QED-C

QuEnergy

RESILIENCE

Exploring the role of quantum security and cyber for the electric grid

Link to full report including interactive graphics: https://quantumconsortium.org/QuEnergy23

Executive Brief

The grid and quantum technology are evolving

The way we approach security for the electric grid must undergo a paradigm shift to neutralize emergent threats and manage a decentralized infrastructure that is becoming exponentially more complex. The industry cannot and is not standing still as it copes with a new menu of demands – from intermittent renewables and distributed energy resources (DER) to electrification of transport and buildings. We now face a dynamic, decentralized, and decarbonized grid requiring two-way flow networks to exchange information and electrons. Quantum technology holds a special place in this world as both a potential threat to and a first-line defender of our energy infrastructure. That's why the Department of Energy (DOE) and the industry are diligently working to evaluate quantum-based challenges and opportunities. Stakeholders recognize that they must seize this moment to bolster defense, resilience, and confidentiality across every grid segment, including generation, transmission, distribution, customer load, asset owners, system aggregators, and service providers.

We are witnessing a new technology race as malicious actors look to weaponize quantum by constructing computers sufficient in capability to break the cryptographic systems used today.

Simultaneously, the system guardians are racing to select new resistant crypto algorithms and test new quantum communications methods to thwart these sophisticated hackers. Beyond using quantum techniques to solve the security problem that quantum technologies are creating, the industry is studying how quantum solutions could solve a wide array of additional problems such as timing, optimization, and stability.

Five upgrades for a more secure & resilient grid

Five key areas have emerged where current and future quantum technology can play a role addressing the challenges testing the electric grid today:

1. **Physical Grid Anomalies**
– detecting a range of changes (possibly electrical, magnetic, temperature, etc.) in the electrical grid with quantum sensors
2. **Contingency Analysis for Resilience**
– analyzing grid operations with quantum computers to increase efficiency and durability
3. **Secure Control Communications**
– protecting against attacks to grid controls by leveraging new security algorithms and quantum communication methods
4. **Secured Distributed Assets**
– protecting against attacks to assets connected to the grid by leveraging new security algorithms and quantum communication methods
5. **Synchronization Without GPS**
– using quantum sensing (timing) for resilience against attacks that could destabilize electric grid operations

When complicated topics such as national scale grid operations, internet communications security, and quantum technology arise, care must be given to reference the following perspectives:

- Energy, security, and quantum practitioners have different objectives. They each operate with a different lexicon and point of view. In security, practitioners are taught to consider a balance of protections for security systems: confidentiality, integrity, and availability, known as the CIA triad. This can help someone working in security understand the objectives of an electric grid operator, which is to "keep the lights on." That primary concern translates into an emphasis on protections for availability and integrity, perhaps at the cost of confidentiality. Therefore, some novel quantum technologies which focus on confidentiality could be viewed as less critical in certain circumstances for the electric grid. However, this does not mean those technologies are not important in specific scenarios, say when managing secret or confidential information, which could lead to an emphasis on integrity or availability.

- Consensus on feasibility and impact is challenging for quantum technology. Certain use cases in quantum, such as the need for cyber security protections against future quantum computers, strongly influence decisions and actions taken today regarding quantum technology. There is a spectrum of theorical possibility, decision level confidence, operational readiness, and practicality that governs preference and choice in this area.

  While grid, quantum, and security folks are envisioning a long timeline of change, the pressure of steal now, decrypt later attacks casts a looming shadow over the immediate horizon. Encouragingly, the industry appears to be optimistic about the role quantum technologies can play in creating more resilient and secure grid.

This report shares key ideas and concepts applicable to the power industry as a starting point for further exploration of the application of quantum security in the electric sector. Additionally, it outlines clear pathways to develop grid security and quantum technology collaboratively for practical advancements.

The Quantum toolbox

These six quantum-relevant methods for increasing security on the electric grid are available in varying degrees of maturity. Some are already feasible and some won't be ready for a few years. The variety of concerns with each is not listed here but the anticipated availability has been integrated into the timelines for projects leveraging the technology to account for when they could benefit the electric grid. Industry experts are eager to understand how Quantum Information Science (QIS) can improve energy security and, critically important, how to be ready to implement these technologies when needed. Each of the following six quantum-relevant methods offers unique capabilities and potential ways to contribute to greater grid security. And some can be used in varying combinations.

1. Post-quantum cryptography (PQC): Defending against adversaries

PQC addresses the challenge of future quantum computers breaking cryptography by developing encryption algorithms resistant to both classical and quantum attacks on conventional IT systems. By adopting PQC, the electric grid can maintain secure communication channels, protect sensitive data, and ensure the integrity of grid operations. Standardization efforts and collaboration among stakeholders are crucial for the successful implementation of PQC, enabling a smooth transition to a secure and resilient electric grid in both the classical and quantum eras.

2. Quantum key distribution (QKD): Securing communication

QKD offers a method of secure communication, utilizing the fundamental principles of quantum mechanics. It provides information-theoretic security, enabling the exchange of encryption with the ability to identify interception or eavesdropping. QKD uses light rays (photons or particles) over fiber optic cable or open-air media for its point-to-point communications. If a third-party views information during transmission, the intended recipient will no longer be able to view it. This will increase the error rate, which the recipient can notice.

3. Quantum random number generation (QRNG): Reinforcing cryptographic systems

Randomness plays a critical role in cryptographic systems; the security of encryption algorithms heavily relies on the quality of the random numbers. Traditional pseudo-random number generators (PRNGs) are inherently deterministic and susceptible to predictability. In contrast, QRNG employs the inherent randomness of quantum phenomena to generate true random numbers. By utilizing quantum processes, such as photon counting or quantum fluctuations, QRNG can produce genuinely unpredictable numbers, making it an indispensable tool for strengthening encryption schemes. By integrating QRNG into the electric grid's security infrastructure, the vulnerabilities arising from predictable random numbers could be reduced.

4. Quantum sensing (QS): Enhancing grid security

Quantum sensing technologies present a novel and powerful approach to monitoring and securing the electric grid. These technologies exploit the unique characteristics of quantum systems to enhance the precision, sensitivity, and reliability of measurement devices. Quantum sensors can detect minute changes in physical parameters such as voltage, current, temperature, or magnetic fields, enabling the identification of anomalies and potential threats in real-time. By providing highly accurate and tamper-resistant data, quantum sensing contributes to early threat detection, fault diagnosis, and rapid response in the face of cyber-attacks or physical disruptions, fortifying the resilience of the electric grid.

Quantum sensing can also be used for precise timing and synchronization of devices on the grid. For example, atomic clocks rely on quantum properties of atoms to provide accurate timekeeping in a variety of applications. Quantum sensors can provide entanglement to enable synchronization across large distances with high accuracy and surpassing the limitations of classical methods.

5. Quantum entanglement (QE): Upgrading information sharing security

Quantum entanglement, a phenomenon described as "spooky action at a distance" by Einstein, provides an intriguing foundation for secure communication and information sharing. Entangled particles exhibit an intimate correlation such that measuring one particle instantaneously affects the state of its entangled partner, regardless of the spatial separation between them. This property may be harnessed to develop secure communication protocols, enabling the transmission of information with intrinsic protection against eavesdropping. By exploiting quantum entanglement, the electric grid could benefit from secure data transfer, preventing unauthorized access and tampering. This then safeguards critical information and ensures the integrity of grid operations.

6. Quantum computing (QC): Embracing and defending against the power of quantum

Quantum computing represents a transformative technology that holds tremendous potential for both positive and negative applications in the field of grid security. Quantum computers pose a significant threat to traditional cryptographic algorithms; they also offer new avenues for advanced encryption methods. Post-quantum cryptography algorithms, specifically designed to withstand attacks from quantum computers, can be employed to secure critical grid infrastructure. Furthermore, quantum computers can be utilized for optimization algorithms, facilitating grid management, load balancing, and anomaly detection. By strategically integrating quantum computing capabilities, the electric grid can adapt to the evolving security landscape while harnessing the benefits offered by this revolutionary technology.

Quantum Security Use Cases

The QED-C recently hosted a workshop consisting of energy, security, and quantum experts. They identified the top areas where the energy sector could benefit from current and future quantum-relevant security technologies. The aggregated data (Table 1) shows 1) the tool our participants turned to most often was quantum computing; and 2) grid resilience was the most common challenge addressed across quantum technologies. In all, the attendees came up with 276 use cases, all listed with the methodology in the appendix.

Table 1:
Key security use case categories in the electric sector

Use case categories	PQC	QC	QE	QKD	QS	Grand total
Defense in Depth	1			1		2
DER Communications				1		1
Efficiency		5			1	6
Forecasting		3				3
Material Science		1				1
Monitor and Control Network	1					1
OT Network	1			1		2
Resilience		11	2		7	20
SCADA Network	1					1
Substation Communications				1		1
Synchronization					3	3
Grand Total	**4**	**20**	**2**	**4**	**11**	**41***

***Note:** Accounting for multiple technologies per use case and removing non-energy use cases there were 41 concepts for categorization in Table 1. Graphics and analysis for the rest of this report use the original 40 use cases for naming and scoring.

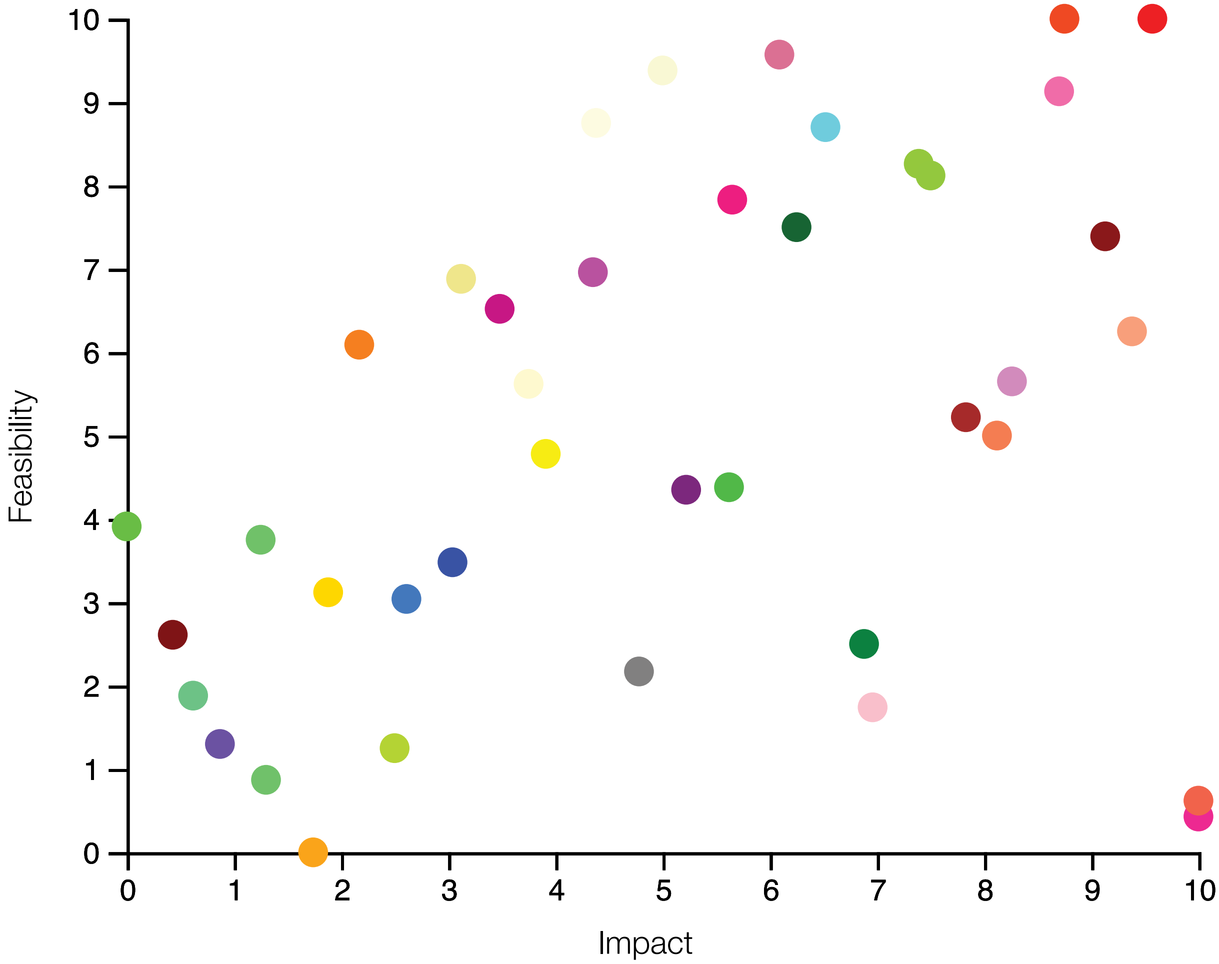
Of the 276 individual use cases identified 40 were rated as "high importance." These high importance use cases can be categorized into 13 areas. We adjusted the categories for analysis, which reduced the groupings to 11. Here's a look at our process:

- We removed two ideas that weren't specific to the electric grid (**QKD as a Service** and **Quantum Network Components**)
- QRNG was used several times but always in combination with other technologies, such as PQC and QKD; in those cases, each use case was categorized here with the paired technology
- When ideas which offered two solutions for the same action (e.g., PQC or QKD) both were counted
- Ideas that used multiple actions, especially for resiliency, were split. But we attributed them as one idea for the rest of the report, which requires consistency in the voting data. For example, one idea, simply called **Transmission**, included four technologies:
    - QE to enable grid security and substation security
    - QS to detect tiny perturbations in EM field
    - Transmission of data for QS and QC to enable transduction (up-conversion or down-conversion of data) as well as transmission and communication, which requires photons
    - QC to process data and take predictive actions through optimization and contingency analysis

Experts in the quantum computing industry, energy sector, and academia assessed each of the 276 use cases in terms of relative feasibility and impact, providing deeper insight into each idea. **Quantum Secure Communications for Monitoring and Control** was deemed to have the greatest feasibility and the highest impact over the other ideas. The scatterplot (Figure 1) shows two other use cases occupying the upper right quadrant: **QRNG and QKD for Securing Grid and Distributed Energy Resources (DER) Communications** and **Real-time Anomalous Voltage Differential Sensing.**

The average of votes from all members on the 40 selected concepts normalized on a 0 to 10 scale.

Figure 1:
Overall Impact/Feasibility



This legend applies also to Figures 9, 14, 18 and 23

- Quantum secure communications for monitoring & control
- Security constrained unit commitment
- Security constrained optimal power flow
- Contingency analysis
- Performance sensors for critical infrastructure
- GPS-independent time synchronization
- Anomalous voltage differential sensing
- Optimize power flow by dispatching controllable resources to improve energy efficiency
- QC optimization for EV charging via connected charging stations and microgrids (or distributed standalone renewable sources)
- Defense-In-Depth
- Security vulnerability at the OT/IT Seam
- Grid resilience optimization
- Communication security across smart grids
- Resilience and security in distribution grid
- Concept: breakthroughs in material science and quantum chemistry via quantum computation
- Transmission: quantum entanglement / sensing / and data
- Real time sensing / forecasting and optimization of power generation and flow
- QS & QE for anomaly detection for resilience and security
- PNT QS for PNT to securely track EVs as assets or load
- QC for forecasting (weather / market participation)
- Real-time anomalous voltage differential sensing
- Critical failure path identification
- Q-algorithms for consistency analysis related to power system assessment & location allocation & power system control
- Planning (transmission expansion / generation expansion / distribution grid with EV integration)
- QS/QE for anomaly detection and timing to secure and synchronize the grid and distributed energy resources (e.g. solar / storage / electric vehicle)
- QC for contingency analysis
- QRNG and QKD for securing grid and distributed energy resource (DER) communications
- QC for climate modeling / forecasting
- Fast DC fault detection: key for offshore wind integration
- Capital Investment and planning optimization
- Security constrained unit commitment
- PQC Proxy for SCADA
- QKD as a Service
- Quantum network components
- Grid resilience optimization
- FLISR being achieved with Quantum ML by detecting anomalies
- Cyber attack discovery
- Optimizing for resilience across changing demand patterns / variable generation / and extreme event impacts
- Understanding new or changing assets on the grid.
- PQC for OT assets with a small key length to operate cost-effectively

Communications and securing the grid dominate the upper right quadrant (Figures 2-6).

