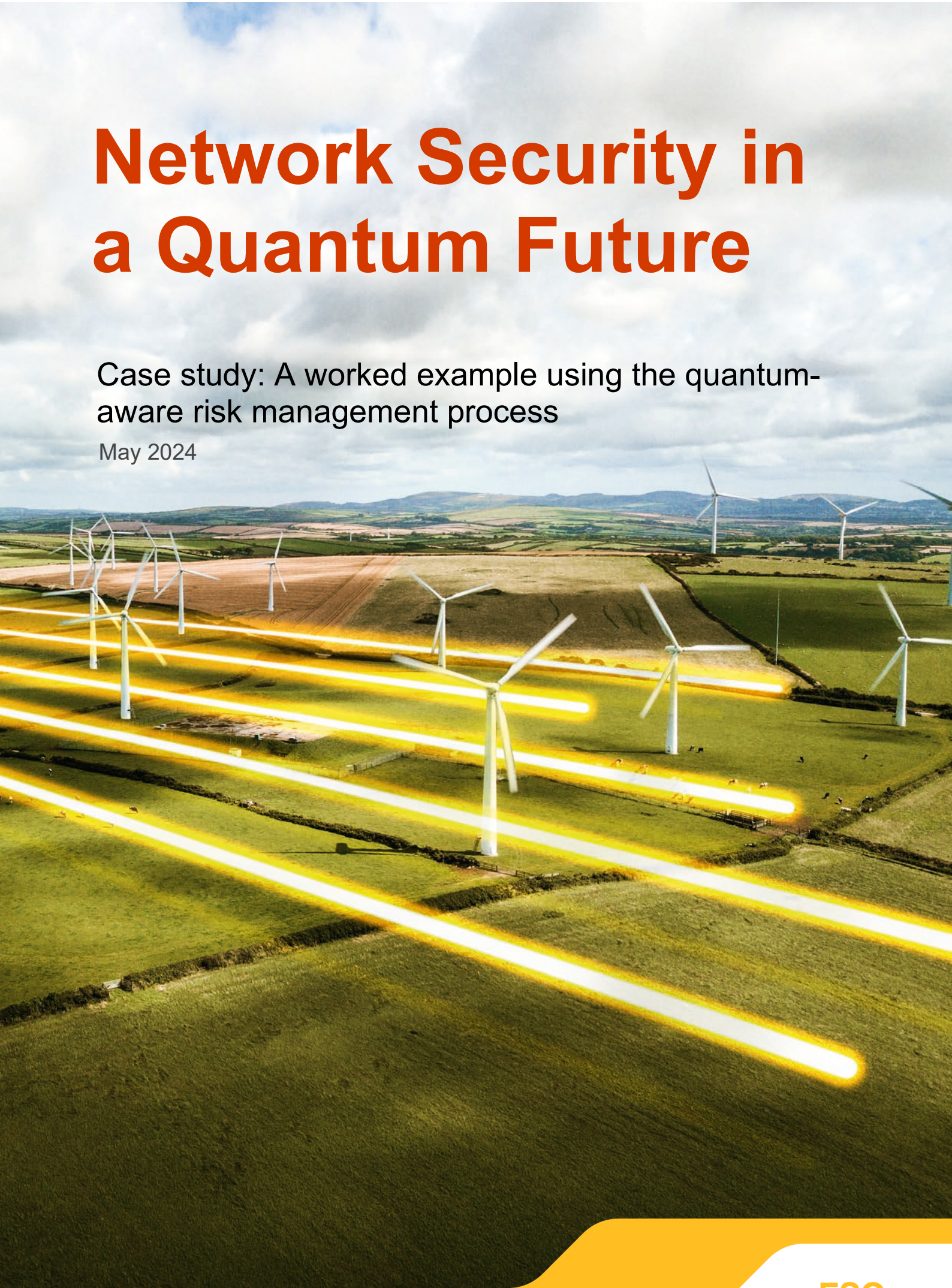
Network Security in a Quantum Future

Case study: A worked example using the quantum-aware risk management process

May 2024



ESO

Ofgem Strategic Innovation Fund Contributing Partners

ESO	National Grid ESO
cambridge consultants Part of Capgemini Invent	Cambridge Consultants
THE UNIVERSITY of EDINBURGH	University of Edinburgh
WARWICK THE UNIVERSITY OF WARWICK	University of Warwick

Executive Summary

Quantum computers promise to deliver an entirely new paradigm in computing, enabling problems that were previously intractable on traditional computers to be solved in far shorter timescales. This new technology will bring many benefits through its ability to deliver extremely powerful and rapid computation. But it will also open up a critical threat: quantum computers will be able to undermine the mathematical foundations of widely-used cybersecurity approaches such as public-key cryptography (PKC), exposing currently-protected assets to significant risk of attacks.

This is of particular concern for the energy sector, given the long life and diversity of energy network assets, the widespread use of PKC in energy network cybersecurity schemes, and the high likelihood of energy networks being targeted for cyberattacks by malicious actors. This challenge is the focus of our Ofgem SIF Discovery Project, **Network Security in a Quantum Future**.

Energy sector stakeholders need to respond to the threat posed by cryptographically relevant quantum computers (CRQCs) in a timely, but fiscally responsible way. To do this, it is necessary to first characterise the risk using a clear framework or process that takes into account the needs and types of assets within energy networks. This will then enable priorities to be assigned, and appropriate mitigations to be linked to vulnerable systems.

In our sister report under this Discovery project, "Assessing the cybersecurity implications of the quantum threat to the energy network," we have presented an initial framework for undertaking such assessments – which we have called the Quantum-Aware Risk Management process. We developed this framework based on both existing risk management frameworks, and our team's research into the nature and control of quantum-enabled threats.

In the supplementary **Worked Example Case Study** report presented here, we demonstrate how the process could work in practice on a (fictional) exemplar system (referred to in this report as the 'System of Interest') that illustrates a likely energy system use case – in other words, a system within the energy network, that needs to be assessed for vulnerability to a post-quantum attack, and to have appropriate mitigations identified and put in place.

