face of such cyber risk, is a challenge to businesses.

Project Looking-glass will develop novel techniques and technology to quantitively measure the performance and effectiveness of security controls helping the Networks maintain security during the Net Zero transition.

In this project, we will build upon the existing software defined everything (SDx) infrastructure that the Phoenix platform provides, to overcome this challenge. Phoenix is being trialled at SGN facilities to provide cybersecurity and operational betterment as part of their digitalisation roadmap.

This project will embrace innovative use of big data analytics and machine learning techniques to measure the effectiveness of cybersecurity controls. We will devise formal repeatable measurement indicators to quantify the efficacy of cybersecurity control.

This innovation project applies maturing techniques and technologies from other domains to the field of Operational Technology (OT) cybersecurity and business robustness. We will capture human behaviours, security intelligence, and operational datasets to provide an automated computation at scale.

The success of this innovation project will provide SGN with objective measure and awareness of its robustness. It will accelerate uptake of the right security controls that underpins the hyperconnectivity required to meet Net Zero targets for SGN and other network operators.

Third Party Collaborators

Deltaflare

MOD Cyber Resilience Programme

Nominated Contact Email Address(es)

sgn.innovation@sgn.co.uk

Project Description And Benefits

Applicants Location (not scored)

Southern Gas Networks

St Lawrence House, Station Approach, Horley, England, RH6 9HJ

deltaflare limited

Oriel House, 26 the Quadrant, Richmond, England, TW9 1DL

MOD Cyber Resilience Programme

MOD Corsham, Westwells Rd, Corsham SN13 9GB

Project Short Description (not scored)

Project Looking-glass will provide real-time assessment of Network Operator's resilience and robustness through big data analysis of infrastructure and security data, ensuring the Networks are secure during the Net Zero transition.

Video description

https://youtu.be/bP9kHIQI4N0

Innovation justification

Following the enactment of the Network & Information System (NIS) regulations in 2018, the cybersecurity regulators have been working with Operators of Essential Services (OESs) to increase the resilience and robustness of their networks. The operators have adopted security controls based on their risk exposure.

Selecting of appropriate and proportional cybersecurity controls, and the assessment of their effectiveness is challenging. The skill-sets, time, and technologies required to carry out these assessments place a large burden on the operators. Lack of resources leads to such assessments not being carried out adequately or at all.

This project will create formal methodologies to derive a quantitative score of active security controls' effectiveness. Our Phoenix platform will ingest operational and security data to use in its analytics and machine learning engine to measure the effectiveness of each active security control.

This will be translated into resilience and robustness and would provide SGN with real time knowledge to make decisions on how to best maintain and increase the security of their facilities.

This project is novel as it provides a change of mindset around the way OT cybersecurity is viewed and procured. It challenges the current approach that assumes security until failures occur. Instead, it provides the tools to adopts an assurance and pre-emptive mindset. It delivers new technologies to practically measure the effectiveness of cybersecurity controls through hardware and software monitoring, human behaviour, and big data analytics.

Our project will provide the techniques and technological advancement to assess, maintain and procure cybersecurity controls in a way that has not been carried out before. This will reduce costs to the operators and create economic value for the UK.

Due to the innovative approach, this style project would normally have a risk profile that is too high for BAU or other funding methods. In addition, if the project were funded under BAU or other methods, it would take significantly longer, and the solutions would arrive too late to enable effective transition to net zero. This project addresses a current challenge by the gas and electricity operators and the outcome would benefit the networks and Ofgem.

The staged approach from feasibility to trial and to full roll-out makes it suitable for the SIF funding mechanism. It allows SMBs to deliver innovation to large operators such as SGN.

Benefits Part 1

Financial - cost savings per annum on energy bills for consumers
New to market – products, processes, and services

Benefits Part 2

The net value to the Consumers would be measured against a number of Key Performance Indicators (KPIs) associated with the selected benefits. During the Discovery Phase these KPIs would be evolved and tuned to provide a more accurate assessment.