Figure 2:
QRNG and QKD for Securing Grid and Distributed Energy Resources (DER) Communications

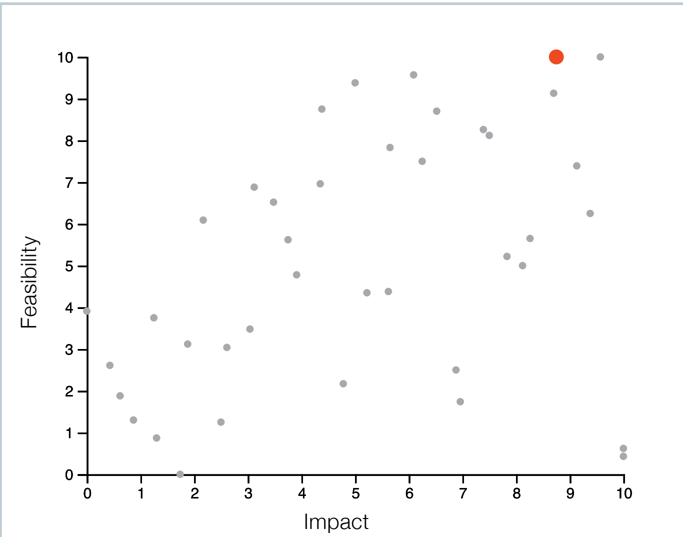


Figure 3:
Quantum Secure Communications for Monitoring and Control

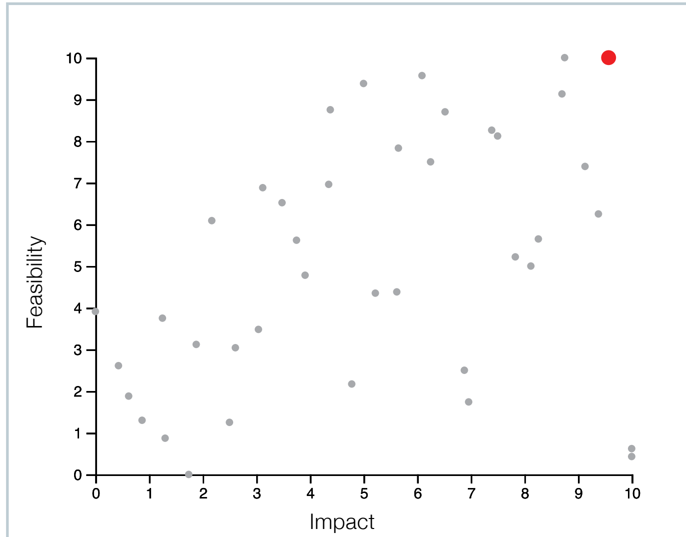


Figure 4:
Real-time Anomalous Voltage Differential Sensing

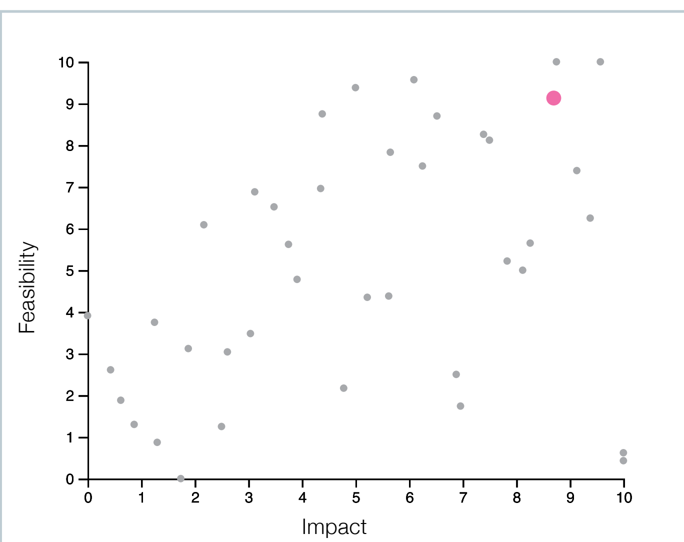


Figure 5:
QS & QE for Anomaly Detection for Resilience and Security

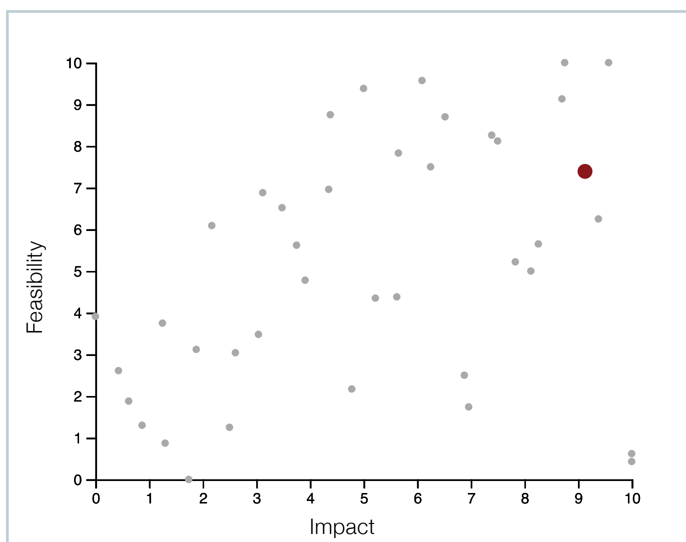
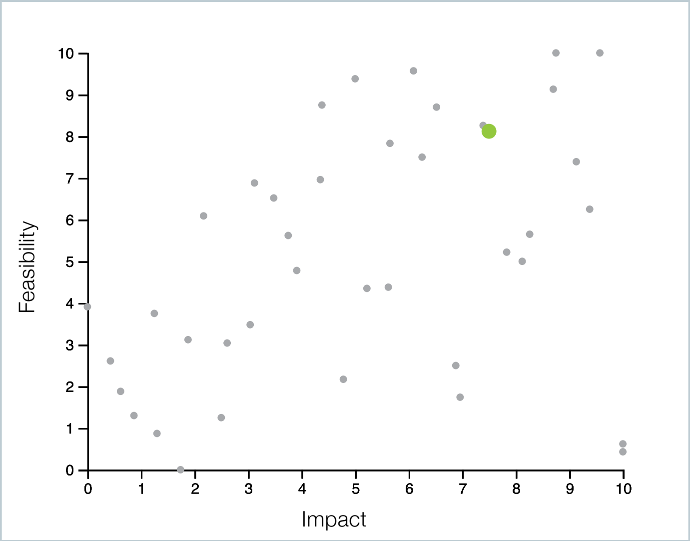


Figure 6:
Grid Resilience Optimization



There were two concepts that had very high impact, but almost no feasibility – **QC for Climate Modeling/ Forecasting** and **Critical Failure Path Identification** (Figures 7-8).

Figure 7:
Critical Failure Path Identification

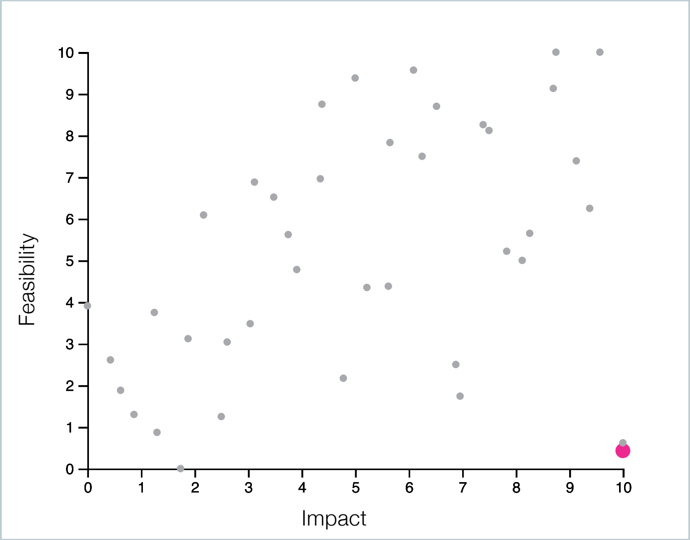
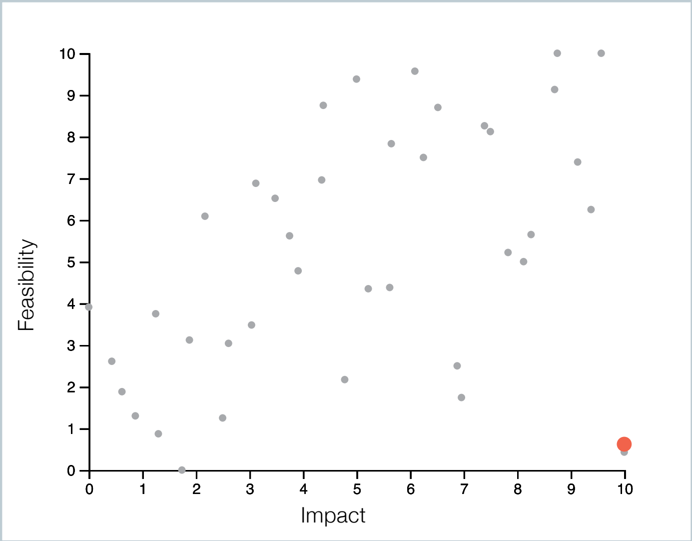
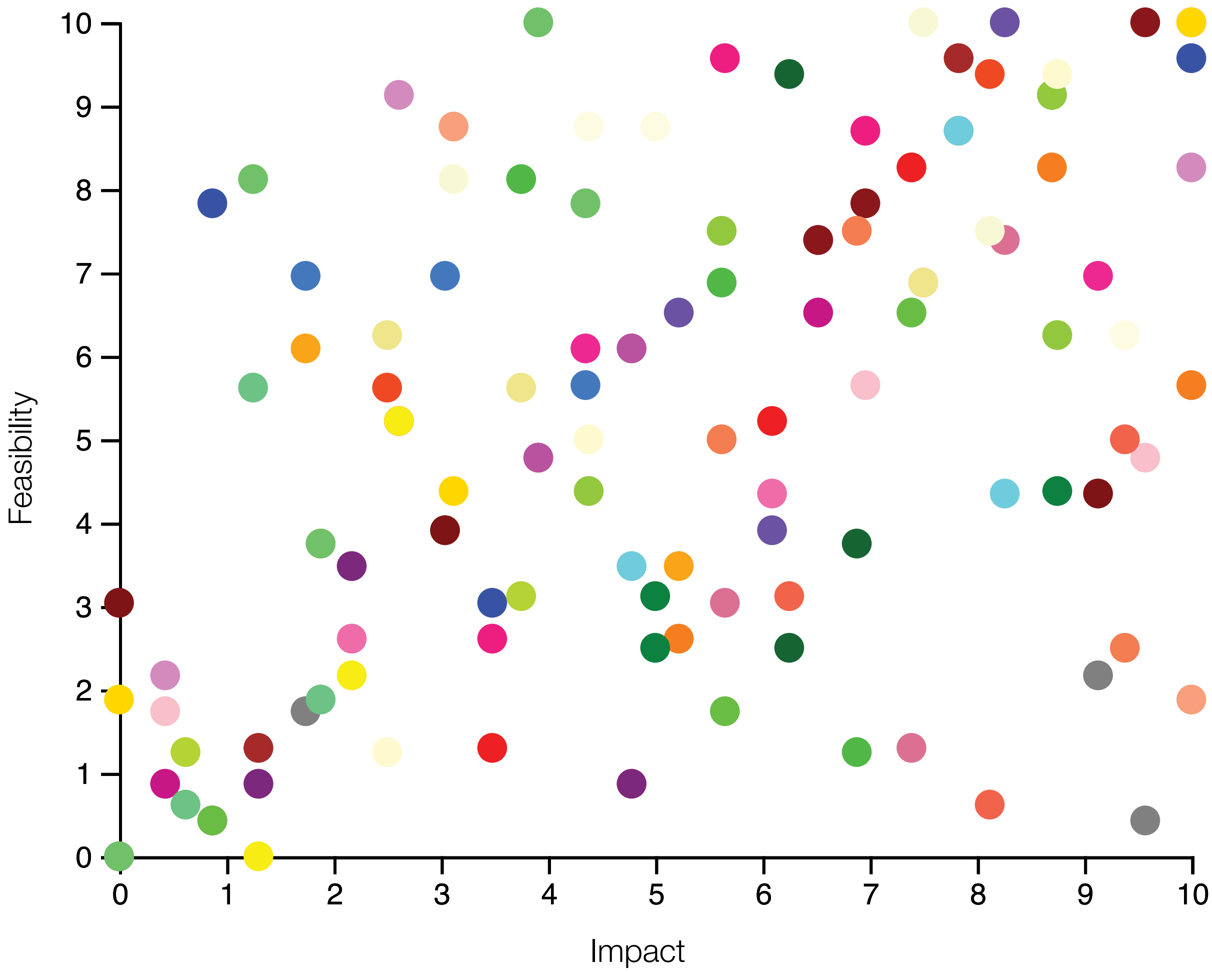


Figure 8:
QC for Climate Modeling / Forecasting



By looking at the Feasibility vs. Impact matrix for different populations of participants, patterns started to emerge (Figure 9). For example, there was very little consistency in voting among the groups. **Quantum Secure Communications for Monitoring and Control** was the only idea that won high feasibility and impact across industry, federally funded research and development centers (FFRDC), and academia (Figure 10).

Figure 9:
Industry, FFRDC, Academia



See color code legend on page 11

Industry and FFRDC agreed that QRNG & QKD are promising for DER (Figure 11). Industry experts thought that **Planning** was very important while FFRDC and Academia gave it less weight (Figure 12). Academia felt that **Fast DC Fault Detection for Offshore Wind** would be very advantageous (Figure 13).

Figure 10:
Quantum Secure Communications for Monitoring and Control

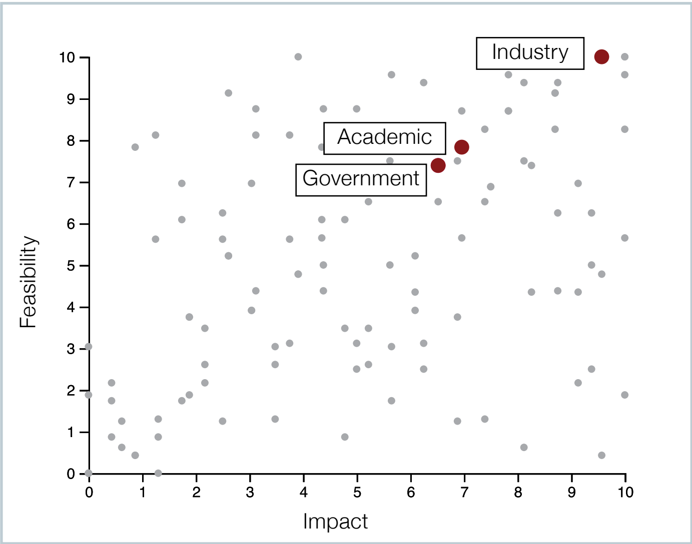


Figure 11:
QRNG & QKD for DER

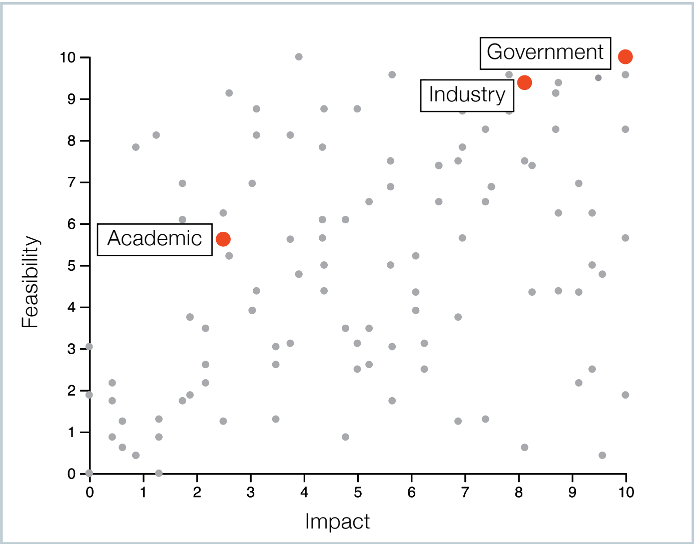


Figure 12:
Planning

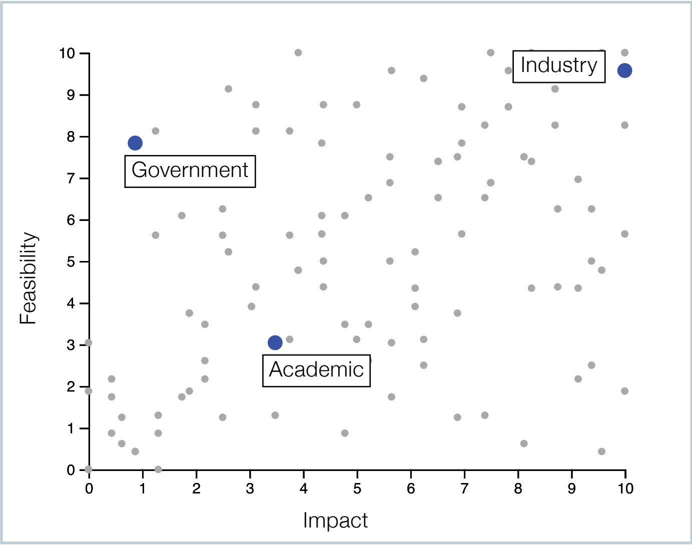
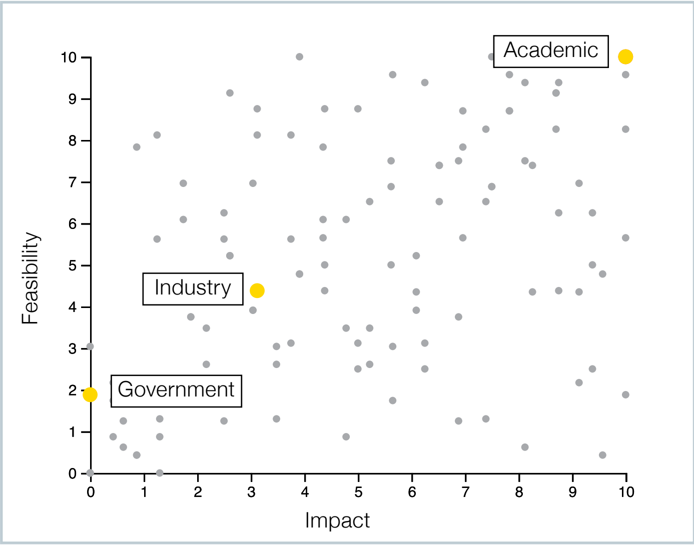