Our selected exemplar/System of Interest is based on the balancing system for the grid. Components are:

- An "Internal system" - power balancing system operated by NGESO.
- An "External entity" - large power generation facility.
- The "Web services" of the "external entity" – these process bids and offers from the balancing system to generate more power on the grid.
- The "Management system" - provides operational metering data about the energy generated, to the balancing system.
- We assume all communications are performed using TLS encryption to secure JSON (Java Script Object Notation) payloads containing the relevant data.

We identified seven potential post-quantum attack scenarios for the System of Interest and worked through each of these to assess technical likelihood, impact level, and mitigations, supported by a structured asset model.

The resulting analysis enables us to draw initial conclusions about the potential usability and effectiveness of the proposed process, and how it might support an energy network operator looking to use this approach to quantum threat assessment and mitigation planning.

Our key findings from this case study are:

- The Quantum-Aware Risk Management process, as currently outlined, offers a strong starting point for developing an effective tool to support energy network operators in addressing the quantum threat.
- However, there are some areas that would need to be addressed in future development phases, to enable improved usability and wider applicability:
    - The process is currently heavily manual and requires a large amount of analysis, even for simple systems. Future development should consider automation and simplification of some

aspects of the approach, supported by appropriate software tools, to ensure that the entire energy system can be assessed in a feasible timescale.

  - Selecting the correct mitigation for a specific system requires the assessor to understand the bandwidth and computational limitations of the system, and the impact that the different mitigation types will have on those properties. This may require training and support, as well as clear guidance and supporting information provided within the tool itself.
  - The current process does not address authentication risks well, because it is based on an underlying asset model which focuses on protecting confidentiality of shared data as the priority risk. This should be addressed in future versions of the model.
  - For real systems in the energy network, not all properties will be known during the initial phase of the assessment. Taking such uncertainties into account - and making the process of updating or adding in new information about a system as straightforward as possible - will be important in further development of the software tool in the next stage of this project.

- The case study also highlighted the types of trade-offs around complexity and timing that energy network security professionals will have to consider, when making decisions on quantum threat mitigation strategies (for a full discussion, please see the analysis and conclusions in Sections 4-5 of this report):
  - For example, assessment and mitigation recommendations should consider the fact that post-quantum cryptography (PQC) alone is not always the most effective mitigation for legacy energy systems. PQC is potentially complex and expensive to deploy and has not had a significant amount of real-world experience compared to traditional cryptographic methods. Alternative mitigation solutions such as physical key sharing and hybrid techniques (which place a traditional algorithm in series with a post-quantum algorithm) will be important to consider, even if only as interim mitigation solutions.
  - Equally, some alternative mitigation approaches may become impractical or less effective over time. Looking at our System of Interest, if we consider threats to the communication of operational metering data, the only potential high-impact mitigation solution we identified would be to adopt physical key exchange. But because the number of balancing system participants will grow significantly in future as the energy sector becomes more distributed, the logistical complexity of implementing a physical key exchange solution is likely to become unwieldy eventually.
  - As another example of the importance of timing considerations, there is a risk of high impacts to the energy system from attackers forging the signatures of trusted software vendors in the energy supply chain. However, such risks can only manifest from the day that a cryptographically relevant quantum computer becomes available. As a result, there is less urgency to address this threat than for other risk types, despite its higher consequences. Conversely, confidentiality risks, which have less significant impacts, can effectively be launched today in the form of store-now, decrypt-later attacks.

The findings presented here are only an initial view on the proposed process and approach and have been demonstrated only for a single test case. As well as the areas identified for improvement above, other important considerations (such as cost of mitigations) will also need to come into the mix for future phases of development. Further inputs from energy sector stakeholders and potential users, work-throughs of a variety of different case studies, and additional detail and refinement from the project team, will all be critical for the next stage of evolving the Quantum-Aware Risk Management process towards a design for a usable MVP tool.

Contents

1 Introduction

This report is the third in a series of outputs from the Strategic Innovation Fund project, “Network Security in a Quantum Future”. This report provides an overview of the Quantum-Aware Risk Management process that was derived in the second report and, as a case study, applies the process to a model of a (fictional) energy sector system. The aim of this analysis is to illustrate the practical use of the process, and to identify areas where the process may be improved in future work.

Section 2 presents the Quantum-Aware Risk Management process, including an asset model for recording information about energy systems that use public-key cryptography.

Section 3 presents the System of Interest and explains its function.

Section 4 presents the results of the analysis from walking the System of Interest through the process.

Section 5 draws conclusions and makes recommendations for future phases.

2 Quantum-Aware Risk Management Process Summary

The Quantum-Aware Risk Management process is outlined below.

Essentially, this is a high-level view of the framework that an energy network operator would use to identify, and effectively plan mitigations for, quantum-enabled threats to the security of energy network assets. The process as outlined here could form the basis for development of a software tool to enable energy network operators to accomplish this task efficiently and in a fully-informed way, on an ongoing basis and for a variety of different systems.

The process is divided into three phases: Prepare, Categorise, and Select.

2.1 Prepare – Activities/Steps in the Process

1. Identify the threat actors with the technical capability to launch quantum-enabled attacks and characterise their motivations.
2. Identify the quantum-enabled attacks that could be launched by the threat actors.
3. Identify software components that are vulnerable to quantum-enabled attacks.
4. Evaluate the risk posed by these vulnerabilities
    a. Identify attack scenarios based on steps 1-3 and the system architecture of interest
    b. Evaluate the likelihood of attack scenarios
    c. Evaluate the impact of attack scenarios
    d. Evaluate the risk posed by attack scenarios
5. Identify a set of mitigations that can be applied to quantum-enabled attacks.

2.2 Categorise – Activities/Steps in the Process

6. Categorise the system using a bespoke asset model (outlined in Section 2.2.1)

Note: As the user’s understanding of the system grows, the user may need to revisit the risk assessment from the Prepare phase, to update the impact of specific risks.

2.2.1 Asset Model

The asset model used to categorise systems of interest is presented in the sister report “Assessing the cybersecurity implications of the quantum threat to the energy network”. It is summarised in Figure 1 and Table 1.

