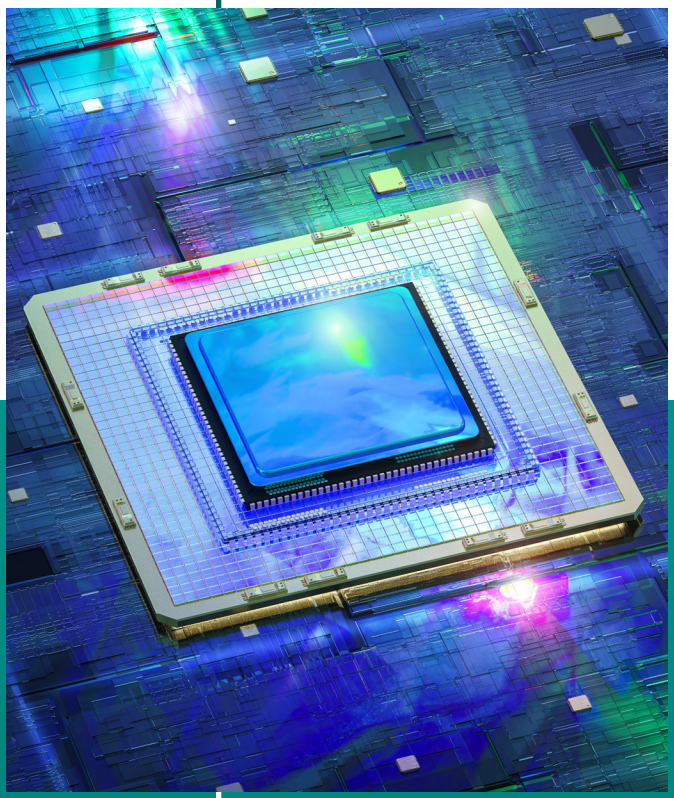

An EPRI White Paper

QUANTUM CHALLENGE RESULTS: QUANTUM TECHNOLOGIES FOR AI-ENHANCED UTILITY CYBERSECURITY

TABLE OF CONTENTS

INTRODUCTION

Quantum science and technology (quantum) has the potential to solve a wide range of existing challenges in the energy industry today. For this reason, EPRI led a quantum challenge in 2022 focusing on how quantum technologies can benefit the energy industry relative to cybersecurity challenges. The goal of the challenge was to identify opportunities for the energy industry to accelerate the adoption of quantum while leveraging artificial intelligence for improved utility cybersecurity. The primary goal of the challenge was to inspire and educate individuals, generate new enthusiasm and investment, and foster collaboration between the energy industry, quantum-focused companies, universities, national laboratories, the U.S. Department of Energy, and others.

CYBERSECURITY APPLICATIONS

Increasingly sophisticated cyber actors target critical energy infrastructure, including physical and virtual assets of the bulk-power system through malware, denial-of-service attacks, phishing, and more.[1] The frequency and potential severity of these attacks have been increasing in recent years.[2] Securing energy systems against cyber threats is a critical priority for electric utilities and the public. Utilities are increasingly dependent on information technology and telecommunications infrastructure to enable the reliability and security of the electric grid. Quantum cybersecurity, including tools such as cryptography, encryption, and artificial intelligence (AI), may offer more robust and compelling opportunities to safeguard critical and personal data than traditional security methods.

AI is particularly compatible with quantum computing (QC) and cybersecurity because AI enables machines to learn and self-evolve, allowing quantum computers to recognize data patterns, detect cyber threats, and develop self-learning algorithms that will enhance cybersecurity. AI—based on a mathematics, statistics, cognitive science, philosophy, and linguistics—is the science and engineering of making intelligent machines.[3] AI can imitate human intelligence in areas such as mathematical computation and forecasting, image recognition, and more recently understanding and generating human language. In recent years, advances in the energy sector have made AI solutions a desirable paradigm for solving data-driven problems that can be automated.