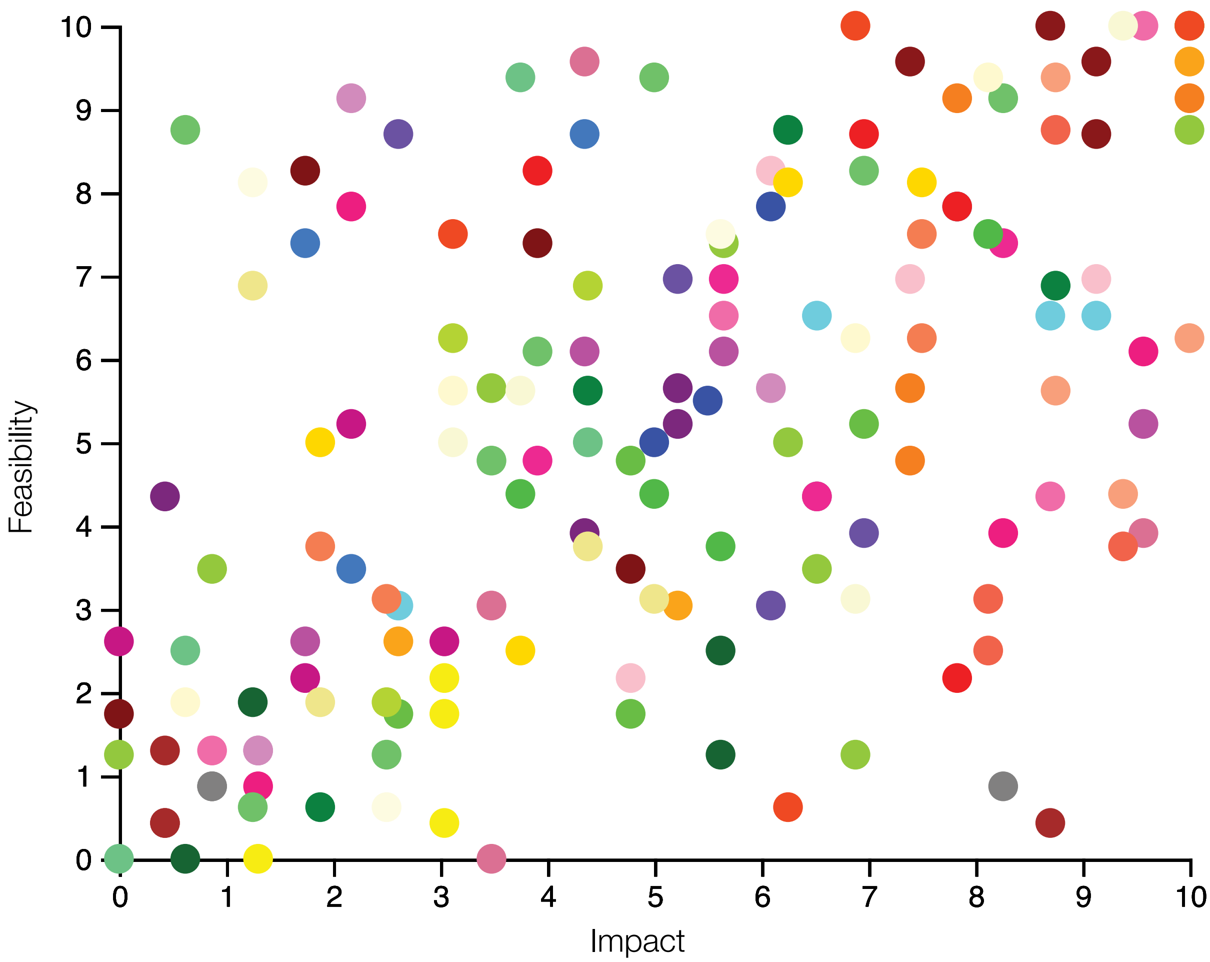
Figure 13:
Fast DC Fault Detection for Offshore Wind



Breaking down the scores further revealed differences among industry participants with experiences in energy, PQC, quantum communications, and quantum computing (Figure 14). For example, these groups focused on **Quantum Secure Communications for Monitoring and Control** as well as **Grid Resilience Optimization.** However, the security-focused participants were most interested in PQC and communications, and they supported **Defense in Depth**. By contrast, the energy and quantum computing cohort saw that as less of a priority. Perhaps the quantum experts don't have the security industry context regarding this trend.

Figure 14:

Industry (Energy, PQC, Communications, Compute)



See color code legend on page 11

The industry participants found agreement for **Quantum Secure Communications for Monitoring and Control** (Figure 15) and **Grid Resilience Optimization** (Figure 16), but disagreement on **Defense in Depth** (Figure 17).

Figure 15:
Quantum Secure Communications for Monitoring and Control

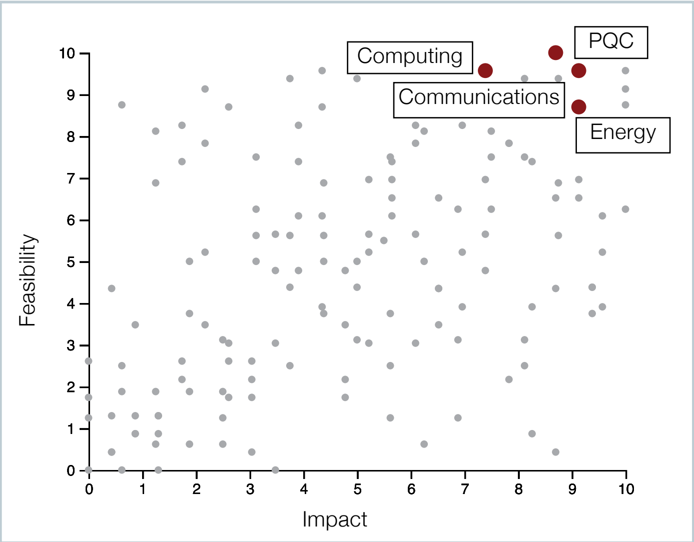


Figure 16:
Grid Resilence Optimization

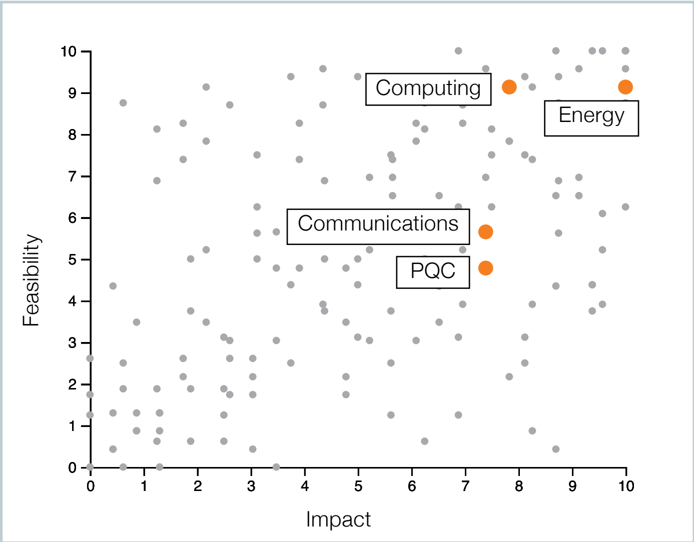
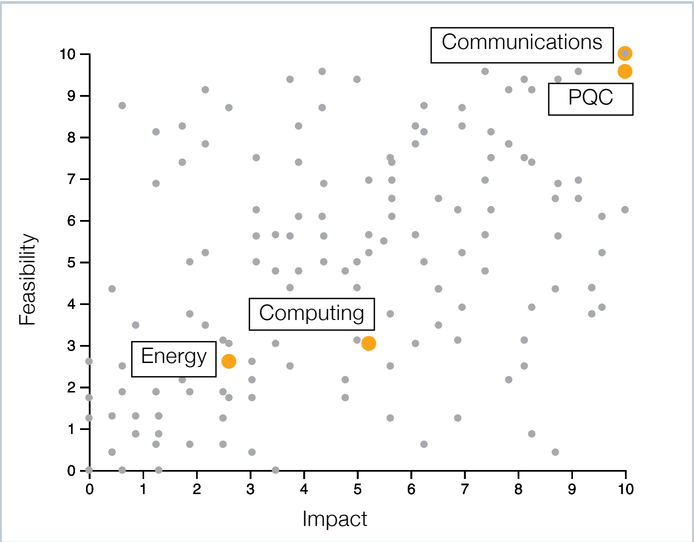
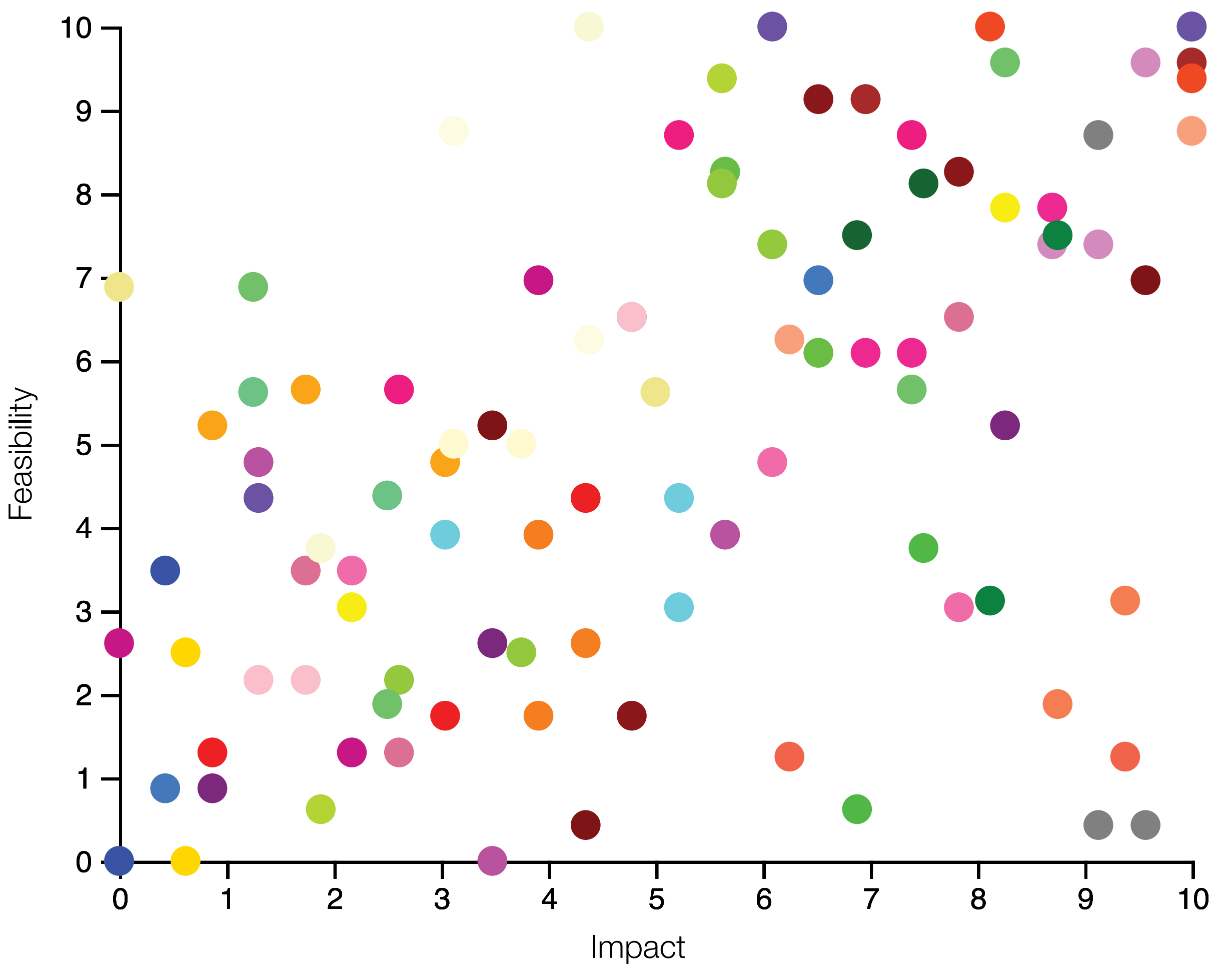


Figure 17:
Defense in Depth



The DOE/FFRDC participants (Figure 18) were aligned on the top ideas, including the exploration of **QRNG and QKD for Security Grid** and **DER Communications** (Figure 19); **Real-time Anomalous Voltage Differential Sensing** (Figure 20), and **Q-algorithms for Consistency Analysis Related to Power Systems Assessment**, **Location Allocation**, and **Power System Control** (Figure 21). Critical differences emerged regarding ideas for **Communications Security on Smart Grids** among communications, energy, and QC experts. QC specialists in particular were not finding this very compelling or feasible because of implementation challenges. (Figure 22).

Figure 18:
DOE/FFRDC (Energy, Communications, QC)



See color code legend on page 11

Figure 19:
QRNG and QKD for Security Grid and DER communications

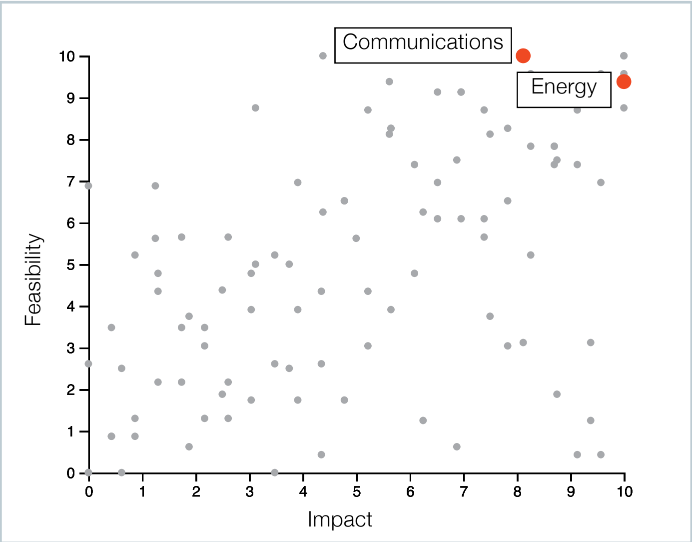


Figure 20:
Real-time Anomalous Voltage Differential Sensing

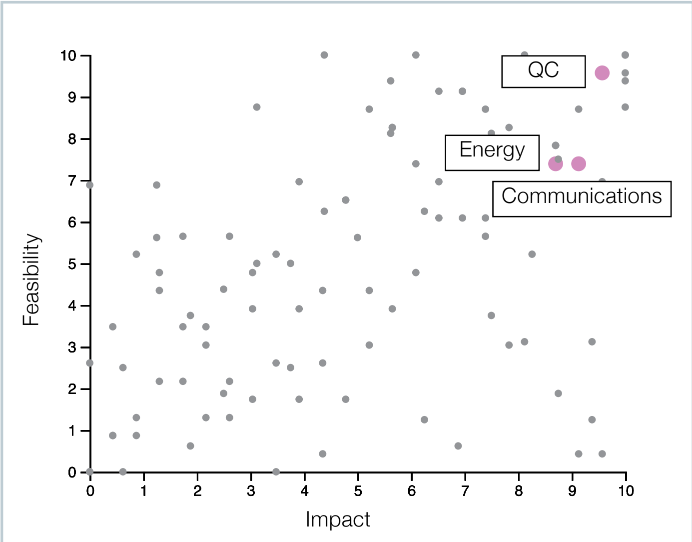


Figure 21:
Q-algorithms for Consistency Analysis Related to Power Systems Assessment, Location Allocation, and Power System Control