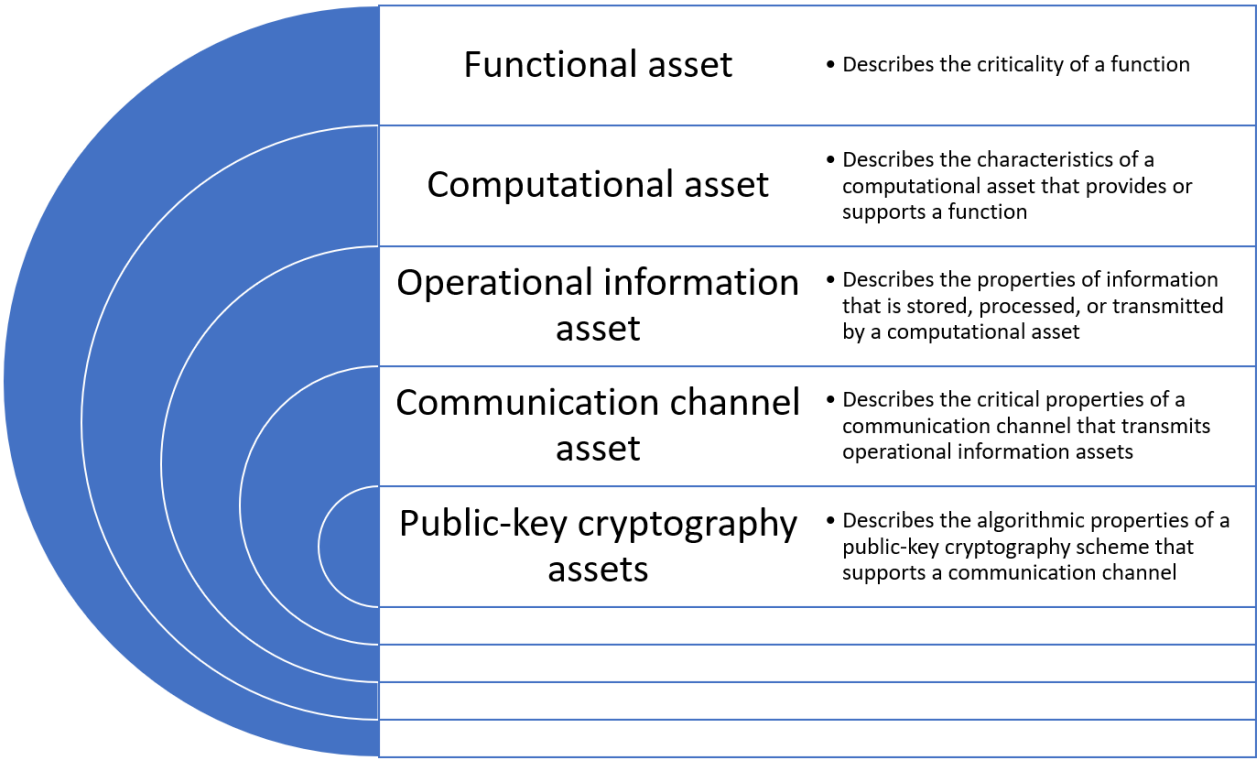


Figure 1 – Graphical representation of the asset model.
Note that at each tier, there could be a many-to-many relationship between the asset types; e.g., a functional asset may be supported by multiple computational assets, each of which may support other functional assets.

Asset type	Description	Syntax
Functional	The functional assets of a system are the functions that the system needs to perform. A system can perform many functions, and so can have multiple functional assets.	**Functional asset name(criticality: {High, Medium, Low})**
Computational	Computational assets are the computational elements that deliver the functions defined by functional assets.	**Computational asset name(processing power: {High, Medium, Low}, memory capacity: {High, Medium, Low})**
Operational information	Operational information assets are collections of data that are used to inform decisions that drive the delivery of functional assets.	**Operational information asset name (confidentiality impact: {High, Medium, Low}, confidentiality lifetime: {time with units}, integrity impact: {High, Medium, Low})**
Communication channel	Communication channel assets are used to transmit operational information assets from one computational asset to another, in order to achieve a function.	**Communication channel name(latency demand: {time in units}, bandwidth demand: {High, Medium, Low})**
Public-key cryptography	Public-key cryptography assets are the techniques used to protect the confidentiality and integrity of operational information assets.	**Public-key cryptographic asset name(key rotation period: {time in units}, underlying algorithm: {algorithm name})**

Table 1 – A summary of the asset model syntax

2.3 Select - Activities/Steps in the Process

7. Assign the controls identified in the Prepare phase to assets identified in the Categorise phase, assessing the impact on risk and complexity of implementing the mitigation for that system context.

3 System of Interest

This fictional 'System of Interest' – which we have taken as the basis for our case study to demonstrate how the above-described process would work in practice - is based on a generic use case common within energy systems worldwide. It should not be taken as a literal example of a real-world system. The decision to use a fictional system for our case study was driven by the need to protect confidentiality of real-world systems currently in use in energy networks; however the case study system was characterised with significant input from NG ESO's security team, to ensure verisimilitude.