The industry is widely believed to be on the verge of a life-threatening cyber-attack (reference Gartner prediction by 2025 study). The measure of avoided cybersecurity-related losses would be established by taking into account:

- quantified cost of losses as considered within SGN OT cyber risk assessments
- quantified cost of losses as captured in SGN hazard and consequence analysis
- global moving average of industrial cyber events
- risk avoidance cost associated with currently unmonitored cybersecurity controls

During the Discovery phase, the above would provide a justified quantitative measure of the costs saved by the networks and consumers. We would also carry out a market study on the value that would be generated by offering this new technology to the national and international market as a measure of economic value.

During the Alpha phase, we will use the existing Phoenix install bases to measure the demand put on each security control and calculate the cost to the network associate with the failure of those controls. This would provide an empirical justification and tuning of the potential for cost savings.

The full extent of the cost savings related to the avoided losses would be realised during the Beta phase when the entire network is protected.

The overall spend on smart technologies and OT cybersecurity enhancements in the RIIO-2 regulatory period is estimated to be more than £1b across all the regulated gas and electricity operators. This forecast is based on current cybersecurity monolithic procurement model.

We anticipate being able to rollout this solution across the entire SGN network by the end of RIIO-GD2 period. During the Beta phase, we will measure the effectiveness of controls selected in the RIIO-GD2 to provide an analysis of potential cost saving that would have been achieved by selecting the right controls. We would use this learning to enable SGN to select addition controls during RIIO-GD3.

At this stage we would be able to show that a considerable cost saving (estimated at 15%) would be achieved in funding request in the new funding period.

Project Plans And Milestones

Project Plan and Milestones

The Discovery phase of this project will be executed across 3 work packages. A quality management plan will be put in place to track the objectives, timeline, and deliverables. The project teams will meet frequently to discuss requirements and to review the risk register.

Project Work Packages (WP) are as follows:

1- Data Capture -- Lead: deltaflare, Output: Report, Funding: £13,262

We will carry out an assessment and collation of cybersecurity controls deployed across different tiers of SGN facilities. This will be categorised based on the risk avoided, type of site, and number of consumers.

SGN will support this phase by providing input documentation and resources.

2- Assessment Methodology -- Lead: deltaflare, Output: Report, Funding: £50,768

We will select the top 8-10 current and future planned controls and develop the methodologies and techniques for assessment of their effectiveness. We will calculate the test coverage of these tests to use in our cost benefit calculation.

The assessment techniques will consider technology and people/processes type controls. Technological controls will be assessed based on how hardware and software systems empirically function.

People and processes related controls will be analysed using the Machine Learning (ML) engine of Phoenix. Therefore, this phase will study and ascertain the behavioural indices and data sources that would be available during Alpha phase. It will also define the data preparation, training, and validation stages during Alpha.

Testing specification and requirement for the Big Data Analytics and Machine Learning engines will be devised in this work package.

The MOD will provide expertise in the selection of applicable security controls used in the Defence Industry and support in devising techniques for implementation in the Alpha phase.

The main risks to this phase of the works is inadequacy of available data for machine learning.

The success of this WP will be the development of repeatable techniques to be implemented in Alpha.

3- Feasibility Study -- Lead: deltaflare, Output: Report, Funding: £23,977

We will carry out a feasibility study and cost benefit analysis for the trial of this technology and approach in the Alpha phase and full roll out in Beta phase.

SGN will support this phase by ensuring that the feasibility and roll out plans take SGN business requirements into account.

No major constraints have been identified for this Phase of the project. We are able to work flexibly and in parallel on aspects of these WPs to de-risk the project delivery.

Regulatory Barriers (not scored)

We are confident the proposed innovation would not provoke any regulatory barriers that could affect or hinder delivery of either the Alpha or Beta phases.

The regulations applicable to this project is the Network Information Systems (NIS) Regulations 2018. These regulations requires Operators of Essential Services (OESs) to build and increase their resilience and robustness. As such this project is fuelled by the requirements placed upon OESs. It helps to enhance their capability to respond to their legal obligation.

The SMEs of the project team work closely with NCSC, and the NIS regulators and maintain a close relationship with the DCMS and BEIS. We will continue to input into the official guidance provided to the Operators and stay abreast of upcoming changes to the regulations.

The project team will also be working closely with internal SGN stakeholders including Policy, IT, Energy Futures and Hydrogen teams, to help consider any policy and procedural impact.