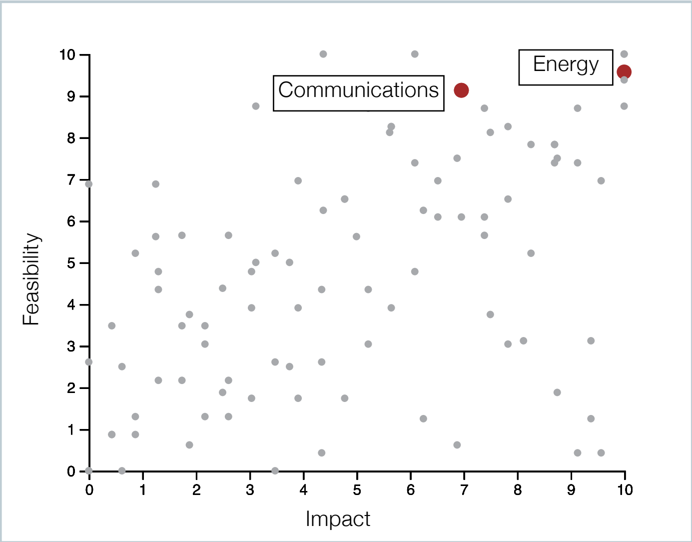
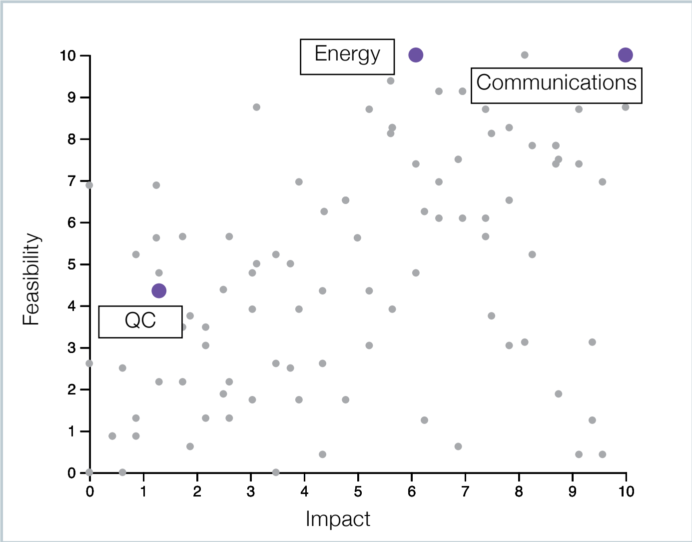


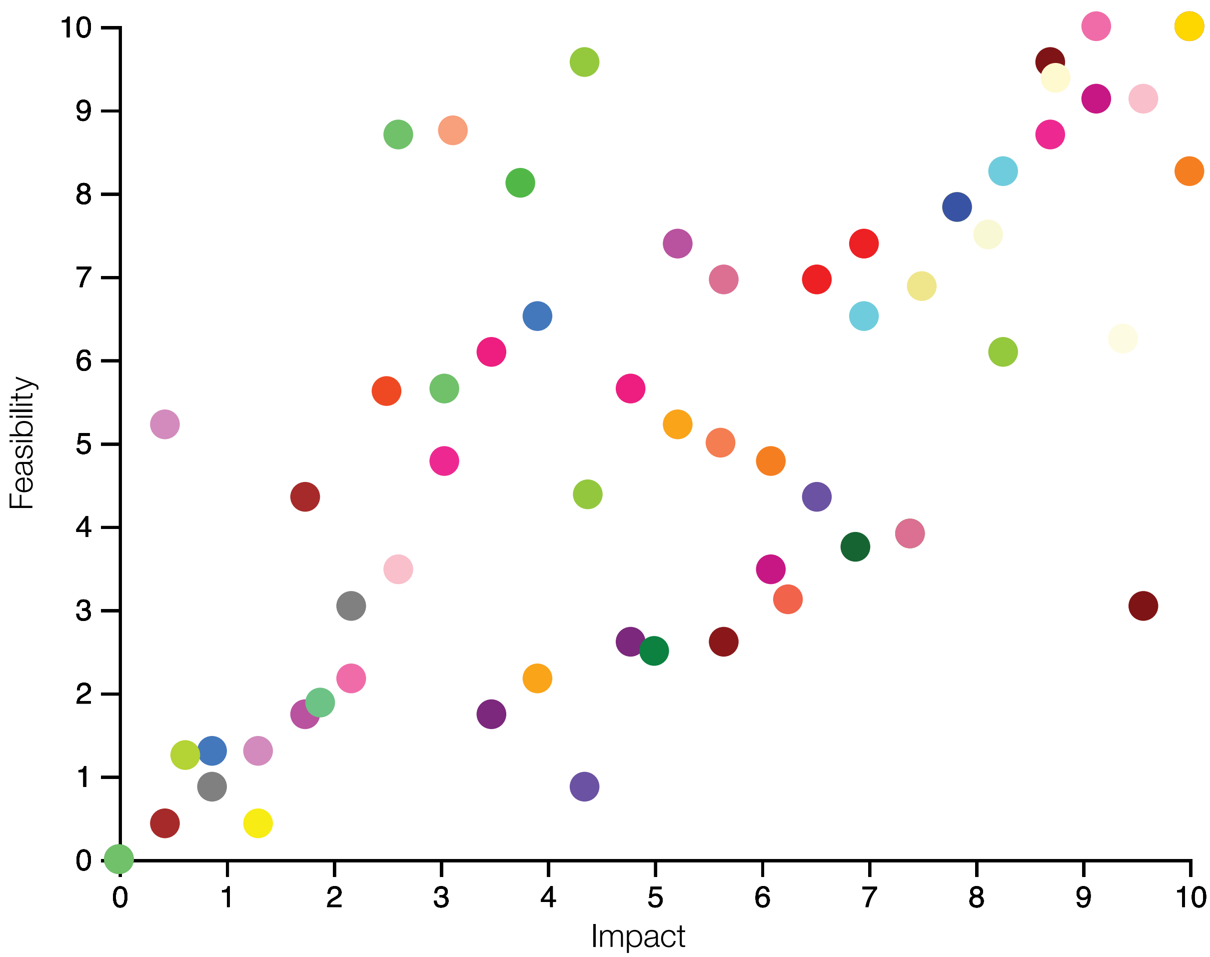
Figure 22:
Communication Security on Smart Grids



Note: Figure 19 and Figure 21 did not have QC participants involved.

Finally, our two pools of academics with sensing and energy backgrounds (Figure 23) were generally split on all the highly impactful and feasible topics (Figures 24-26).

Figure 23:
Academics (Sensing and Energy)



See color code legend on page 11

Figure 24:
Security Constrained Optimal Power Flow

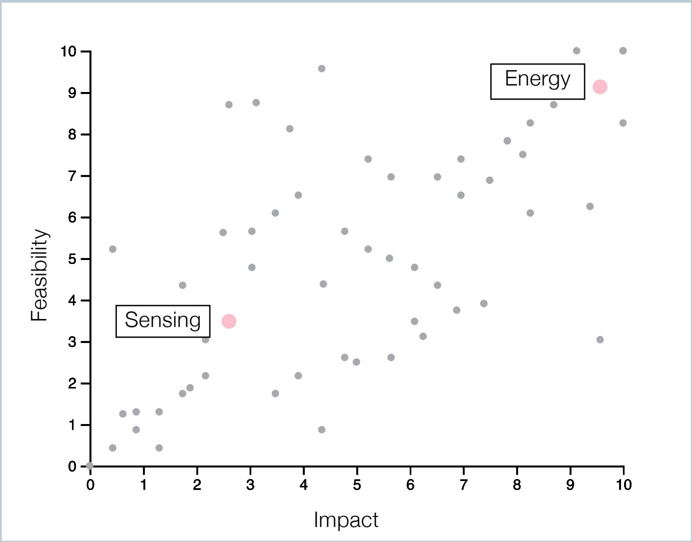


Figure 25:
PNT QS for PNT to Securely Track EVs as Assets or Load

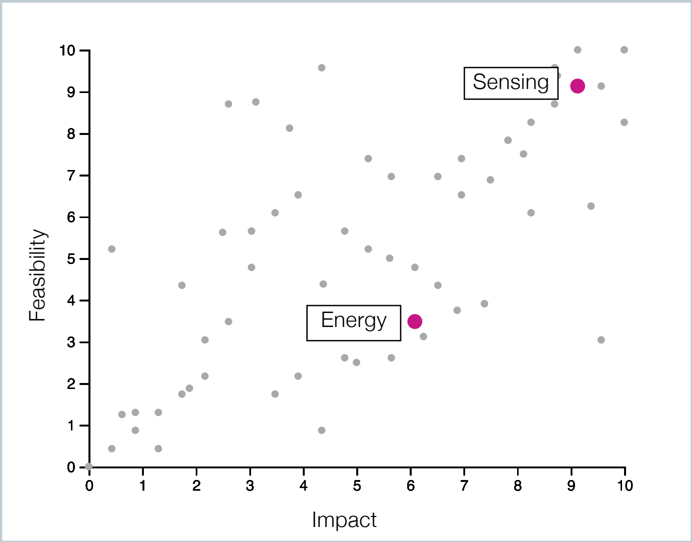
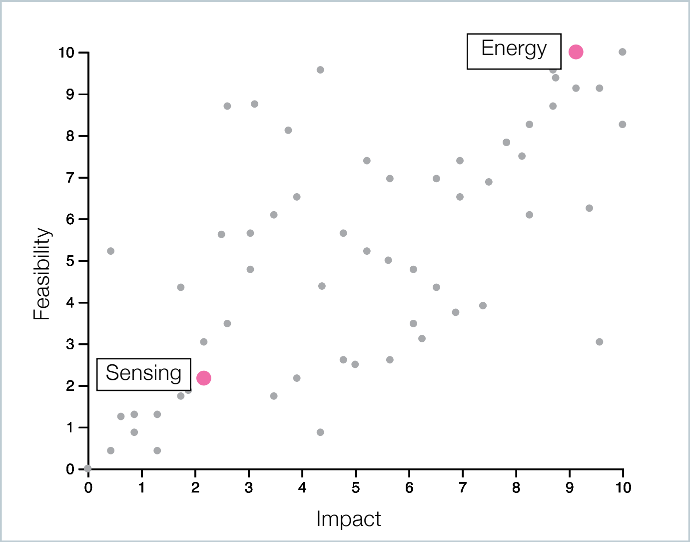


Figure 26:
Contingency Analysis



Physical Grid Anomalies

Quantum sensing could help with physical grid anomaly detection by tracking electrical, magnetic, and thermal/ temperature changes. Higher fidelity data from quantum sensors could be used to create better prediction models for degradation and faults. Additionally, quantum sensors which provide more accurate voltage differentials can be used to create greater resilience and security in the power grid. These promising concepts require further evaluation.

Grid voltages fluctuate all the time for many different reasons, like variations in output, corroded connections, overloading on the network, defective electrical products, and more. Fluctuations can wreak havoc if the voltage differentials are higher than expected. On top of that, malicious actors are proliferating along with entry points, thanks, in part, to DER. They are finding new ways to disrupt power flow, upset frequency regulation, and upend grid stability.

QS, along with quantum entanglement, could enable utilities to identify much subtler changes in the electric or magnetic fields around the grid and with greater precision – and potentially across greater distances.

QS would do this by enabling a high degree of visibility and situational awareness of the grid and grid assets at the distribution and transmission levels. For example, QS can detect the slightest changes to frequencies and power flow to identify a source, pattern, and location of a problem before they produce cascading effects. QS and entanglement can also sense interceptions, providing additional security.

This solution can work in several ways. QS can collect data and compare it to historical expected values. If the data does not match historical expected values, the user could investigate whether they have a security or a hardware issue. With machine learning, based on the QS data, the grid can get smarter and recognize the fingerprints of specific assets.

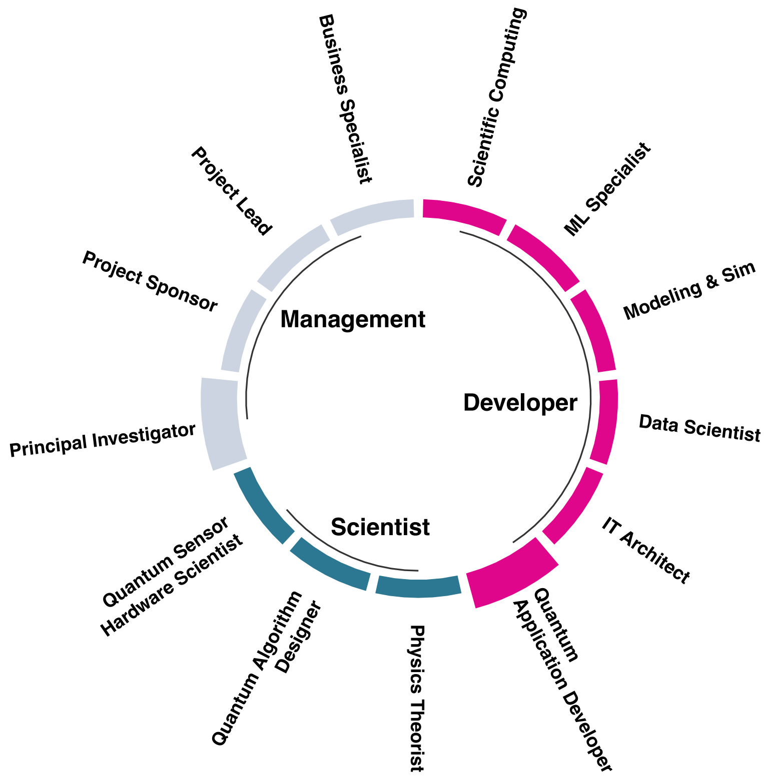
Quantum magnetometers like SQUIDs, NV centers, atomic, etc., are more sensitive and can achieve higher resolution than conventional magnetometers potentially enabling earlier detection of anomalous events and initiating compartmentalization of source.

If successful, operators will be better able to predict if and when transformers will blow out by looking at magnetic and electric fields differentials.
Quantum sensing could also identify problems in unmanned energy generators and secure timing independent of GPS.

To advance this concept beyond the idea, a sample set of skills and timeline are shown in Image 1, Staffing and Timeline for Physical Grid Anomalies:

Image 1

Staffing and Timeline for Physical Grid Anomalies



Physical Grid Anomalies						
Project	**QS & QE for Anomaly Detection for Resilience and Security**					
Goals	Detect cyber security attack. Detect sensor anomaly events for QA/QC. Secure timing independent of GPS					
Timeline	3m	6m	9m	12m	15m	18m
Activities	Research magnetometers	Problem design & expert interviews	Data rationalization & acquisition	Research, design and experiment	Infrastructure and application runtime	Publication
Project	**Anomalous Voltage Differential Sensing**					
Goals	Predication of when transformers will blow out by looking at magnetic & electric fields by differences in the fields from the norm, Real-time monitoring for problem in the grid based on magnetic & electric fields. Could determine problems in an unmanned energy generator					
Timeline	1yr	2yr	3yr	4yr	5yr	6yr
Activities	Research		Solve		Develop	

Contingency Analysis for Resilience

Quantum contingency analysis is a means to more accurately identify vulnerabilities and then build strategies to bolster resilience. The need is acute. The challenges to the grid have become more complex: Outages due to severe weather are more frequent than in the past, causing major failures. DER is stressing resources and creating more entry points for bad actors. Some experts are particularly concerned with monitoring of the infrastructure underground, which accounts for 20% of the grid and is growing.

Quantum annealing and gate-based quantum computers with the appropriate suite of quantum software could be utilized to solve optimization, power flow, and dynamics. The resulting information could provide an understanding of the upgrades needed in the power grid to improve energy storage or positioning of lines and transformers. Or it could identify locations of sustainable power generation and upgrades needed for efficient distribution.

In each case, the ability of quantum computing to handle highly complex problems is essential. Traditionally, utilities engineers could consider the outage of only one or two components at a time. They'd use simulations and then, through a sequential system, solve linear equations (SLEs) for every single outage scenario and combination. Using future quantum computing, utilities can analyze a higher number of contingency plans by simultaneously solving scenario-based power flow problems. They can also take into account dynamics for contingency, which complicates the analysis exponentially.

As a result, for both information technologists (IT) and operational technologists (OT), QC could give them the ability to handle a much bigger solution space than is possible classically. This then simplifies control complexity for operators – especially given an ability to update plant parameters based on new information, almost in real time.

The Quantum Approximate Optimization Algorithm (QAOA) or the Variational Quantum Eigensolver (VQE) in a gate-based QC could help utilities make better decisions, such as where to inject battery power. This would require modeling the problem for execution on a quantum computer. If modelled correctly, a quantum computer could help find better solutions when many variables are unknown, such as operations of assets behind the meter — like consumer batteries and power walls.