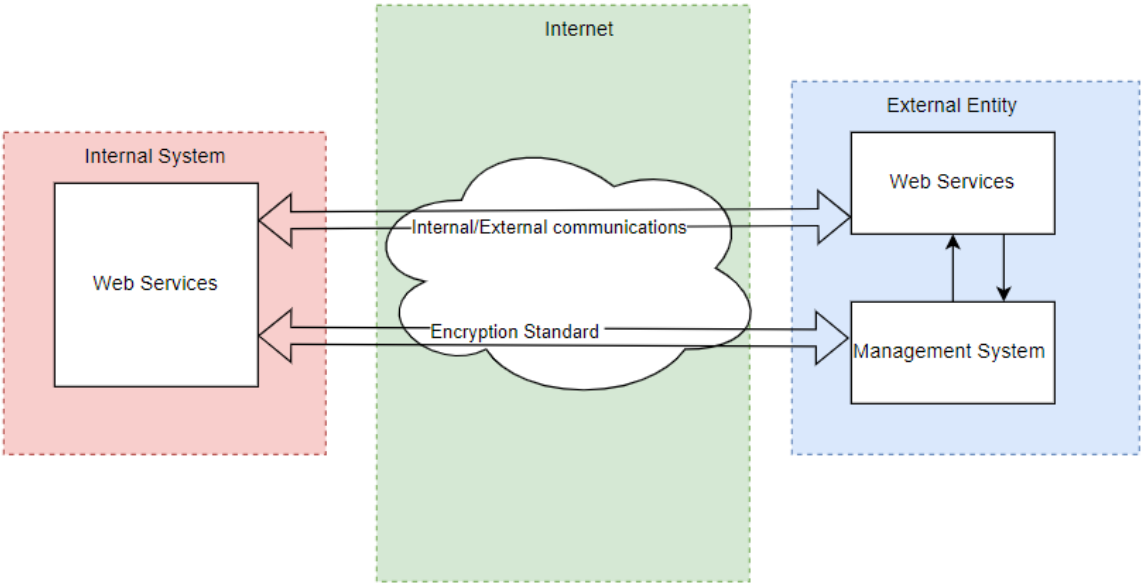


Figure 2 – The 'System of Interest' for the Quantum-Aware Risk Management Process case study analysis

Figure 2 presents our example energy system:

- The "Internal system" is power balancing system operated by NGESO.
- The "External entity" is a large power generation facility.
- The "Web services" of the "external entity" process bids and offers from the balancing system to generate more power on the grid.
- The "Management system" provides operational metering data about the energy generated, to the balancing system.
- All communications are performed using TLS encryption to secure JSON (Java Script Object Notation) payloads containing the relevant data.

4 Model analysis – Outputs from Applying the Quantum-Aware Risk Management Process to the System of Interest

Our next step was to work through the Quantum-Aware Risk Management process for this energy network 'System of Interest'. The purpose was to demonstrate how the process would work for an energy network security professional who needed to identify vulnerability to – and mitigate for - quantum-enabled attacks for such a system. We also wanted to see where we might need to adjust or optimise the process in future iterations (with a view to ultimately designing a supporting software tool).

Below are the outputs from the corresponding activities/steps within the Quantum-Aware Risk Management Process outlined in Section 2.1, after applying these steps to create an analysis of quantum threats to the exemplar System of Interest.

4.1 Prepare – Outputs of process (as applied to the System of Interest)

1. *Activity: Identify the threat actors with the technical capability to launch quantum-enabled attacks and characterise their motivations.*

   For this activity, high-capability nation state attackers with an objective to undermine grid stability shall be assumed.

2. *Activity: Identify the quantum-enabled attacks that could be launched by the threat actors.*

   In our sister report "Assessing the cybersecurity implications of the quantum threat to the energy network," a number of quantum-enabled kill chains are described. Table 2 summarises these, and describes their application to the System of Interest.

Kill chain name	Interactions with the System of Interest
Basic eavesdropping (K1)	The basic eavesdropping scenario assumes that the encrypted communications are entirely performed using public-key encryption. This is not applicable in this case.
Advanced eavesdropping (K2)	The communication between the load balancing system and power plant's bids/offers system is potentially vulnerable to advanced eavesdropping. This is reliant on the attacker i) having access to a cryptographically relevant quantum computer and ii) being able to launch a man-in-the-middle attack between the two entities. The communication of operational metering data between the load balancing system and the power plant is potentially vulnerable to advanced eavesdropping. This is reliant on the attacker i) having access to a cryptographically relevant quantum computer and ii) being able to launch a man-in-the-middle attack between the two entities.
Issuing malicious commands over an encrypted connection (K3)	The sending of bids/offers between the power plant and the balancing system is potentially vulnerable to malicious interference. This is reliant on the attacker i) having access to a cryptographically relevant quantum computer and ii) being able to launch a man-in-the-middle attack between the two entities. The sending of operational metering data from the power plant to the balancing system is potentially vulnerable to malicious interference. This is reliant on the attacker i) having access to a cryptographically relevant quantum computer and ii) being able to launch a man-in-the-middle attack between the two entities.
Installing signed malicious firmware/software (K4)	Computational assets within the balancing system are potentially vulnerable to maliciously signed software being installed on them. This is reliant on the attacker i) having access to a cryptographically relevant quantum computer and ii) the attacker being able to insert malicious software into the balancing system supply chain. Computational assets within the power plant are potentially vulnerable to maliciously signed software being installed on them. This is reliant on the attacker i) having access to a cryptographically relevant quantum computer and ii) the attacker being able to insert malicious software into the balancing system supply chain

Table 2 – Kill chains applied to the System of Interest

3. *Activity: Identify software components that are vulnerable to quantum-enabled attacks.*

   In this case we find that TLS versions 1.2 and 1.3 are vulnerable to quantum-enabled attacks, due to their reliance on RSA and Diffie-Hellmann.

4. *Activity: Evaluate the risk posed by these vulnerabilities*

   The outputs of the analyses undertaken to evaluate the risks associated with quantum-enabled attacks are shown in Tables 3-5.

   Our analysis identified seven attack scenarios to assess for likelihood. For the “Technical likelihood” evaluation (shown in Table 3), we have only considered the technical feasibility of the attack, under the assumption that the threat actor has access to a cryptographically-relevant quantum computer. To produce an overall risk score, we used the risk matrix found in Appendix I, Table I-2 from NIST SP800-30, to calculate risk level based on likelihood and impact.