1 Idaho National Laboratory. "Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector." August 2016.
2 *Cyber Security Vision for 2030*. EPRI, Palo Alto, CA: 2021. 3002022715.
3 *An Introduction to AI, Its Use Cases, and Requirements for the Electric Power Industry*. EPRI, Palo Alto, CA: 2019. 3002017143.

Advancements in AI have led to new defensive cybersecurity solutions superior to traditional cybersecurity solutions.[4] For example, information technology (IT) operations have integrated AI-based cybersecurity operations, enabling utilities to detect attempted cyberattacks at high detection rates with few false positives. There are claims that AI solutions provide improved cyber security risk reductions compared to traditional solutions, and more work should be performed to independently validate such claims.[5]

Cryptography is also an important component of critical infrastructure cybersecurity as it is used to secure all kinds of data, including data stored on servers as well as data in transit through authentication techniques.[6] The simultaneous requirements of strong and fast authentication mechanisms are difficult to achieve through standard encryption. The increased computational power of QC can address complex operational and data-intensive challenges related to cybersecurity. Quantum key distribution and quantum cryptography utilize the properties of quantum mechanical systems to secure digital communications systems, for example the transmission of data between control centers.

EPRI has developed a Cyber Security Roadmap for 2030² in collaboration with utilities and industry stakeholders. This action plan to transition cybersecurity into an essential embedded design of utility operations identifies the critical future states for cybersecurity. EPRI will continue to analyze cyber threats to the critical infrastructure on which we all depend and monitor developing trends in quantum for cybersecurity use cases.

QUANTUM CHALLENGE OVERVIEW

EPRI initiated an innovation challenge to identify opportunities for the energy industry to potentially accelerate adoption of new quantum technologies to augment artificial intelligence and cybersecurity. Participants submitted written proposals around the goal of discovering plausible use cases for quantum technology for enhanced utility cybersecurity. The primary goal of the challenge was to inspire and educate individuals, generate new enthusiasm, investments, and ideas to the field and increase the connection between individuals and organizations around the world. Therefore, the challenge was open to utilities, startups, energy and/or quantum technology subject matter experts, colleges and universities, and individuals worldwide.

A panel of industry experts (known as Challenge Advisors) reviewed each proposal received by the EPRI team. The Challenge Advisor panel included individuals affiliated with Oak Ridge National Laboratory, Brookhaven National Laboratory, the U.S. Department of Energy Office of Technology Transitions, Qubits Ventures, University of Waterloo, Techstars, and EPRI. All proposals were reviewed in a blind fashion to avoid biasing the results in any way. This was done by removing all personally identifiable information (PII) and company name or product information so that reviewers did not know which people or organizations they were reviewing. Challenge Advisors graded proposals on a scale based on value, creativity, technical readiness, and relevance as defined below.

- **Value** – encompasses the solution's ability to address a problem/need for the energy industry, the potential impact/scalability of the solution, and its competitiveness with the incumbent technologies or alternative solutions as well as cost savings or value generation.
- **Creativity** – represents a novel or disruptive change to the current state of the art and is fundamentally different from existing solutions.
- **Technical readiness** – the rate of the technical feasibility and maturity and the proposed case's readiness for integration. Factors for consideration include third-party testing/validation, compliance with industry standards/safety certifications, or proof of market traction.
- **Relevance** – evaluates the proposed concept's incorporation of all three components of the prompt: 1) artificial intelligence, 2) quantum technology, and 3) cybersecurity.

Challenge Advisors selected the top three proposals based on the evaluation criteria listed above. The three winning proposals were awarded a monetary prize.

- First-place team was awarded $10,000.
- Second-place team was awarded $7,500.
- Third-place team was awarded $5,000.

4 *Artificial Intelligence for Cybersecurity: Use Cases*. EPRI, Palo Alto, CA: 2022. 3002024831

5 Darktrace Cyber AI. "Enterprise Immune System: Product Brief."

6 IBM Corporation. "Security in the Quantum Computing Era," Arnmonk, NY, 2022. https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/quantum-safe-encryption.