Today's quantum computers are accessible through the cloud for experimentation with optimization and simulation problems; however, for now, we are limited in the extent to which we can help with performance optimization at larger scales.

The success of quantum contingency analysis will emerge in many forms:

- Improved response times versus classical optimization
- Through grid statistics, including more uptime, improved efficiency, better systems — as demonstrated by fewer blackouts or brownouts
- Higher power quality, as evidenced by fewer cascading power failures

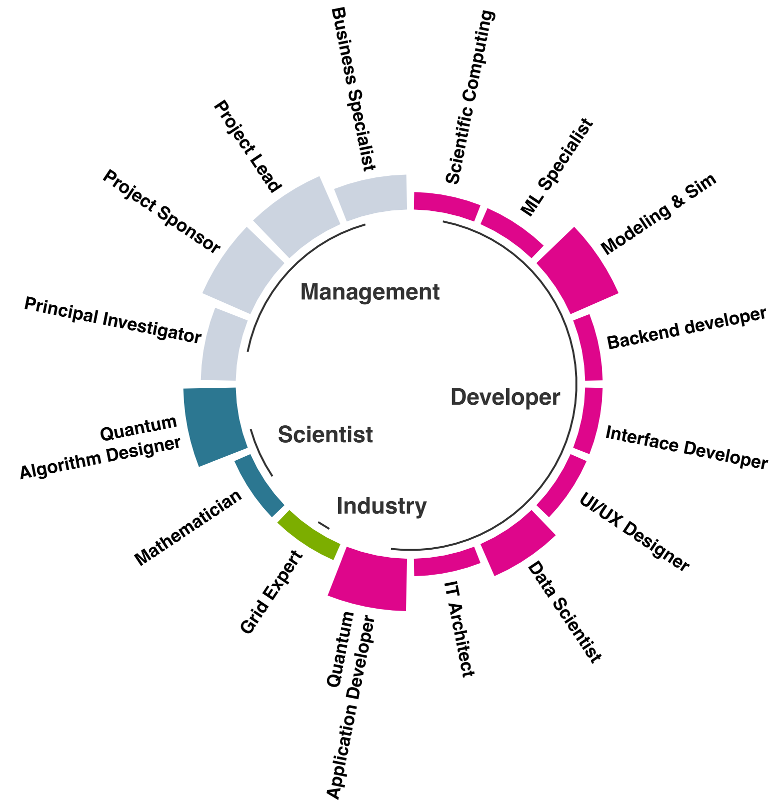
Resilience also includes data collection from QS for analysis by QC. For example:

- Today quantum sensors are read with classical results, but in the future these sensors could be connected through a quantum internet direct to central quantum computers
- For underground infrastructure, QS could sense magnetic fields for what we can't see
- QS could help to determine the potential limit for line and voltage violations

To advance this concept beyond the idea a sample set of skills and timeline are shown in Image 2, Staffing and Timeline for Contingency Analysis for Resilience:

Image 2

Staffing and Timeline for Contingency Analysis for Resilience



Contingency Analysis for Resilience						
Project	**Contingency Analysis**					
Goals	Speed, scalability, better convergence, improved resilience					
Timeline	2m	4m	6m	8m	10m	12m
Activities	Problem definition & design	Data rationalization & acquisition	Research, design, experiment & infrastructure, runtime			Publish & deploy
Project	**Optimization for Resilience**					
Goals	Compare against classical optimization: response time, explored problem space. Grid statistics: uptime, efficiency, system stability (blackouts / brownouts), power quality (cascading power failures)					
Timeline	1yr	2yr	3yr	4yr	5yr	6yr
Activities	Educate & collaborate	Research	Solve	Develop		
Project	**Planning Optimization: Distribution Grid with EV integration, Transmission Expansion, Generation Expansion**					
Goals	Sustainable energy production, reduced environmental impact, increase flexibility, increased resilience					
Timeline	2yr	4yr	6yr	8yr	10yr	12yr
Activities	Gather data sources and test algorithms on quantum devices (Feasibility)	Scalability to larger sized optimization and simulation problems (Scalability)		Planning used for real-world power grid use cases (Demonstration)		

Secure Control Communications

PQC was seen as offering an immediate opportunity to secure all types of data and information across grid operations with 24/7 monitoring and control. These include certificates and digital signatures at the endpoints, whether for sensors or control systems. One important target for PQC security enhancement are Supervisory Control and Data Acquisition (SCADA) systems. Depending on their operations, industries may decide to implement PQC algorithms directly to meet their cybersecurity needs. Or they may deploy a software or hardware-based proxy which enables quantum-safe sessions between devices that are not ready to support PQC.

PQC algorithms can have both open source or commercially supported variants. It has the advantage that it can be implemented in hardware or software and can be deployed via IT policy allowing it to be configured centrally then enforced across many distributed systems. Also, it can be set up with cryptographic algorithm agility in mind. This means that old algorithms can be swapped out as additional ones become available. It can operate on legacy systems with backwards compatibility if the systems can handle the processing need. The U.S. military has approved this method and currently uses it.

PQC would work by connecting nodes on the grid (transmission sites, transformers, etc.) to a data network secured by PQC. QRNGs are an optional part of PQC and can be used at each node - or they can be cloud-based - to provide quantum random numbers to seed encryption keys. The energy distribution commands can be authenticated with PQC to prevent attacks such as injection of unwanted commands or man-in-the-middle interference. Security systems can monitor certificates and digital signatures using PQC at endpoints for sensors, control systems, and other vulnerable components of the grid.

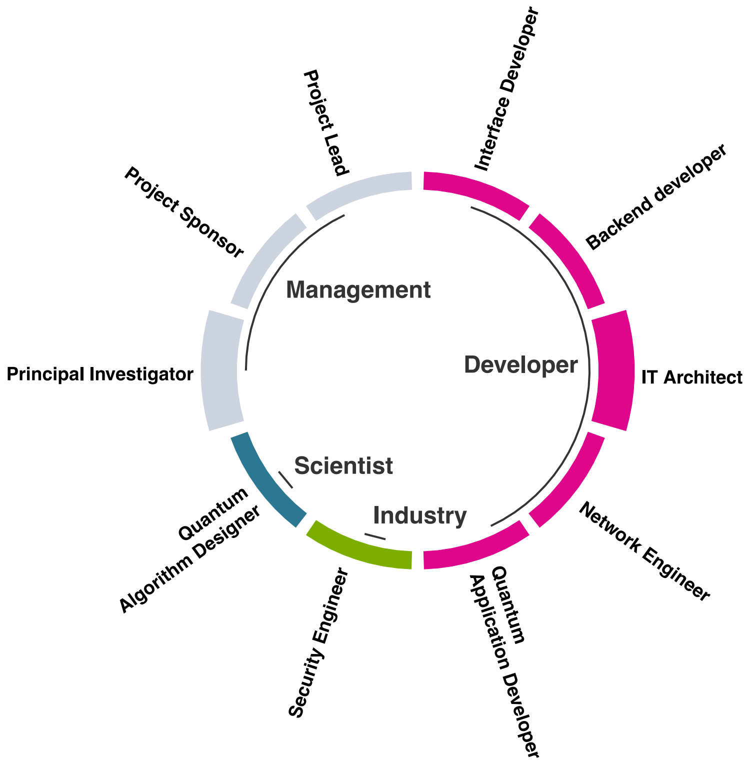
Not every piece of grid infrastructure can be set up for PQC directly. As an interim step, they can use a proxy. In this case, the proxy utilizes PQC to encapsulate connections between endpoints that do not support PQC. Technicians can determine the device requirements and optimize efficiency for deploying the proxy. The proxy solution gives SCADAs crypto agility because new PQC protocols can easily be swapped in the proxy with no change to other infrastructure.

Successful PQC implementations will be able to withstand attacks on control and communications networks. They will also be able to minimize overhead, including runtime, power demands, and computing resources.

To advance this concept beyond the idea, a sample set of skills and timeline are shown in Image 3, Staffing and Timeline for Secure Control Communications:

Image 3

Staffing and Timeline for Secure Control Communications



Secure Control Communications						
Project	**PQC Proxy for SCADA**					
Goals	Not all endpoints have the compute resources that are capable of processing PQC. Figuring out what proxies are needed, which device need to be upgraded/replaced are core problems					
Timeline	1m	2m	3m	4m	5m	6m
Activities	Research tools and knowledge	Determine device requirement, architecture	Initial deployment & field trial Full deployment			Full deployment
Project	**Quantum Secure Communications for Monitoring & Control**					
Goals	Resilient data communication across energy infrastructure which can withstand attacks on the control and communications network segment of the grid. Not too high overheads to implement PQC and QRNG (runtime, power demands, compute resources etc. should be minimized)					
Timeline	4m	8m	12m	16m	20m	24m
Activities	NIST PQC Algorithms are already approved and currently being standardized	Develop the entire network stack to incorporate PQC-based encryption. Change systems and procedures			Deploy PQC software onto existing network nodes and verify the new procedures. Carry out threat testing	

Secured Distributed Assets

The electrical grid by nature requires geographical dissemination of many technical systems. Quantum technologies can play a role to secure communications across electrical power meters, main stations, and substations. One such solution, QKD, relies on quantum networks to exchange information and can add a new level of protection for distributed assets.

With QKD, quantum mechanical photons cannot be measured while in flight without introducing errors. Users can encode random information – generated with quantum random number generators (QRNG) – on the states at a transmitter then send the information to a receiver for measurement. The encoded information is delicate, but the system can be setup with acceptable reliability. If the error rate is below a certain threshold, then the user can process the data set. If the error rate increases, then it can be evidence of faults or eavesdropping resulting in security actions to protect the keys. At the end, the transmitter and receiver will share a key known only to them, making this solution information-theoretic secure.

For now, QKD has limited physical range. To date, distances are limited to 120 kilometers. Quantum repeaters would extend the range of reliable transmission of information to more than several hundreds of kilometers. They work by creating entangled pairs of particles using fiber optics as photon communication channels. These particles get distributed to different nodes along the communication channel. In this setup, adjacent entangled pairs share a measurement, which extends the entangling to non-adjacent pairs.

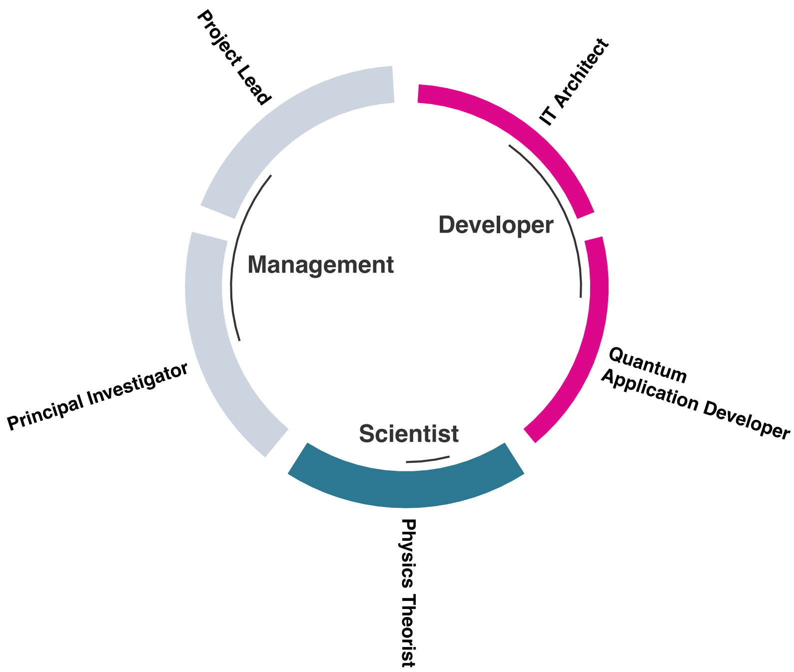
Additional advancements for QKD are to develop a quantum version of a conventional optical transceiver that can either distribute quantum keys or data. Users can do this by encoding in amplitude and phase, which is known as continuous variable encoding, or CV-QKD. It has been shown when using homodyne detection in CV-QKD, this quantum tech can be deployed along with conventional signals that are many orders of magnitude brighter without adding errors to the quantum transmissions. This simplifies the deployment costs since you do not need dedicated dark fiber or to reduce the total classical power sent down an optical fiber.

QKD or quantum entanglement can help energy asset owners by providing additional layers to secure communications between different energy assets. It could also be important to power companies and their customers as well as telecom companies, each of whom rely on secure communications. Network and devices upgrades can be considered for certain communication channels now paving the way for future scale.

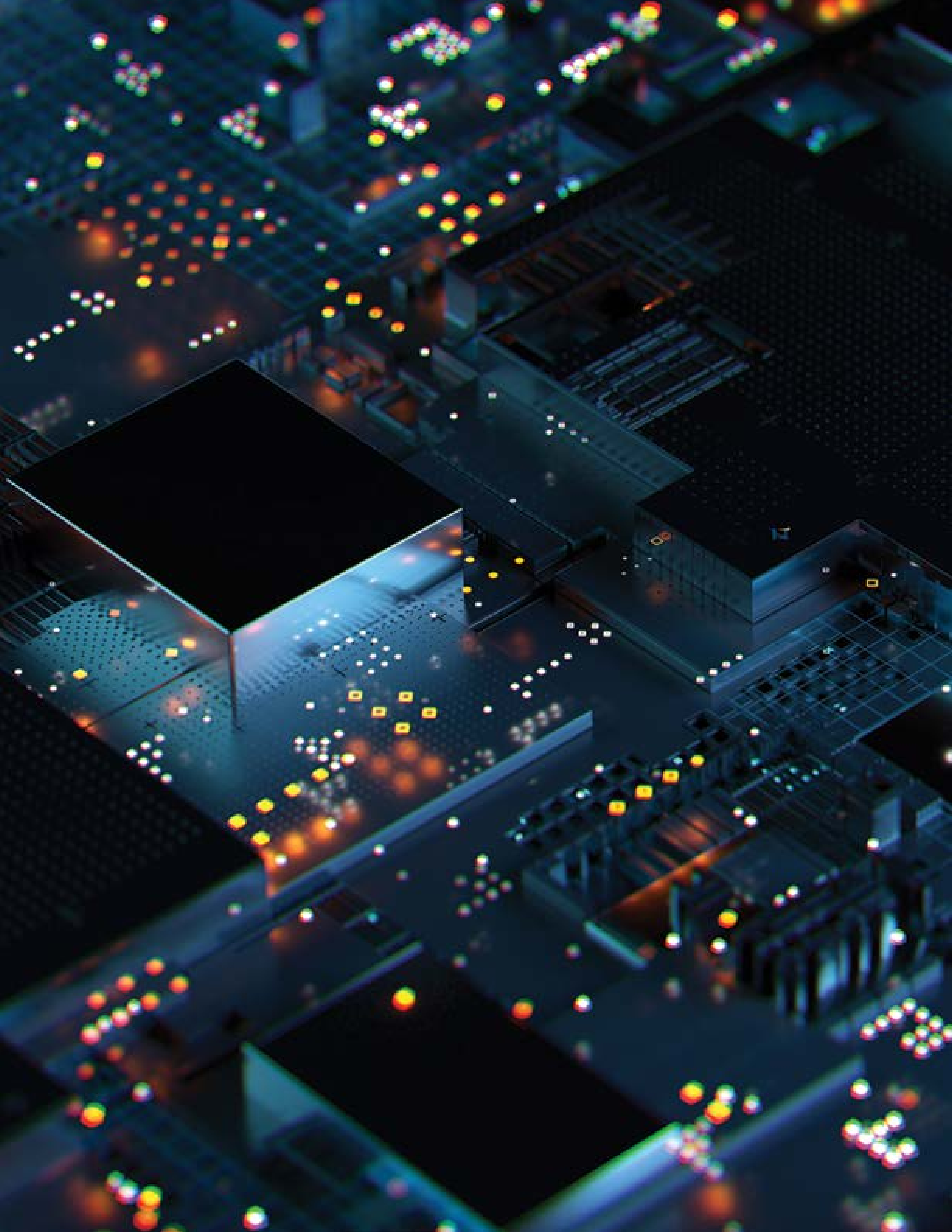
To advance this use case consider a team including a minimum of these skills, as shown in Image 4:

Image 4

Staffing and Timeline for Secured Distributed Assets



It is estimated that a discovery project in this field would take roughly six months to complete.



Synchronization Without GPS

The grid is growing ever more complex with multiple nodes of connection. Quantum sensing along with quantum entanglement can be used to help secure and synchronize the grid and distributed energy resources like solar, storage, and electric vehicles.

Successful implementation will see quantum sensors performing at least a nanosecond faster than classical sensors. Faster performance can promote more transactive energy among producers, consumers, and grid operators. Quantum sensors could also improve the size, weight, power, and cost (SWaP-C) and therefore be able to scale efficiently.