Attack Scenario ID	Attack Scenario description	Technical likelihood	Justification
1	Attacker decrypts the bids/offers between the balancing system and the power plant	High	Both systems are static, so launching a man-in-the-middle attack is relatively easy. There is no time limit on this type of attack, as the encrypted traffic and key exchange can be performed offline after being captured.
2	Attacker decrypts the operational metering data between the power plant and the balancing system	High	Both systems are static, so launching a man-in-the-middle attack is relatively easy. There is no time limit on this type of attack, as the encrypted traffic and key exchange can be performed offline after being captured.
3	Attacker falsifies a bid from the power plant to the balancing system	Moderate	It is assumed that any attacker with access to a cryptographically-relevant quantum computer has the technical capability to create a realistic looking data structure. This attack would be time limited by the key exchange frequency between the systems.
4	Attacker identifies the session key between the two entities and falsifies an acceptance from the balancing system to the power plant. To maximise the impact of this attack, the attacker also prevents legitimate data from being received by the power plant.	Moderate	It is assumed that any attacker with access to a quantum computer has the technical capability to create a realistic looking data structure. This attack is against the session key, so would be time limited by the key exchange frequency between the systems.
5	Attacker sends false operational metering data from the power plant to the balancing system	Moderate	It is assumed that any attacker with access to a quantum computer has the technical capability to create a realistic looking data structure. This attack would be time limited by the key exchange frequency between the systems.
6	Attacker installs signed, malicious software on the balancing system	Moderate	Obtaining the public key would be trivial through OSINT. Calculating the private key is assumed to be within the attacker's capability. The attacker must then find a way of injecting the signed, malicious software into the balancing system supply chain. The amount of time that the attacker has to do this is a function of how frequently trusted suppliers rotate their signing keys. A full analysis would consider the controls in place around the installation of signed software for the facility, but as the key rotation is potentially multiple years, for this analysis it is assumed that the attacker would eventually find a way.
7	Attacker installs signed malicious software on the power plant	Moderate	Obtaining the public key would be trivial through OSINT. Calculating the private key is assumed to be within the attacker's capability. The attacker must then find a way of injecting the signed, malicious software into the balancing system supply chain. The amount of time that the attacker has to do this is a function of how frequently trusted suppliers rotate their signing keys. A full analysis would consider the controls in place around the installation of signed software for the facility, but as the key rotation is potentially multiple years, for this analysis it is assumed that the attacker would eventually find a way.

Table 3 – Quantum-enabled attack scenarios and their technical likelihoods, as applied to the System of Interest

Attack Scenario ID	Attack Scenario description *(from Table 3)*	Impact description	Impact level	Impact assessment justification
1	Attacker decrypts the bids/offers between the balancing system and the power plant	Bids/offer information is revealed to the attacker approximately 8 hours after transmission.	Very low	Bids/offers are typically issued on a 30 minute basis and are published on a website after acceptance. This assessment assumes that new shared secrets are established between parties for each bidding period and that the shared secrets are not reused across multiple bidding periods. Longer periods of key reuse would undermine this assumption.
2	Attacker decrypts the operational metering data between the power plant and the balancing system	Operational metering data is made available to the attacker.	Very low	There is very little an attacker can do with operational metering data. Aggregates of this data are regularly published on websites and the totals from various power sources (gas, solar, nuclear, imports, biomass, wind, coal) are published live through the ESO app.
3	Attacker falsifies a bid from the power plant to the balancing system	A power plant receives a false request asking for power that is not required.	Moderate	In the event that the power plant acted on the bid, different types of power plant will have different levels of impact depending on their ramp up time and output power, etc. If the plant in question is a large provider, then over-producing would potentially cause an increase in grid frequency. For this to be problematic, the excess energy generation would have to be sustained, requiring a persistent attack. Automated control systems would attempt to compensate for this and in extreme cases some suppliers would disconnect from the gird if it exceeded their operating frequency. Energy export via interconnectors would also provide an avenue to release excess energy. As a result of existing controls and balances, it is not considered that this attack alone poses a significant threat to grid stability but could have financial impacts should the over-producing plant seek renumeration.
4	Attacker identifies the session key between the two entities and falsifies an acceptance from the balancing system to the power plant. To maximise the impact of this attack, the attacker also prevents legitimate data from being received by the power plant.	Energy that was relied upon for grid stability does not get generated.	High	If the power plant is a significant supplier to the grid, an attacker could cause a frequency reduction by preventing them from receiving bids, whilst maliciously offering to fulfil them on the plant's behalf. For this attack to have a significant impact, the generator would need be a significant contributor, or the attack would need to be launched against several generators simultaneously. Independent frequency measuring systems would detect this, and the attacker would need to compromise operational metering data (see scenario 5) to create the illusion that the power plant was acting on the bids. A full analysis of this scenario would require a detailed knowledge of the alternative communications channels between the balancing system and power plants and their ability to intervene in a timely manner.

Attack Scenario ID	Attack Scenario description *(from Table 3)*	Impact description	Impact level	Impact assessment justification
5	Attacker sends false operational metering data from the power plant to the balancing system	Balancing system makes an incorrect decision based on inaccurate operational metering data.	High	The impact of this scenario is dependent on how large a generator the power plant is. It is also assumed that the attacker is only targeting a single source of operational metering data and not multiple power plants at once. Regardless, inaccurate operational metering data could result in a power plant looking like it is running at capacity when it is not running at all. In this situation the balancing system would lose that power plant as an option, limiting their ability to balance the grid.
6	Attacker installs signed, malicious software on the balancing system	Balancing system computers become compromised by malware.	Very High	Malware installed on the balancing system could jeopardise the system's ability to operate.
7	Attacker installs signed malicious software on the power plant	Power plant computers become compromised by malware.	Very High	Not only could losing the computer system jeopardise the power plant's ability to operate, but all other scenarios (miscommunication of operational metering data, false bid acceptance) are potentially realisable once the power plant computers can no longer be trusted.