As this project and innovation is trialled and rolled out, it will substantially increase capability of the Network Operators and the regulator to respond to changes to the regulations. We anticipate that this affordable increase in capability would result in raising of the bar, leading to tighter regulations, and thus achieving a higher resilience and robustness of the UK energy systems.

Commercials

Route To Market

The challenges identified in this project submission are applicable to all industrial automation where cybersecurity is identified as a risk. Specifically, Operators of Essential Services such as SGN, that are governed by the NIS Regulations 2018 would be legally required to demonstrate deep understanding of their resilience and robustness and plan for adoption of future controls.

The interest from the MOD, the project's non-funded partner, further highlights the applicability of this technological innovation in other markets.

The output of this project will not hinder but foster and encourage development of competitive markets. The capability to measure the performance of cybersecurity technologies, unlocks new smarter procurement campaigns that will benefit suppliers.

Regular engagement with business stakeholders is key to ensuring a successful adoption within the business. The project team will achieve this by holding regular workshops throughout the project during Discovery, Alpha, and Beta phases. This proactive approach will be coupled with regular assessments of the benefits.

The dedicated SGN Innovation Project Manager will be responsible for the implementation of this project and will be supported by the Innovation PMO. SGNs Innovation team are well established through experiences from other funding routes such as NIA and NIC and have developed a good working relationship with key business areas to ensure successful implementation. We also have a capable and broad knowledge of SGNs business activities, as well as the wider energy network industry in the UK.

Learnings will be disseminated to other licensees and the MOD through providing regular project updates. The adoption of any project learnings will be supported by maintaining effective levels of communication with relevant stakeholders and interested parties through regular update and showcase meetings/forums.

Our project partner, deltaflare, have extensive experience in design, delivery, and assurance of OT and OT cybersecurity solution for the UK Critical National Infrastructure. They provide OT cybersecurity subject matter expertise into standard bodies, governmental agencies (NCSC, Ofgem) and numerous Operators of Essential Services. deltaflare builds and supports the Phoenix platform, a software-defined platform that delivers OT security controls and operational functionality to industrial plants.

The project team are also engaged with several network review groups who have a common desire to improve system resilience. These forums will also help the review and adoption of any developed solutions.

The continued internal engagement during Discovery and Alpha phases ensures business readiness for adoption of this innovation into Business as Usual as part of Beta.

Intellectual property rights (not scored)

Each Project Partner shall own all Foreground IPR, including Phoenix platform components, that it independently creates as part of the Project, or where it is created jointly then it shall be owned in shares that are in proportion to the work done in its creation. The exact allocation of Foreground IPR ownership will be determined during the contractual negotiations with the Project Partners on the agreement for the project.

We intend to ensure each Project Partner will comply with Chapter 9 SIF Governance Document through the contractual terms governing the project. However, precisely how this is done will be subject to contractual negotiations with the Project Partners on the agreement for the project.

Costs and value for money

Cost: The overall project cost is £118,557. A total project contribution of 25.8% has been made meaning total SIF funding requested is £88,007.

Balance of Costs: The majority of the deliverables will be created by deltaflare with support from UK MOD with all deliverables being assured and implemented by the lead partner SGN.

Partner Costs: A summary of each partners costs and contributions are outlined below.

SGN

- Total Cost: £13,056
- SIF Funding Requested: £13,056

Deltaflare

- Total Cost: £105,500
- SIF Funding Requested: £74,950

UK MOD

- Total Cost: Support given free of charge as Project Sponsor.

Value for Money: This project aims to apply an automated approach to cybersecurity, providing increased robustness and security of supply to customers during the net-zero transition. The innovation involved in developing this system it is crucial for securing energy supply.

Deltaflare has elected to provide considerable funding towards the implementation of this projects as part of its R&D efforts. We believe in the value that this project bring to the Networks and UK resilience and robustness in the face of cybersecurity risks. As leaders in this field, we feel it is our duty to support the UK's ambition to securely digitalise its Critical Infrastructure.

The monetary and intellectual contribution of the project partners provide clear indication of value delivered in this phase and future phases of this innovation project.

Document Upload

Documents Uploaded Where Applicable

Yes

Documents:

SIF Discovery Round 2 Project Registration 2023-04-12 4_57

Looking-glass-Show-and-Tell.pptx

This project has been approved by a senior member of staff

☑ Yes