QUANTUM CHALLENGE PROPOSAL WINNERS

A number of groups submitted proposals across a range of topic areas related to quantum-enhanced cybersecurity for energy applications. The award process was competitive with numerous creative and valuable submissions. The following section provides a summary of the winning proposals.

First Place: DC Power Flow Contingency Analysis with NISQ-Era Hybrid Quantum Algorithms, Infleqtion

The U.S. electric grid currently powers nearly 130 million households, making it essential that its operation is not interrupted, whether by environmental factors, cybersecurity threats, or other issues. Grid size and load are expected to increase as we electrify various industries and rapidly integrate smaller, cleaner energy sources in an effort to decarbonize the grid, making the efficient computation of grid security protocols key. One of these protocols is contingency analysis, which studies the effect of outages in some power system elements on the rest of the grid. In Infleqtion's proposal titled "DC Power Flow Contingency Analysis with NISQ-era Hybrid Quantum Algorithms," the team presents a path towards a quantum advantage in utilities security through a hybrid quantum-classical algorithm for performing power system contingency analysis.

The core of the quantum advantage lies in a Hybrid Multiple Phase Estimation Algorithm (HMPEA), which can be applied to solve a linearized model of power flow in an energy grid. The HHL (Harrow, Hassidim, Lloyd) quantum algorithm, which can lead to exponential speedups for solving linear equations, fails to perform well on current hardware due to its imperfect phase estimation module, which suffers due to limited qubit resources. HMPEA concatenates phase estimation modules in such a way that it effectively multiplies the qubit count by the number of modules without increasing hardware requirements. This allows for a higher precision phase estimation without the need to improve hardware, while still maintaining the exponential computational speed up that HHL provides.

Infleqtion proposed installing forthcoming large-scale quantum computers at various junctions in the power grid to allow for periodic quantum computation of contingency analysis via HMPEA. This is an ambitious goal with several hurdles along the way. First, it must be experimentally demonstrated that HMPEA provides significant gains over classical techniques via quantum simulations and operating on actual quantum hardware. Once it has established that HMPEA would be an advantageous approach, the distribution of quantum resources across the grid or using cloud-based QC would need to be evaluated to maximize the reliability of contingency analysis, as well as balance financial considerations. Despite these challenges, quantum technology presents a unique opportunity to truly modernize the grid, and evaluating its costs vs. benefits should be considered.

Second Place: Atomic Clock Enhanced Grid Security, Infleqtion

Infleqtion (formerly ColdQuanta) endeavored to enhance the security of power grids. Modern power grids are left vulnerable to cyber attacks due to their critical reliance on global positioning systems (GPS) for timekeeping. Accurate timekeeping itself is critical to the reliability of the power grid. Thus, Infleqtion proposes to leverage quantum technologies for timekeeping and synchronization that are more secure and precise than existing technologies.

The submission featured a four-phase approach to enhancing grid security. Distributed atomic clocks across the grid provide the foundation of the proposal, with subsequent phases incorporating enhancements in-line with expected technological developments, culminating in full-scale integration with quantum computers. The anticipated deployment timescales are informed by the technology roadmap from Infleqtion for clocks, quantum networks, and quantum computers.[7]

The same atomic clock technology propagated by GPS signals can be deployed directly on the grid through Chip-Scale Atomic Clocks (CSACs). These are commercially available today, however, at a relatively high cost. Thus, **Phase 1** proposed evaluating the installation of atomic clocks only at critical sites throughout the grid. **Phase 2** proposed ubiquitous deployment of next-generation atomic clocks, which the industry expects will achieve 100 nanosecond accuracy at a much lower cost. Such a deployment would unlock ultra-accurate timing applications, such as traveling wave fault detection and enhanced droop control, both of which enhance grid reliability and security.