Table 4 – Quantum-enabled attack scenarios and their impacts, as applied to the System of Interest

Attack Scenario ID	Attack Scenario description *(from Table 3)*	Technical Likelihood *(from Table 3)*	Impact Level *(from Table 4)*	Overall Risk Level
1	Attacker decrypts the bids/offers between the balancing system and the power plant	High	Very low	**Low**
2	Attacker decrypts the operational metering data between the power plant and the balancing system	High	Very low	**Low**
3	Attacker falsifies a bid from the power plant to the balancing system	Moderate	Moderate	**Moderate**
4	Attacker identifies the session key between the two entities and falsifies an acceptance from the balancing system to the power plant. To maximise the impact of this attack, the attacker also prevents legitimate data from being received by the power plant.	Moderate	High	**Moderate**
5	Attacker sends false operational metering data from the power plant to the balancing system	Moderate	High	**Moderate**
6	Attacker installs signed, malicious software on the balancing system	Moderate	Very High	**High**
7	Attacker installs signed malicious software on the power plant	Moderate	Very High	**High**

Table 5 – Overall risk levels for each of the Quantum-enabled attack scenarios

5. *Activity: Identify a set of mitigations that can be applied to quantum-enabled attacks*

   The identified list of mitigations is taken from our sister report "Assessing the cybersecurity implications of the quantum threat to the energy network" and is as follows:
   - Post Quantum Cryptography (PQC)
   - Hybrid approaches
   - Key lengthening
   - Increase key exchange frequency
   - Architectural changes
   - Alternative key exchange mechanics
   - Phase out asset.

4.2 Categorise - Outputs of process (as applied to the System of Interest)

6. *Activity: Categorise the system using a bespoke asset model (outlined in Section 2.2.1)*

   The asset model outlined in Section 2.2.1 has been populated with details from the System of Interest, as shown below.

   Readers are reminded that this system is fictional, and asset details do not directly correspond to a real-world system in the energy network.

Asset model - Details by asset type for System of Interest (fictional energy network system case study)

Functional assets:

- Grid balancing (criticality: high)
- Power generation (criticality: high)

Computational assets:

- System balancing web services (processing power: high, memory capacity: high)
- Power plant web services (processing power: high, memory capacity: high)
- Power plant management services (processing power: high, memory capacity: high)

Operational information assets:

- Bids/offers (confidentiality impact: low, confidentiality lifetime: 30 mins, integrity impact: high)
- Acceptance data (confidentiality impact: moderate, confidentiality lifetime: 30 mins, integrity impact: high)
- Operational metering data (confidentiality impact: low, confidentiality lifetime: n/a, integrity impact: high)
- Balancing system services software (confidentiality impact: low, confidentiality lifetime: multiple years, integrity impact: high)
- Power plant services software (confidentiality impact: low, confidentiality lifetime: multiple years, integrity impact: high)

Communication channel assets:

- Web service-Web service communications (latency demand: 1 minute, bandwidth demand: low)
- Operational metering data communications (latency demand: 1 second, bandwidth demand: low)

Public-key cryptography assets:

- TLS 1.3 on Web service-Web service communications (key rotation period: 30 mins, underlying algorithm: Diffie-Hellman)

- TLS 1.3 on operational metering data (key rotation period: unknown, underlying algorithm: Diffie-Hellman)
- Unspecified authentication algorithm between internal system and external entity (key rotation period: unknown, underlying algorithm: unknown)
- Digital signatures on balancing system software (key rotation period: dependent on supplier, underlying algorithm: unknown)
- Digital signatures on power plant software (key rotation frequency: dependent on supplier, underlying algorithm: unknown)

Note that for real systems in the energy network, not all properties will be known during the initial phase of the assessment. Constructing a tool that enables energy network operator security teams to make decisions, while still taking such uncertainties into account, will be important in further development of the software tool in the next stage of this project.

It is also noteworthy that not all algorithms will be discovered simultaneously for all systems, so constructing the asset list may highlight areas that require further investigation.

4.3 Select - Outputs of process (as applied to the System of Interest)

7. *Activity: Assign the controls (mitigations) identified in the Prepare phase to assets identified in the Categorise phase, assessing the impact on risk and the complexity of implementing the mitigation for that system context.*

The final phase of the Quantum-Aware Risk Assessment process is to **assign possible mitigations to the risks** (i.e., the Attack Scenarios augmented with likelihood and impact information) **identified**, given the characteristics of the System of Interest.

Based on the characterisation information in the Asset Model above, both types of Communication Channel Assets - **Web service-web service communications** (relevant for Attack Scenarios 1,3, and 4), and **Operational metering data communications** (relevant for Attack Scenarios 2 and 5) - are using Public-Key Cryptography (PKC) assets that are vulnerable to quantum-enabled attacks.

Digital signatures are relevant for Attack Scenarios 6 and 7 (installation of signed malicious software on balancing system and power plant). While the digital signatures have not had an underlying algorithm specified, for the purposes of this analysis we have assumed that digital signatures are also vulnerable.

Table 6 below shows an evaluation of the complexity of each potential mitigation approach (low, moderate or high), and its likely impact (low, moderate or high). Risks (i.e., the seven attack scenarios) have been grouped in the tables below, for ease of analysis.

Mitigation Type	Description of Mitigation	Applicability to Web Service-Web Service channel *(relevant for Attack Scenarios 1,3, and 4)*	Applicability to Operational Metering channel *(relevant for Attack Scenarios 2 and 5)*	Applicability to Digital Signatures for power plant/balancing system software *(relevant for Attack Scenarios 6 and 7)*
Post Quantum Cryptography (PQC)	Replace at-risk cryptography with an algorithm specifically designed to be resistant to quantum computers	All of the computational assets for this service are characterised by high computational power and high memory, making the implementation of PQC feasible. The bid/offers information asset being communicated by the channel has a high confidentiality impact rating for only 30 mins, currently thought to be below the threshold for being vulnerable to a quantum-enabled attack. The current control's key rotation frequency is 30 minutes, which is below the feasibility threshold for an attack against the integrity for the asset. The latency demands of the channel are extremely relaxed, meaning altering the underlying cryptographic algorithm is unlikely to have an impact. TLS supports downgrading the underlying algorithm to find a system that works for both entities, so the upgrade would not need to be simultaneous. However, until both the power plant and the balancing system support PQC a vulnerable algorithm would be used. Checks would need to be made to ensure that the intermediate networking systems could support the PQC algorithm. Overall, this would be a **moderate complexity upgrade**, with a **moderate impact on the associated risks**.	The properties of this channel are similar to the web service-web-service channel. The notable exceptions are that the acceptable latency constraint is tighter, and the confidentiality impact is lower. An analysis would need to be performed on the feasibility of deploying PQC on the assets involved and impacts on intermediate networking equipment, above and beyond the properties identified in the asset model. The lower confidentiality impact further erodes the argument for upgrading to PQC. Overall, this would be a **high complexity upgrade** to perform with a **moderate impact on the associated risks**.	The computational assets that support this scenario are characterised by high computational power and high memory, making the implementation of PQC feasible. The confidentiality impacts of the information asserts involved are low. Limiting the benefits of PQC. The integrity impacts of the information assets involved are high. Increasing the benefits of PQC. There are no known bandwidth constraints for the transfer of digital signatures, making the use of PQC signatures feasible. Key rotation frequency is out of the hands of the consumer without an explicit contract. The adoption of PQC would need to be negotiated with the software supplier to be feasible. The operating systems of the affected devices may require upgrading, as current operating systems do not support PQC signatures out of the box. Overall, this would be a **high level of complexity to upgrade** with a **high impact on the associated risks.**
Hybrid approaches	Replace broken cryptography with a hybrid of a standard cryptographic approach and a PQC approach	This is similar to the PQC scenario, with the added advantage of not being entirely reliant on unproven technology. The increased computational demands are likely to be within the computational power/memory limits of the assets involved. Overall, this would be a **moderate complexity upgrade**, with a **moderate impact on the associated risks**.	This is similar to the PQC scenario, with the added advantage of not being entirely reliant on unproven technology. The increased computational demands are likely to be within the computational power/memory limits of the assets involved. But the increased latency introduced by that computation would need to be assessed to see if it was acceptable. Overall, this would be a **high**	Using both a traditional and a PQC signature to validate the integrity of the software would carry additional computational cost and process overhead. Overall, this would be a **high level of complexity to upgrade**, with a **high impact on the associated risks.**