Atomic clocks could be placed on the grid, in substations, and on DERs like solar, wind, storage, and electric vehicles. This would ensure proper timing and synchronization. The atomic clocks, especially those that use entanglement, also have the advantage of providing GPS-independent timing for the exquisite needs of future power grids that integrate multiple assets (including renewables). They also provide the ability to work seamlessly between substations and other grid components. But entanglement is much harder to implement for now.

Yet time synchronization between grid assets is critical; that dependence can be exploited all too easily if the grid relies solely on GPS, which can be spoofed, jammed, or hacked. Quantum sensing cannot replace GPS yet. But since it depends on different inputs, quantum sensing can supply redundancy, particularly in cases where the grid is GPS-denied. Critical infrastructure can then obtain timing, as well as inertial position and navigation, from an on-board quantum sensing system and during satellite disruption.

That can help enable vehicle-to-grid technologies. Additional quantum sensing for timing could support transactive energy at varied timescales — similar to financial markets.

For future power grids, atomic clocks can provide GPS-independent timing. They will need to integrate multiple assets, including renewables and electric vehicles, while working seamlessly between substations and other grid components.

It is estimated that a discovery project in this field would take roughly two years to complete.

Next Steps

Securing the electric grid in the quantum age demands a collaborative effort among grid operators, the quantum industry, and security professionals. As explored in this report, multiple grid segments including generation, transmission, distribution, customer load, asset owners, system aggregators, and service providers require robust security measures to protect against cyber threats. By harnessing the power of quantum technologies, innovative solutions can be implemented to enhance grid security and resilience.

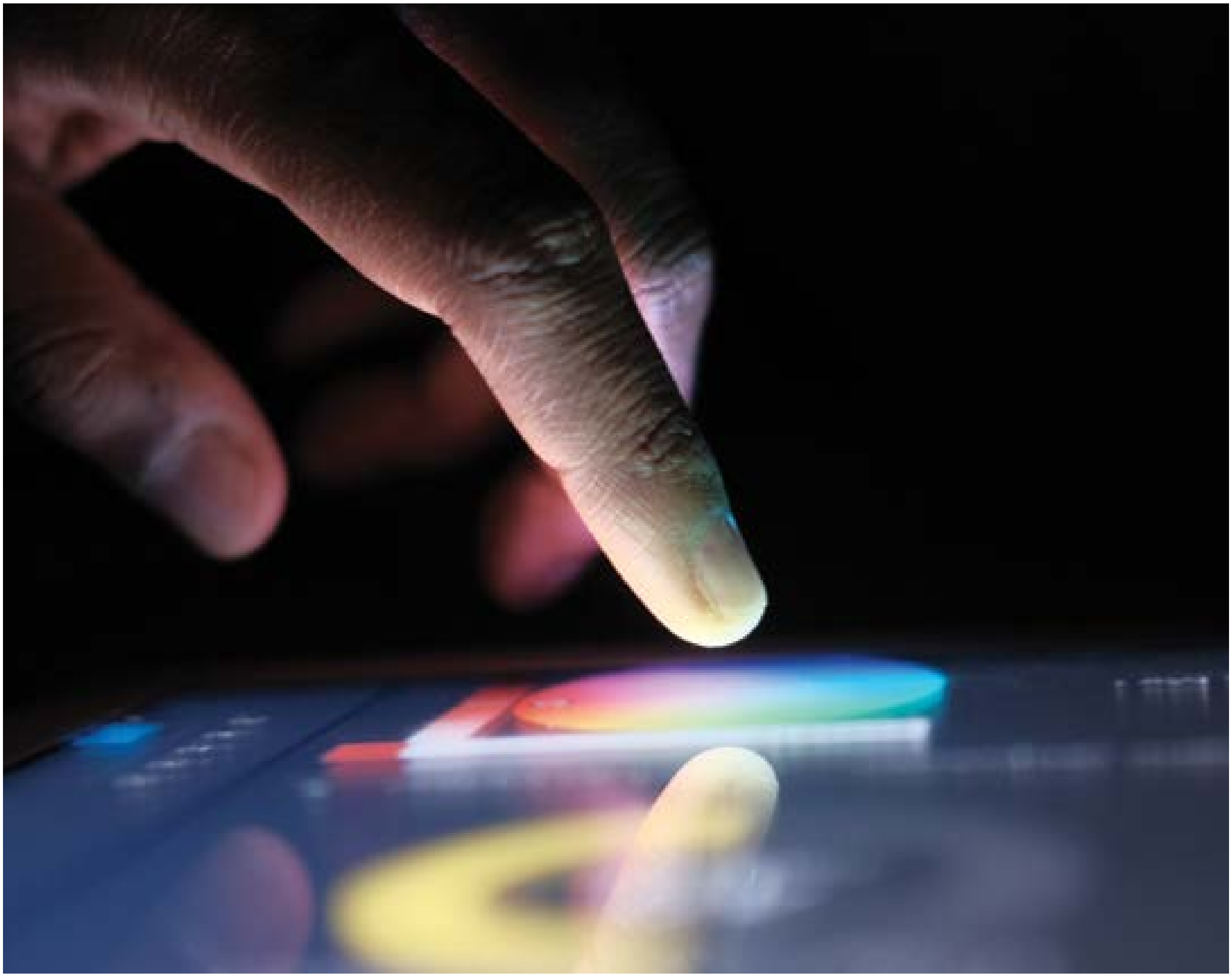
Quantum sensing to detect anomalous voltage differentials would be an important first step. Quantum sensing technologies can provide precise and real-time measurements of voltage variations, enabling early detection of potential threats or anomalies that could compromise grid stability. Leveraging sensing for synchronization, a critical aspect of grid operations, could also be beneficial near term.

Utilizing quantum computing for contingency analysis could enhance the grid's resilience by analyzing various scenarios and optimizing response strategies to mitigate disruptions or cyber-attacks.

Embracing new security controls for both centralized and distributed assets is key for future confidentiality and integrity. PQC and QKD protocols can play a key role in this future, especially when supported by QRNG.

To achieve these advancements in grid security, collaboration among grid operators, the quantum industry, and security professionals is paramount.

Grid operators must actively engage with the quantum industry to drive research, development, and standardization efforts. Security professionals play a crucial role in evaluating and implementing robust security measures and ensuring compliance with industry standards and best practices. Together, they can all pave the way for a safer and more reliable energy infrastructure that powers our societies in the face of emerging challenges.



Acknowledgements

Group	Organization	Name
Academic	Southern Methodist University	Jianhui Wang
Academic	Stony Brook University	Peng Zhang
Academic	Stony Brook University	Yifan Zhou
Academic	The Pennsylvania State University	Nilanjan Ray Chaudhuri
Academic	University of Denver	Amin Khodaei
Academic	University of Southern California, Information Sciences Institute	Ajey Jacob
FFRDC	Argonne National Laboratory	Rajkumar Kettimuthu
FFRDC	Brookhaven National Laboratory	Julian Martinez-Rincon
FFRDC	Brookhaven National Laboratory	Shinjae Yoo
FFRDC	Brookhaven National Laboratory	Meng Yue
FFRDC	Idaho National Laboratory	S M Shafiul Alam
FFRDC	Lawrence Berkeley National Laboratory	Wibe de Jong
FFRDC	Lawrence Berkeley National Laboratory	Mary Ann Piette
FFRDC	Lawrence Livermore National Laboratory	Jean-Paul Watson
FFRDC	Los Alamos National Laboratory	Carleton Coffrin
FFRDC	Los Alamos National Laboratory	Charlotte Duda
FFRDC	MITRE	Charles Fancher
FFRDC	MITRE	Yaakov Weinstein
FFRDC	Oak Ridge National Laboratory	Suman Debnath
FFRDC	Oak Ridge National Laboratory	Nick Peters
FFRDC	Pacific Northwest National Laboratory	Henry Huang
FFRDC	Pacific Northwest National Laboratory	Carlos Ortiz
Government	Department of Energy	Rima Oueid
Government	National Energy Technology Laboratory	Yuhua Duan
Government	National Energy Technology Laboratory	Hari Paudel
Individual	Coherent Computing Inc.	Sonika Johri

Industry	Accenture	Carl Dukatz
Industry	Aegiq Ltd.	Tom Lyons
Industry	Anametric	Jim Gable
Industry	Anametric, Inc.	Wil Oxford
Industry	Cisco	Alireza Shabani
Industry	Ethicqual	Elif Kiesow Cortez
Industry	GE Research	Ananrita Giani
Industry	Hamamatsu Corporation	Takaaki Otake
Industry	Hitachi America	Takuya Okuyama
Industry	IBM	Travis Scholten
Industry	IBM	Jeffrey Sumrall
Industry	Iff Technologies	Kirk McGregor
Industry	Infleqtion	Seth Caliga
Industry	Infleqtion	William Clark
Industry	IonQ	Travis Pyne
Industry	Keysight	Eric Holland
Industry	Keysight	Gabe Lenetsky
Industry	Nebula Space Enterprise	Peter Stridh
Industry	Patero Inc.	Peter Bentley
Industry	Patero Inc.	Crick Waters
Industry	PsiQuantum, Inc.	Roland Acra
Industry	Quantinuum	Ryan McKenney
Industry	Qubitekk	Corey Mcclelland
Industry	Qubitekk	Scott Packard
Industry	Resilient Entanglement	Rozhin Eskandarpour
Industry	Safe Quantum Inc.	John Prisco
Industry	SandboxAQ	Nadia Carlsten
Industry	StratConGlobal	Joanna Peters
Industry	Telepath Systems, Inc.	John Juhasz
Industry	Verizon	Lee Sattler
Not-for-profit	National Quantum Literacy Network	Tonya Thornton
Not-for-profit	WOMANIUM	Prachi Vakharia
Utility	Dominion Energy	Joseph Rigatti
Utility	EDF	Matthew Bishara
Utility	EDF R&D	Etienne Decossin

Utility	Electric Power Research Institute (EPRI)	Shelby Karpa
Utility	Electricity Information Sharing and Analysis Center (E-ISAC)/NERC	Lauren Alexander-Binns
Utility	EPB	James Ingraham
Utility	EPRI	Jeremy Renshaw
Utility	Pseg	Ahmed Mousa
Utility	Southern California Edison	Amanda Olson
Utility	TVA	Ken Carnes
Utility	TVA	Darren DeBaillon

Additionally, the event was open to a broader set of 'observers' including QED-C members and government agencies. Observers had the opportunity to participate in limited activities after idea generation was complete.

Planning and Facilitation

The following individuals were invaluable in organizing the workshop and preparing this report.

Department of Energy

Rima Oueid
In collaboration with the U.S. Department of Energy
Office of Technology Transitions and Office of Electricity

QED-C - Use Case TAC Members

Rima Oueid, DOE (Sensing Use Cases Chair)
Carl Dukatz, Accenture (Compute Use Case Chair)
Terry Cronin, Toshiba
Kevin Glynn, Northwestern
Joanna Peters, StratConGlobal
Keeper Sharkey, Odestar
Abhijit Choudhury, INA Solutions
Ann Cox, DHS
Kirk McGregor, IFF Tech
John Penuel, L3Harris
Elizabeth Wood, AT&T

QED-C

Celia Merzbacher
Jonathan Felbinger
Erin Weeks

Accenture | Accenture Federal Services

Carl Dukatz
Shreyas Ramesh
Kellyn Beeck
Stephen Harper
Garland Garris
Kung-Chuan Hsu
Max Howard
Victoria Hazoglou
Bo Sun
Andrew Driscoll
Frankie Piccirillii
Bri Neff
Nancy Miller

Methodology

Workshop goals: surface high-impact, feasible ideas

- Capture many ideas on the use quantum to secure the electric grid then create a diverse set of concepts to investigate
- Clearly define and refine popular ideas and match to quantum approaches for future exploration including timeline to realization
- Isolate the ideas with the highest impact and feasibility then identify a path to bring these ideas to fruition

Structure: encourage collaboration, fresh thinking

The workshop was designed to create the maximum number of collaboration opportunities among attendees with knowledge of the energy sector and attendees familiar with quantum technologies. It was important that the groups be self-sufficient, finding answers quickly to their own questions so that they could complete all the exercises.

Facilitators and attendees from the quantum sector were briefed on the workshop several days before the event took place to ensure smooth operations.

Participants from the energy sector did not receive a detailed briefing to encourage fresh thinking and new ideas.

Value chain matrix: a bi-directional flow

The primary tool to guide conversations during the ideation session was the Electricity Industry Value Chain – Matrix:

	A. Customer Load/ Energy Asset Owner	B. Aggregator/ Service Provider	C. Distribution	D. Transmission	E. Generation
Description	- Identification and prioritization of primary bidirectional assets (bidirectional EVs, storage, PV, microgrid) - DC power transformed to AC power via inverters - Efficiency factor assessment and improvement	- Forecasting and monitoring - Identification and prioritization of primary bidirectional assets (bidirectional EVs, storage, PV, microgrid) - DER asset aggregator and dispatch (e.g., virtual power plant) - Execute and maintain transactive ledger - Distributed control and notification	- Real time voltage and frequency control across home, buildings, and energy resources - Radial Distribution Networks - Distributed control and signaling according to specified parameters - Dynamics and stability - Large scale coordination - Events and outages	- Occur over one of three power grids (interconnections) that make up North America's power system - Supply at average current of 60 Hertz - Generation facilities dictate power dispatched to grid based on demand predictions - Use Base-Loading and Peaking power plants to manage demand - Increase voltage to transmission network levels - Monitor flow of electricity, monitor reactive power flow, reactive power compensation, improve power factors	- Identification of primary fuel and supply chain of resource as a result of two-way flow network (coal, gas, nuclear, hydro, wind) - Mechanical power transformed to electrical power through generator - Efficiency factor (usually thermal but can be other) assessment and improvement - Connect generation plant to power grid
Post Quantum Computing (PQC) Security Algorithms					
Quantum Random Number Generation (QRNG)					
Quantum Key Distribution (QKD)					
Quantum Entanglement (QE)					
Quantum Sensing (QS)					
Quantum Compute (QC)					

The columns at the top of the matrix describe stages of the electricity supply chain: customer load/energy asset owner, aggregator/service provider, distribution, transmission, and generation. This organizational structure provided participants with starting points to think of specific use cases that could benefit from quantum computing. The pieces of the value chain were not meant to be considered independent of each other. Attendees were also encouraged to think about how the five categories interact and which processes and operations touch multiple parts of the value chain.

The value chain was intended to be thought of as bi-directional, rather than a one-way flow from generation to end customer. As Rima Oueid, Commercialization Executive with the U.S Department of Energy's Office of Technology Transitions, stated in her opening remarks, "The grid is becoming a two-way flow electric and data network."

This bi-directional flow is realized through the evolution of smart grids, which are electricity networks enabled with sensors and digital communication technologies that allow grid operators to monitor usage and network health while ensuring the grid's stable operation.

This increasingly complex grid system has ushered in a need for more advanced technologies, such as quantum and edge computing. Participants were prompted to think of the emerging security controls and requirements for the future grid, and not just solve for pain points in today's electric grid.

The left side of the matrix shows categories of quantum approaches, including PQC, QRNG, QKD, quantum entanglement, quantum sensing, and quantum computing.

Workshop process: idea generator

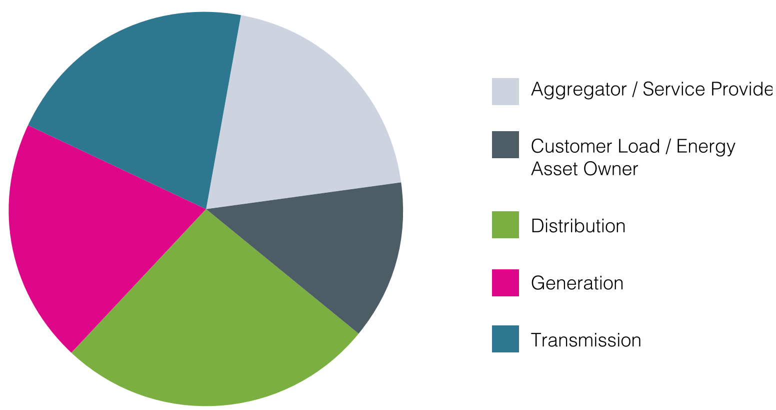
The workshop was designed to create as many ideas as possible up front, methodically select ideas that the participants thought would be the most important, and then develop the remaining ideas into meaningful and actionable concepts. This process yielded three content pieces: Ideas, Concept Cards based on the ideas, and Concept Posters built from the concept cards.

Brainstorm, analysis, selection

Workshop participants were placed into groups to complete a 45-minute ideation session. For the first step, each participant generated ideas in a 15-minute individual brainstorm and placed their ideas onto the Value Chain – Matrix. The groups then took 25 minutes to discuss their ideas, and finally five minutes to vote for the ideas they thought had the most potential.