Mitigation Type	Description of Mitigation	Applicability to Web Service-Web Service channel *(relevant for Attack Scenarios 1,3, and 4)*	Applicability to Operational Metering channel *(relevant for Attack Scenarios 2 and 5)*	Applicability to Digital Signatures for power plant/balancing system software *(relevant for Attack Scenarios 6 and 7)*
			complexity upgrade, with a **moderate impact on the associated risks**.	
Key lengthening	Increase the key length for a standard cryptographic approach	Keeping a traditional algorithm with a longer key size would preserve the confidentiality of the data for longer and lengthen the amount of time a given session could be left running without needing to change keys. Key lengthening still requires a software algorithm change to the system and would have an impact on the bandwidth consumed by the key exchange. Overall, this would be a **moderate complexity upgrade** with a **low impact on the associated risks**.	Keeping a traditional algorithm with a longer key size would preserve the confidentiality of the data for longer and lengthen the amount of time a given session could be left running without needing to change keys. Key lengthening still requires a software algorithm change to the system. Overall, this would be a **high complexity upgrade** (given the assessment requirements) with a **moderate impact on the associated risks**.	Given the infrequency of key rotation for digital signing process, this mitigation is unlikely to have much impact on the risk. As with all signature-based mitigations, there is additional complexity stemming from the fact that the signatory is outside of the managing organisation. Overall, this would be a **moderate complexity upgrade** with a **low impact on the associated risks**.
Increase key exchange frequency	Mandate the rotation of private keys	For small confidentiality lifetimes, like those associated with the information assets for this scenario, rotating the keys more frequently is likely to be a cheap way of ensuring that the attacker cannot access the information within the time window that it is sensitive. Key rotation mechanics already likely exist within the system, so it is likely that this is a low complexity upgrade. Overall, this would be a **low complexity upgrade** with a **low impact on the associated risks**.	For latency constrained scenarios, increased key rotation can introduce an unacceptable delay. Such a change would need to be assessed before implementation. Key rotation mechanics already likely exist within the system,. Overall, this would be a **moderate complexity upgrade** with a **low impact on the associated risks**.	Rotating the private key/public key pairing for the digital signature for a piece of software introduces an overhead to ensure that the current public key is still valid. This would not only require an update at point of install, but would potentially require checks every time the system was run, depending on operating system configuration. Overall, this would be a **high complexity upgrade**, with a **moderate impact on the associated risks**.
Architectural changes	Restructure the system in a way that limits the man-in-the-middle opportunities for the attacker	Rearchitecting the solution to avoid man-in-the-middle attacks would likely require significant investment and analysis. Overall, this would be a **high complexity upgrade** with an **unknown impact on the associated risks**.	Rearchitecting the solution to avoid man-in-the-middle attacks would likely require significant investment and analysis. Overall, this would be a **high complexity upgrade** with an **unknown impact on the associated risks**.	Other controls could be introduced to ensure the integrity of the software from different suppliers. For example, secure web portals to push updates from authenticated users. However, this would need to be negotiated on a case by case basis with suppliers. Overall, this would be a **high-complexity upgrade** with an **unknown impact on the associated risks**.

Mitigation Type	Description of Mitigation	Applicability to Web Service-Web Service channel *(relevant for Attack Scenarios 1,3, and 4)*	Applicability to Operational Metering channel *(relevant for Attack Scenarios 2 and 5)*	Applicability to Digital Signatures for power plant/balancing system software *(relevant for Attack Scenarios 6 and 7)*
Alternative key exchange mechanics	Continue to use symmetric cryptography, but find alternative channels to establish the shared secret	There are no other well-established communication channels that would allow the secure passing of private keys for this scenario. Physically transferring symmetric keys is possible, though carries its own risks in terms of the security of the courier and the physical security of the portable media being used to store the keys. Additional policies would need to be put in place to ensure that this was done in a secure manner. Overall, this is a **high complexity upgrade** with a **high impact on the level of risk**.	There are no other well-established communication channels that would allow the secure passing of private keys for this scenario. Physically transferring keys would carry the same issues as risks 1,3, and 4. Overall, this is a **high complexity upgrade** with a **high impact on the level of risk**.	Not applicable.
Phase out asset	Accelerate the removal of the asset with an intent to either a) discontinue the service being supported by the asset function, or b) replace the asset with an asset that can support one of the above mitigations	Not applicable: service is still required.	Not applicable: service is still required.	Not applicable: service is still required.

Table 6 – An evaluation of the common mitigations against each risk

In summary, the options for securing this system (the System of Interest) against quantum-enabled attacks are:

For risks (Attack Scenarios) 1, 3, and 4, the mitigation assessments are:

- Post Quantum Cryptography (PQC): moderate complexity, moderate impact
- Hybrid approaches: moderate complexity, moderate impact
- Key lengthening: moderate complexity, low impact
- Increase key exchange frequency: low complexity, low impact
- Architectural changes: high complexity, unknown impact
- Alternative key exchange mechanics: high complexity, high impact
- Phase out asset: n/a

For risks (Attack Scenarios) 2 and 5, the mitigation assessments are:

- Post Quantum Cryptography (PQC): high complexity, moderate impact
- Hybrid approaches: high complexity, moderate impact
- Key lengthening: high complexity, moderate impact
- Increase key exchange frequency: moderate complexity, low impact

- Architectural changes: high complexity, unknown impact
- Alternative key exchange mechanics: high complexity, high impact
- Phase out asset: n/a

For risks (Attack Scenarios) 6 and 7, the mitigation assessments are:

- Post Quantum Cryptography (PQC): high complexity, high impact
- Hybrid approaches: high complexity, high impact
- Key lengthening: moderate complexity, low impact
- Increase key exchange frequency: high complexity, moderate impact
- Architectural changes: high complexity, unknown impact
- Alternative key exchange mechanics: n/a
- Phase out asset: n/a

5 Conclusions

Armed with the outputs above, an energy network security team would be better enabled to make decisions with confidence about how the quantum threat is likely to impact the System of Interest, how to prioritise the associated risks, and how to consider the different mitigation options.

Key areas that we identified for future development of the process and tool, based on the case study analysis, are:

- Even for a simple system, the process required a significant amount of (largely manual) analysis. Opportunities to streamline the process and automate aspects, using modelling tools that can manage quantum-enabled attacks, should be considered as we develop future iterations.

- Selecting the correct mitigation for a specific system requires the assessor to understand the bandwidth and computational limitations of the system, and the impact that the different mitigation types will have on those properties. This may require training and/or support, as well as clear guidance and supporting information provided within the tool itself.

- The risk assessment process as currently laid out does *not* include consideration of any risks around the compromise of authentication keys. This omission is effectively an artefact of the asset model, which does not explicitly record authentication algorithms. This should be amended in future iterations of the process and asset model.

- For real systems in the energy network, not all properties will be known during the initial phase of the assessment. Enabling energy network operator security teams to make decisions while still taking such uncertainties into account - and making the process of updating or adding in new information about a system as straightforward as possible - will be an important consideration in further development of the software tool in the next stage of this project.

The case study also highlighted the types of trade-offs around complexity and timing that energy network security professionals will have to consider, when making decisions on quantum threat mitigation strategies:

- Assessment and mitigation recommendations should consider the fact that post-quantum cryptography alone is not always the most effective mitigation for legacy energy systems; other mitigation approaches should also be considered. Post-quantum cryptography is potentially complex and expensive to deploy, and has not had a significant amount of real-world experience compared to traditional cryptographic methods.
- Alternative mitigation techniques that may be relevant for energy networks include physical key sharing (which avoids the need for public-key cryptography for many applications, but also presents logistical challenges in some cases, as discussed below), and hybrid techniques (which place a traditional algorithm in series with a post-quantum algorithm, so attackers would need to compromise both in order to make progress).

- Specifically for the communication of bids/offers and acceptances (associated with Attack Scenarios 1,3, and 4) the highest impact change would be to establish a shared secret between the two entities via the transportation of physical media. This would introduce new risks and require new policies on both sides. The adoption of a hybrid PQC solution would have a moderate impact on the risks with moderate complexity. This is seen as the superior solution to adopting a PQC-only approach, as it also mitigates the risk that a vulnerability is found in the PQC algorithm itself.

- For the communication of operational metering data (associated with Attack Scenarios 2 and 5), the latency requirements demand that a more careful analysis be performed, to have confidence in any mitigation solution. The only high-impact mitigation solution identified is to adopt physical key exchange (see 'Alternative Key Exchange Mechanics', in the mitigations lists above), which seems feasible initially given the static nature of the relationship between the entities. However, a challenge is that the balancing system is required to interact with a large number of market participants, and that list is likely to grow as the energy sector becomes more distributed. The complexity of implementing a physical key exchange solution would grow accordingly, and is likely to become unwieldy. An alternative mitigation option, such as lengthening the keys, may be quicker to achieve than completely changing the underlying algorithms, and could buy the system some extra time until upgrading to a PQC or hybrid approach could be fully analysed and explored.

- For the checking of digital signatures, (Attack Scenarios 6 and 7) the technical likelihood of such an attack is predicated on the existence of a cryptographically-relevant quantum computer. There is no opportunity for an attacker to launch a delayed attack (such as a Store-Now-Decrypt-Later attack against the confidentiality of shared data). As a result, there is less urgency to address this challenge than for the other risk types, despite its higher consequences. Much of the complexity arises from the need to negotiate the software signature technique with the software vendor, and the lack of support for PQC in current operating systems. Architectural changes, using PQC to establish secure tunnels between the vendor and the installer would protect against tampering of the software between release and installation, thus partially reducing the risk. However, other sources of tampering would still be undetectable in the event the attacker had access to a cryptographically-relevant quantum computer.

- A final point on timing: This analysis assumes that the risks associated with the System of Interest are likely to manifest within the lifetime of the system. In some ways, this is dependent on the expected date of a cryptographically-relevant quantum computer (CRQC) being developed and becoming available; but in any case, all of the functions being performed within this system are essential services, and unlikely to become obsolete before the advent of CRQCs.

The findings presented here are of course only an initial view on the proposed process and approach, and have been demonstrated only for a single test case. Other important considerations (such as cost of mitigations) will also need to come into the mix for future phases.

Further inputs from energy sector stakeholders and potential users, work-throughs of a variety of different case studies, and additional detail and refinement from the project team, will all be critical for the next stage of evolving the Quantum-Aware Risk Management process towards a design for a usable MVP tool.