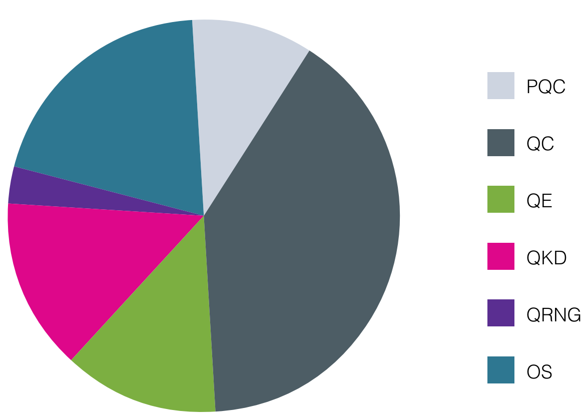
The workshop groups came up with a total of 276 ideas. The ideas were well distributed across the grid areas; however, the majority of ideas fell into the quantum computing solution area.

Ideas by Position in the Value Chain:



Aggregator / Service Provider	55
Customer Load / Energy Asset Owner	37
Distribution	72
Generation	54
Transmission	58
Grand Total	**276**

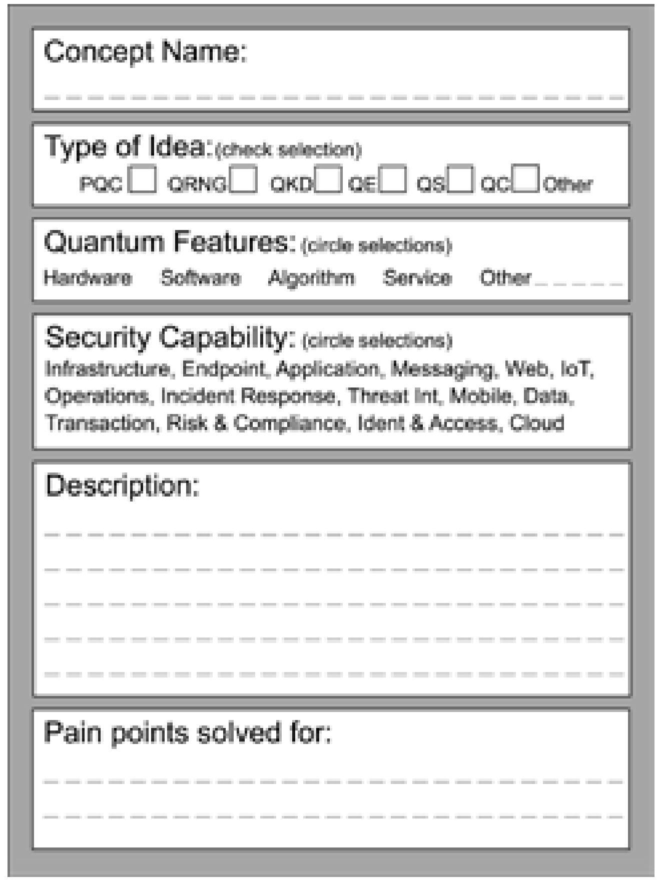
Ideas by Solution Type:



PQC	28
QC	111
QE	36
QKD	38
QRNG	7
QS	56
Grand Total	**276**

Concept Cards: winnowing ideas

Each group selected the ideas that had the most votes and created a “Concept Card” for each idea. As depicted in the figure below, these Concept Cards included the name of the concept, the type of idea, the quantum technology best suited to execute the idea, the related security field, a description of the concept, and the pain points for the concept addressed. The groups had 15 minutes to fill out the Concept Cards. Most groups ended up with between one and three cards that they then presented to the whole workshop audience.



Concept Name:

Type of Idea: (check selection)
PQC ☐ QRNG ☐ QKD ☐ QE ☐ QS ☐ QC ☐ Other

Quantum Features: (circle selections)
Hardware Software Algorithm Service Other

Security Capability: (circle selections)
Infrastructure, Endpoint, Application, Messaging, Web, IoT, Operations, Incident Response, Threat Int, Mobile, Data, Transaction, Risk & Compliance, Ident & Access, Cloud

Description:

Pain points solved for:

A flexible rating system to promote expansive thinking

Concept Cards were rated based on impact and feasibility. Attendees voted on a scale of 1 to 10 – but the rating was not universally defined. Each attendee used their own relative scale. For example, some attendees reported that they scored feasibility by how quickly quantum hardware would reach the level of maturity needed to run the use case. Others thought of feasibility in terms research opportunities and testing on today’s devices.

This rating system empowered the attendees to expand or limit the scope of the original concept based on what they deemed possible given a set scope, timeframe, and the required fields in the Concept Poster. This flexibility led to changes in the concepts’ names and attributes during the actual workshops. In post-workshop attendee interviews, we expanded details in the Concept Posters.

Concept poster: how to execute

After further discussing the feasibility and impact of the Concept Cards, the workshop attendees agreed to focus on three top concepts to develop into Concept Posters. Attendees were instructed to use the original Concept Card as a basis for the Concept Poster. As shown in the following chart, the Concept Posters included a description of the concept, how it works, the problem space it occupies, key features, types of personas the concept will affect (consumers, grid operators, policy makers, etc.), and key metrics and outcomes to measure success. The Concept Posters also included a Collaboration Plan, which identified potential team members and suggested a timeline to complete the project.

Concept Poster & Collaboration Plan

Concept Name:	Description:
Persona:	
How it works:	Features:
Problem Space:	Success Metrics/outcoimes:

Team members

PI	Mathematiciam	Physics Theorist	Scientific Computing	Modeling & Sim	Interface Developper	Data Scientist	Backend Developper	ML Specialist
Project Sponsor	Project Lead	Business Specialist	Q Algos Designer	Qauntum Developper	IT Architect			

Timeline

	Start								Finish
Research									
Solve									
Develop									

List of Ideas

All Ideas (Total 276):

Concept	Energy	Quantum	Group
Security in DERs, EVs as Communication Is Increased	Aggregator / Service Provider	QKD	EV Coms
EV Charger Integration Planning (Optimization - Quantum Annealing)	Aggregator / Service Provider	QC	Planning
Distribution: Breakthroughs in room-temperature superconducting materials via quantum simulation/ quantum computing might pave the way for materials that do not have any energy loss when transmitting and distributing energy (about 5-10% of the energy generated in loss in this stage)	Aggregator / Service Provider	QC	Chemistry
Grid Security	Distribution	QKD	All Coms
Security in Control Center and Substation	Distribution	QKD	Control Coms
Communication With Timing and Event Detection	Distribution	QE	Detection
Power Quality Monitoring	Distribution	QE	Monitoring
Enhanced Measurement and Monitoring	Distribution	QE	Monitoring
Optimization and Fault Detection	Distribution	QE	Detection
Clocking and Synchronization	Distribution	QS	Synchronization
EM Detection (Fault Detection)	Distribution	QS	Fault Detection
Timing (Distributed)	Distribution	QS	Synchronization
Event Analysis	Distribution	QC	Root Cause Analysis
Optimization in Operations (Voltage, Frequency, P, Q, Thermal Limits)	Distribution	QC	Operations & Safety
Customer Load: Quantum Computation via quantum annealing might be able to better model and assets downstream power distribution	Distribution	QC	Forecasting
Security in Substations	Transmission	QKD	All Coms
Grid Security	Transmission	QKD	All Coms

Communication With Timing and Event Detection?	Transmission	QE	Detection
Detect Tiny Perturbations	Transmission	QS	Real-Time Monitoring
Timing (Distributed)	Transmission	QS	Synchronization
EM Detection (Fault Detection)	Transmission	QS	Fault Detection
Contingency Analysis (Operations)	Transmission	QC	Resilience
Transmission Expansion (Planning)	Transmission	QC	Planning
Distribution: Breakthroughs in room-temperature superconducting materials via quantum simulation/ quantum computing might pave the way for materials that do not have any energy loss when transmitting and distributing energy (about 5-10% of the energy generated in loss in this stage)	Transmission	QC	Chemistry
Grid Security	Generation	QKD	All Coms
Communication With Timing and Event Detection?	Generation	QE	Detection
Timing (Distributed)	Generation	QS	Synchronization
Alternate Energy (Distributed)	Generation	QS	Load Monitoring
Event Assessment	Generation	QC	Root Cause Analysis
Generation: Quantum Simulation Via Quantum Computing promises better catalyst for nitrogen fixation (lowering power usage) and more efficient combustion reactions	Generation	QC	Chemistry
Asset Identification and Authentication	Aggregator / Service Provider	PQC	Asset Level
QE To Facilitate Hybrid Solutions for Forecasting	Aggregator / Service Provider	QE	Forecasting
Connection to / With Future Awarded EDA Tech Hubs	Aggregator / Service Provider	QE	Research
QS Targeted at Real-Time Monitoring	Aggregator / Service Provider	QS	Real-Time Monitoring
Increased Situational Awareness Around Cybersecurity and Cascading Events with Compounding Impacts	Aggregator / Service Provider	QS	Cascade Monitoring
QC Supported Algorithms for Better Forecasting	Aggregator / Service Provider	QC	Forecasting

Securing Distribution Networks Using PQC	Distribution	PQC	Distribution Level
PQC for Securing Distribution	Distribution	PQC	Distribution Level
for Securing Distribution	Distribution	QRNG	Distribution Security Entropy
QKD for Secured Communication in Microgrids, Networked Microgrids and Distribution Grids	Distribution	QKD	Microgrid Coms
Electrometry or Magnetometry for Phasing Multiple Generators	Distribution	QE	Synchronization
How to Draw Lessons Learned from Prior Energy Grid Failures, Such as Texas.	Distribution	QS	Root Cause Analysis
Manage Energy Supply System	Distribution	QS	Real-Time Monitoring
Quantum Optimization for Security-Constrained Optimal Operation	Distribution	QC	Operations & Safety
Optimal Energy Distribution for Lowest Energy Loss	Distribution	QC	Operations & Safety
Real-Time Monitoring Along With Forecasting with Optimal Solutions	Aggregator / Service Provider	QC	Forecasting
Energy Distribution Efficiency, Monitoring, and Control	Distribution	QC	Operations & Safety
Monitoring and Using That Data for Efficient Solution Optimization	Distribution	QC	Operations & Safety
Energy Supply Chain Protection Access Distributed Grid	Transmission	PQC	Distribution Level
QS for Monitoring Power Flow	Transmission	QS	Real-Time Monitoring
Standoff Detection of Transmission Wire Performance or Degradation	Transmission	QS	Anomaly Detection
Quantum AI for Stability Assessment and Real-Time Control	Transmission	QC	Operations & Safety
NISQ Algorithms for Ultra-Scalable Power Grid Analytics, i.e., Power Flow, State Estimation, Transient Simulation	Transmission	QC	Operations & Safety
PQC Algorithms to Keep Energy Generators Safe From Attack	Generation	PQC	Asset Level
QS to Monitor Reactants In-Situ	Generation	QS	Reactor Monitoring
Optimized Electrical Line and Generation Locations	Generation	QC	Planning
Design Of More Efficient Reactors (Fuel to Electrical Generation)	Generation	QC	Planning
Optimized Energy Grid & Scalability	Generation	QC	Planning
Security Weakness at the OT/IT Seam. andthe Use of Q Resilience Solutions	Customer Load / Energy Asset Owner	PQC	OT/IT

Security Weakness at the OT/IT Seam. andthe Use of Q Resilience Solutions	Customer Load / Energy Asset Owner	QKD	OT/IT
	Customer load / energy asset owner	QKD	Scada Coms
Operational Technology (SCADA Etc.) as Well as IT Connections	Customer Load / Energy Asset Owner	QKD	Scada Coms
Prediction of Load Balance, and Power Distribution in Rapidly Fluctuating Power Demands	Customer Load / Energy Asset Owner	QC	Load Balancing
Forecasting Demand Through Quantum Optimization	Aggregator / Service Provider	QC	Forecasting
Distributed Energy Resources Placement Optimization	Aggregator / Service Provider	QC	Planning
Communication Security Across the Smart Grids	Distribution	QE	Synchronization
Real-Time Combinatorial Optimization of Energy Distribution Over the Grid (Day-to-Day Ops)	Distribution	QS	Real-Time Monitoring
Grid Resilience Optimization: Optimize the Operation Change During High-Impact & Low-Frequency Events	Distribution	QC	Operations & Safety
Better energy materials using quantum computing simulations for chemistry (transformers, materials in smart grids)	Distribution	QC	Chemistry
Better Energy Storage Material	Distribution	QC	Chemistry
Forecasting loads as no visibility behind the meter (no visibility into give / get from DER distribution energy resources)	Distribution	QC	Forecasting
EM Leakage Detections, Gas Leakage Detection in Transformers	Transmission	QS	Anomaly Detection
QRNG-Assisted Monte Carlo to Assist Finite Element Modelling for, e.g., Fusion Research	Generation	QRNG	Simulation Entropy
Resource Identifications Such as Oil and Gas Deposit in the Deep Subsurface of Earth	Generation	QC	Image Analysis
Better Material Discovery for Plant Construction	Generation	QC	Chemistry
Aerodynamic Modelling for Turbine Blade Design	Generation	QC	Computational Fluid Dynamics
Search of Critical Minerals Such as Rare Earth Elements	Generation	QC	Image Analysis

Weather Forecasting Linked to Energy Resource Usage Prediction (Solar / Wind)	Generation	QC	Forecasting
Analyze Existing Surface Deposit Data Using Quantum Machine Learning	Generation	QC	Image Analysis
Analysis and PQC Standards for Integrated Microgrids	Customer Load / Energy Asset Owner	PQC	Microgrids
QML for Enhanced Anomaly Detection and Monitoring in OT/ IT	Aggregator / Service Provider	QC	Anomaly Detection
Energy Anomaly Pattern Recognition / Clustering / Root Causing / Prediction	QC	QC	Detection
Highly Secure Response Plans in Case of Network Intrusions	Distribution	QKD	Attack Alert
Quantum Clock / system synchronization for sub-nanosecond resolution. Towards GPS-Iindependent applications.	Distribution	QS	Replace GPS Synchronization
Anomalous Voltage Differential Sensing	Transmission	QS	Anomaly Detection
Performance Sensors for Critical Infrastructure	Transmission	QE	Alerting
QRNG for Generation / Operation Simulation	Generation	QRNG	Simulation Entropy
QKD for Securing EV Communicating With the Server & the Network of EVs & Charging Stations	Customer Load / Energy Asset Owner	QKD	EV Coms
Efficient CO_2 Capture Materials (Direct Air or Point Source)	Aggregator / Service Provider	QC	Chemistry
Efficient Battery Materials for Grid-Scale Storage	Aggregator / Service Provider	QC	Chemistry
Optimum Energy Trading Strategies	Aggregator / Service Provider	QC	Trading
Crew Dispatch, Vehicle Dispatch, Logistic Optimization	Distribution	QE	Alerting
Service Restoration by Operating the Switches to Reduce the Outage Duration	Distribution	QE	Recovery
Optimize Power Flow by Dispatching Controllable Resources to Improve Energy Efficiency	Distribution	QE	Alerting
Accurate Clock Sync Without GPS Reliance	Distribution	QS	Replace GPS Synchronization

Improve Synchronization Among Heterogeneous Data Sources	Distribution	QC	Synchronization
QC Optimization for EV Charging Via Connected Charging Stations and Microgrids (or Distributed Standalone Renewable Sources)	Distribution	QC	Charging
Q-Algorithms for Contingency Analysis Related to Power System Assessment & Location Allocation & Power System Control	Distribution	QC	Operations & Safety
Energy Management	Customer Load / Energy Asset Owner	QC	Forecasting
Defense in Depth Architecture With PQC/QKD	Aggregator / Service Provider	PQC	Defense in Depth
Integrating Secure Infrastructure With Third Parties Is a Problem If They Are Not Also PQC Compliant	Aggregator / Service Provider	QRNG	Third Party Security Entropy
PKI for OT Systems With Post Quantum Crypto	Distribution	PQC	OT/IT
Power Flow - Ensuring Physical Feasibility of Network Flows	Distribution	QC	Operations & Safety
Security-Constrained optimal power flow (power flow but considering economics and security) hybrid solution using QC	Transmission	QC	Operations & Safety
Contingency Analysis (N-M Security)	Transmission	QC	Resilience
(Physical) Security Constrained Unit Commitment (Unit Scheduling and Dispatch) at Device Level	Generation	QC	Operations & Safety
Information Transmission Protection	Customer Load / Energy Asset Owner	QKD	All Coms
Security Solutions to Protect Personal Data Domain	Customer Load / Energy Asset Owner	QKD	Information Level
Secure Communications	Customer Load / Energy Asset Owner	QKD	All Coms
QS & QE for Anomaly Detection for Resilience and Security	Customer Load / Energy Asset Owner	QE	Detection
QS for PNT to Securely Track EVs as Assets or Load	Customer Load / Energy Asset Owner	QS	Load Monitoring

QS for Secure Timing Free of GPS	Customer Load / Energy Asset Owner	QS	Replace GPS Synchronization
Annealing to Optimize Location of Grid Assets	Customer Load / Energy Asset Owner	QC	Planning
Optimization for Grid Improvement	Customer Load / Energy Asset Owner	QC	Planning
Chemistry Simulations to Improve EVs	Customer Load / Energy Asset Owner	QC	Chemistry
QC for Forecasting (Weather / Market Participation)	Customer Load / Energy Asset Owner	QC	Forecasting
Providing Encrypted Computation (i.e., FHE on Quantum) Over the QN	Aggregator / Service Provider	PQC	Information Level
Information Transmission Protection	Aggregator / Service Provider	PQC	Information Level
Secure Communications create cryptographic keys, limiting decryption, interception, and falsification. This protects against attacks by using QKD exchange. Can PQC algorithms be protected reducing eavesdropping and exfil attempts? QC can increase secure protocols. Consideration for key synchronization / re-sync (or randomization) must be defined for resilient systems and security confirmation. Quantum solutions must solve today's challenges without simply creating more of the same	Aggregator / Service Provider	QKD	All Coms
QS for Secure Timing Free of GPS	Aggregator / Service Provider	QS	Replace GPS Synchronization
QS for PNT to Securely Track EVs as Assets or Load	Aggregator / Service Provider	QS	Load Monitoring
QS & QE for Anomaly Detection for Resilience and Security	Aggregator / Service Provider	QE	Detection
Annealing to Optimize Location of Grid Assets	Aggregator / Service Provider	QC	Planning

Optimization for Forecasting and Monitoring	Aggregator / Service Provider	QC	Forecasting
QC for Forecasting (Weather / Market Participation)	Aggregator / Service Provider	QC	Forecasting
Enhanced Monitoring Freq and Do Better Control	Aggregator / Service Provider	QE	Monitoring
E&M Sensors	Aggregator / Service Provider	QS	Fault Detection
Information Transmission Protection	Distribution	PQC	Information Level
Provide More Inherent Security for Information in Transit.	Distribution	PQC	Information Level
QS & QE for Anomaly Detection for Resilience and Security	Distribution	QE	Detection
QS for Secure Timing Free of GPS	Distribution	QS	Replace GPS Synchronization
QS for PNT to Securely Track EVs as Assets or Load	Distribution	QS	Load Monitoring
QC for Contingency Analysis	Distribution	QC	Resilience
QC for Forecasting (Weather/Market Participation)	Distribution	QC	Forecasting
Information Transmission Protection	Transmission	PQC	Information Level
Improve Timing and Accuracy Over Greater Distance Providing More Resilient Known State(s)	Transmission	QE	Detection
QS & QE for Anomaly Detection for Resilience and Security	Transmission	QE	Detection
QS for Secure Timing Free of GPS	Transmission	QS	Replace GPS Synchronization
QS for PNT to Securely Track EVs as Assets or Load	Transmission	QS	Load Monitoring
E&M Sensors	Transmission	QS	Fault Detection
Threat Detection / Directed Energy Detection (Energy, Radio, etc.) Physical, Cyber Actions	Transmission	QS	Attack Vectors
Modeling Matching Actual Load to Predictively Adjust Gen and Trans	Transmission	QS	Real-Time Monitoring
Security Constrained Optimal Power Flow	Transmission	QC	Operations & Safety
QC for Contingency Analysis	Transmission	QC	Resilience
HTS Cables Designed by Quantum Computers	Transmission	QC	Chemistry
QC for Forecasting (Weather / Market Participation)	Transmission	QC	Forecasting
QS & QN Enhanced Security Constrained Unit Commitment	Generation	QC	Operations & Safety
Information Transmission Protection	Generation	PQC	Information Level

Quantum Thermodynamics (?)	Generation	QE	Monitoring
QS & QE for Anomaly Detection for Resilience and Security	Generation	QE	Detection
QS for Secure Timing Free of GPS	Generation	QS	Replace GPS Synchronization
Quantum Gravimeters for Oil, Coal Deposit Identification	Generation	QS	Fuel Deposit Discovery
QC for Contingency Analysis	Generation	QC	Resilience
QC for Forecasting (Weather / Market Participation)	Generation	QC	Forecasting
Quantum Simulations for Better Materials	Generation	QC	Chemistry
Annealing to Optimize Location of Grid Assets	Generation	QC	Planning
PQC to Protect Device Communications with the Grid	Customer Load / Energy Asset Owner	PQC	Asset Level
QRNG and QKD for Securing Grid and Distributed Energy Resource (DER) Communications	Customer Load / Energy Asset Owner	QKD	DER Coms
QS/QE for anomaly detection and timing to secure and synchronize the grid and distributed energy resources (e.g., solar, storage, electric vehicles)	Customer Load / Energy Asset Owner	QE	Synchronization
PQC to Protect Device Communications with the Grid	Aggregator / Service Provider	PQC	Asset Level
QRNG and QKD for Securing Grid and Distributed Energy Resource (DER) Communications	Aggregator / Service Provider	QKD	DER Coms
QS/QE for anomaly detection and timing to secure and synchronize the grid and distributed energy resources (e.g., solar, storage, electric vehicles)	Aggregator / Service Provider	QE	Synchronization
PQC to Protect Device Communications with the Grid	Distribution	PQC	Asset Level
QRNG and QKD for Securing Grid and Distributed Energy Resource (DER) Communications	Distribution	QKD	DER Coms
QS/QE for anomaly detection and timing to secure and synchronize the grid and distributed energy resources (e.g., solar, storage, electric vehicles)	Distribution	QE	Synchronization
PQC to Protect Device Communications with the Grid	Transmission	PQC	Asset Level
QRNG and QKD for Securing Grid and Distributed Energy Resource (DER) Communications	Transmission	QKD	DER Coms
QS/QE for anomaly detection and timing to secure and synchronize the grid and distributed energy resources (e.g., solar, storage, electric vehicles)	Transmission	QE	Synchronization

PQC to Protect Device Communications with the Grid	Generation	PQC	Asset Level
QRNG and QKD for Securing Grid and Distributed Energy Resource (DER) Communications	Generation	QKD	DER Coms
QS/QE for anomaly detection and timing to secure and synchronize the grid and distributed energy resources (e.g., solar, storage, electric vehicles)	Generation	QE	Synchronization
QC for Load Monitoring and Prediction for Distributed Generation/DER	Aggregator / Service Provider	QC	Planning
QC for Climate Modeling / Forecasting	Aggregator / Service Provider	QC	Forecasting
QC for Optimizing Distributed Energy Resources	Aggregator / Service Provider	QC	Planning
QC for Contingency Analysis	Aggregator / Service Provider	QC	Resilience
Quantum Computing for Forecasting	Aggregator / Service Provider	QC	Forecasting
QKD for Securing Microgrids	Distribution	QKD	Microgrid Coms
Light Weight Quantum Security Solutions for Distribution Grids	Distribution	QKD	Microgrid Coms
Using Quantum Sensors to Detect Problems Before They Cascade into Larger Problems	Distribution	QE	Detection
QC for Contingency Analysis	Distribution	QC	Resilience
QC for Optimizing Distributed Energy Resources	Distribution	QC	Planning
QS for Remote Imaging to Detect Wildfires	Transmission	QS	Disaster Detection
QC for Contingency Analysis	Transmission	QC	Planning
QC for Optimizing Distributed Energy Resources	Transmission	QC	Resilience
QC for Climate Modeling / Forecasting	Transmission	QC	Forecasting
QS for Remote Imaging to Detect Wildfires	Distribution	QS	Disaster Detection
Quantum Keys for Authentication of Distributed Energy Resource (PV, Wind, etc.) Data and Controls	Distribution	QRNG	Distributed Resource Security Entropy
Quantum Computing for Better Materials Strength, High-T Operation and Batteries	QC	Chemistry	
Quantum Sensor Network to Sense Nuclear Reactor	Generation	QE	Monitoring
QS to Secure Nuclear	Generation	QS	Reactor Monitoring

QC for Contingency Analysis	Generation	QC	Resilience
QC for Optimizing Distributed Energy Resources	Generation	QC	Planning
QC for Climate Modeling / Forecasting	Generation	QC	Forecasting
Microgrid Cybersecurity	Customer Load / Energy Asset Owner	QKD	Microgrid Coms
Behind the Meter Data Sensing: Privacy and Security	Customer Load / Energy Asset Owner	QE	Asset Level
Utilization Analysis and Optimization	Customer Load / Energy Asset Owner	QS	Load Monitoring
Decarbonization - Monitoring Energy Efficiency	Customer Load / Energy Asset Owner	QS	Efficiency Monitoring
Usage & Optimization	Customer Load / Energy Asset Owner	QS	Load Monitoring
Asset Usage Optimization	Customer Load / Energy Asset Owner	QC	Planning
Load Balancing Systems	Customer Load / Energy Asset Owner	QC	Load Balancing
Planning (Budgets, Resources, Contacts)	Customer Load / Energy Asset Owner	QC	Planning
Capital Investment Optimization	Customer Load / Energy Asset Owner	QC	Planning
Pricing Strategies	Customer Load / Energy Asset Owner	QC	Forecasting
Secure Phasor Measurement Unit Data Transmission Through WAMS	Aggregator / Service Provider	QS	Phase Monitoring
Modeling & Forecasting	Aggregator / Service Provider	QC	Forecasting

Better Weather Forecasting for Solar Panels	Aggregator / Service Provider	QC	Forecasting
Secure Communication	Distribution	QKD	All Coms
True RNG for Better Simulation for Planning	Distribution	QRNG	Simulation Entropy
Simulation	Distribution	QC	Planning
System Restoration and Optimal Grid-Forming	Distribution	QC	Operations & Safety
Secure Communication Among Facilities	Transmission	QKD	All Coms
Fast DC Fault Detection: Key for Offshore Wind Integration	Transmission	QS	Fault Detection
Monitoring Losses	Transmission	QS	Load Monitoring
Secure Phasor Measurement Unit Data Transmission Through WAMS	Transmission	QS	Anomaly Detection
Dynamic Simulation for Dynamic Security Assessment	Transmission	QC	Attack Discovery
EMT Simulation for LBRs (Both GFMs and GFLs)	Transmission	QC	Asset Simulation
Security Constrained Unit Commitment	Transmission	QC	Operations & Safety
PMU Data	Transmission	QE	Phase Monitoring
Secure Information About Resource Deposits	Generation	PQC	Information Level
PMU Data from Generating Stations	Generation	QS	Phase Monitoring
Safety in Generation (Nuclear, Hydro, etc.)	Generation	QS	Reactor Monitoring
Sensing for Discovery of Resource Deposits	Generation	QS	Fuel Deposit Discovery
QC for Better Material Discovery for Solar Panels	Generation	QC	Chemistry
Fluid Dynamics	Generation	QC	Computational Fluid Dynamics
Secure Connections in SCADA	Customer Load / Energy Asset Owner	QKD	Scada Coms
Determination of Process Sequence and Patrol Routes for Workers	Customer Load / Energy Asset Owner	QC	Workforce
PQC Proxy - Some SCADA / IOT May Not Support PQC	Aggregator / Service Provider	PQC	Encapsulation
QKD as a Service - Distribute Keys Beyond QKD Node Locations	Aggregator / Service Provider	QKD	QKD as a Service
Improved Single Photon Detectors	Aggregator / Service Provider	QE	Detection

Grid Resilience Optimization	Distribution	QC	Resilience
Load Forecasting	Distribution	QC	Forecasting
Load Forecasting	Transmission	QC	Forecasting
UCP (Unit Commitment Problem) Optimization	Generation	QC	Operations & Safety
Need feedback from everywhere to provide good information to a virtual powerplant-- need to secure this communication	Customer Load / Energy Asset Owner	QKD	VPP Coms
Optimization From a Marketplace Standpoint	Customer Load / Energy Asset Owner	QC	Trading
Optimization From a Marketplace Standpoint	Aggregator / Service Provider	QC	Trading
QKD for Cybersecure Communication Virtual Power Plant to Provide Grid Services	Aggregator / Service Provider	QKD	VPP Coms
Virtual Powerplant - Combine Solar, Wind, etc., to Have a Scalable Service for Power Generation	Aggregator / Service Provider	QKD	VPP Coms
OPF (Optimization of Power Flow) With DER (Distributed Energy Resources) and Electric Vehicles	Aggregator / Service Provider	QC	Planning
Quantum Machine Learning -- Forecasting, Anomaly Detection	Aggregator / Service Provider	QC	Forecasting
Anomaly Identification with Models - Intentional & Unintentional	Aggregator / Service Provider	QC	Detection
IOT Devices Protected With PQC Keys	Distribution	PQC	Asset Level
IOT Devices Protected With QRNG Entropy	Distribution	QRNG	Iota Security Entropy
Key Management for Distributed Devices	Distribution	QKD	Distribution Coms
QKD for Better Key Mgmt. on Devices That Are on Premises That You Don't Control	Distribution	QKD	Third Party Site Control Coms
Fault Location and Identification (FLISR) - Q-Sensors Discovery More Data and That Data Is Then Q-Computed in Model	Distribution	QS	Fault Detection
Stability of Low Inertia Power Grids	Transmission	QE	Stability Monitoring
Improved accuracy and security of time synchronization - GPS accuracy - want to help with synchronization between power grids – i.e., better sync'd time	Transmission	QE	Synchronization

Cyber-attack discovery - modeling is hard - want to know where different systems can interact and what attack vectors there are	Transmission	QC	Attack Discovery
Optimization of network reconfiguration - many need to reconfigure grid when disturbances happen. Want to do quickly when grid online	Transmission	QC	Operations & Safety
Transmission Cables With High Strength That Can Transmit More Power - Material Discovery for Convection Cables	Transmission	QC	Chemistry
Material Discovery for Batteries - Battery Modeling, Batteries Help Maintain Inertia in a System	Transmission	QC	Chemistry
Grid (Circuit) Modeling Inverse, Multi-Modal Modeling HHL Modeling	Transmission	QC	Planning
Accurate Sensing for Natural Energy for Increase Efficiency - Optimized Natural Energy Generation With Q-Sensors	Generation	QS	Load Monitoring
Quantum Optimization - Supply Chain - Market Space Is Large	Generation	QC	Supply Chain Optimization
Securing Communication Between Generation, Storage, and Flexible Demand	Customer Load / Energy Asset Owner	QKD	Scada Coms
Optimization problems like load rebalancing and public safety advice during non-routine mass migration of EVs Such as unexpected natural disasters	Customer Load / Energy Asset Owner	QE	Load Balancing
Understanding New or Changing Assets on the Grid	Customer Load / Energy Asset Owner	QS	Load Monitoring
Security of Transitive Energy From Dispatchable Demand (Securing the Transactions)	Aggregator / Service Provider	PQC	Information Level
Security of the Transaction Ledger	Aggregator / Service Provider	PQC	Information Level
Multi-Party Authentication for Providing Grid Services	Aggregator / Service Provider	QKD	All Coms
Securing Networked Microgrids	Aggregator / Service Provider	QKD	Microgrid Coms
Sensing Solutions for Detecting Transients That Impact Protection and Controls in Ibis	Aggregator / Service Provider	QS	Anomaly Detection

Security of the ICS Sensors to Monitor Energy Assets and Resources	Distribution	QC	Operations & Safety
DERMS Authentication at Distribution Scale of Multiple Plants	Distribution	QKD	DER Coms
Timing Solutions for Distribution	Distribution	QE	Load Balancing
EM Detection for Fault Prediction in Transformers and Other Equipment	Distribution	QS	Fault Detection
PQC Standards That Are More Performant for OT Assets (Benchmarking Performance vs Security, e.g., Key Lengths)	PQC	OT/IT	
Transmission	PQC	OT/IT	OT/IT
Cybersecurity of OT Assets, specifically for Systems That Are Currently Under-Secured Because of the "Cost" Of Encryption in Timing of the Signal	Transmission	PQC	OT/IT
Securing Internal Control Center Communications for Operational Security	Transmission	QKD	Control Coms
Secure Clock for Wide-Area Synchronized Measurements	Transmission	QS	Synchronization
Securing Network Communications Between the Plant and the Power Grid	Generation	PQC	Core Infrastructure Level
Securing Spot Market Interactions	Generation	QKD	Market
Atomic Clocks for More Resilient Comms That Do Not Rely on GPS, in Particular for More Remote Generation Sites	Generation	QS	Replace GPS Synchronization
Gas Sensing	Generation	QS	Fuel Deposit Discovery
Optimize Wholesale Energy Trading	Generation	QC	Trading
Unit Commitment and Dispatch Optimization Problems, Particularly With Stochastic Security Constraints	Generation	QC	Operations & Safety


QED-C