7 Amico, Boshier, et.al. "Roadmap on Atomtronics: State of the art and Perspective," AVS Quantum September 2, 2021; 3(3): 039201. https://doi.org/10.1116/5.0026178.

Regardless of the accuracy of individual clocks, uncertainty remains due to synchronization *between* clocks. **Phase 3** proposes atomic clocks in the grid be connected by quantum networks to enable enhanced synchronization via entanglement. Quantum network integration would result in a grid that is completely resilient to GPS signal loss, while further enhancing positioning accuracy for greater security through precise geolocation of attacks and outages.

Finally, **Phase 4** pairs ultra-accurate atomic clocks with quantum computers deployed at the edge. Such an architecture would allow state estimation (of grid real-time operating conditions) to be performed at the edge, while breakthroughs in quantum sensing and machine learning could be leveraged to process quantum data from local sensors to extract grid features. Though both applications are speculative, they merit additional consideration given the potential of quantum computation and its associated technologies.

Third Place: Quantum Network Analytics, Mark McGuire (individual contributor)

Quantum computing is expected to be helpful in speeding up network analysis and deep learning, enabling better responses and predictions to attacks and outages. Although quantum computers are not big data machines, they can be powerful deep learning tools. A recent study showed that quantum AI could require only as many training examples as parameters, making it possible to train a quantum neural network even when there is not enough data to train a classical neural network.[8] Although this had not been implemented yet, this could allow for a model being created over datasets that are too sparse for today's AI models to utilize, lead the development towards single-shot learning, or speeding up training time for AI/machine learning models. Quantum network analysis could also be used to minimize affected areas in the event of an outage and determine if it was the result of environmental, accidental, or intentional/malicious activity.

The submission suggests using Qiskit, a QC framework, to create a facsimile of a section of the power grid using resistors and power supplies. The equations for power calculations are converted to a quadratic program for Qiskit. The objective function should minimize the power provided while providing sufficient yet not too much power to all relevant parts. Qiskit could then be used to load the functions onto a quantum computer and run it. The validity of results can be confirmed by comparing to the same facsimile solved classically.

While the quantum computer may not presently perform as precisely as a classical computer due to noise and low qubit count, a hybrid approach may be best until the technology develops further and addresses these issues. A classical computer can optimize on a smaller range using the solution provided by the quantum computer, thus finding a solution obscured by noise. This more efficient grid and expected faster responsiveness has implications in case a security incident cripples power production. Better allocation of production can allow for fewer stations to meet the demand, providing a greener, cheaper, and more resilient grid. The main goal of security is to protect a resource, and QC could be used to respond to attacks, working synergistically to lessen the likelihood and impact of attacks.

CONCLUSIONS AND FUTURE DIRECTION

Quantum science and technology (quantum) has the potential to offer significant benefits to the current and next-generation electric power systems. Quantum may provide viable and valuable solutions to energy industry challenges that cannot be easily or quickly solved by classical systems, including cybersecurity challenges. EPRI has evaluated QC cybersecurity use cases for the grid and beyond.[9] Novel methods for controlling and hardening the grid may be required to prevent cyber threats from undermining the electric power system. Quantum can be a tool to harden the grid against future cyber attacks.

The energy industry can significantly benefit from technology advancements in QC. However, broad adoption of these technologies remains to be seen. In general, the rapidly evolving quantum landscape has many technical hurdles to overcome, including cryogenic cooling requirements, and noise that may affect the accuracy of the calculations a quantum computer performs.[9] EPRI's research goal in the next several years will be to research the possible uses cases using quantum, keeping abreast of the rapid changes in the science and technology. EPRI aims to participate in evaluating and enhancing quantum's viability and potential impact across energy industry applications.

8 Caro, M. C., Huang, et.al. "Generalization in quantum machine learning from few training data." Nature Communications, 2022., 13(1). https://doi.org/10.1038/s41467-022-32550-3 [doi.org].

9 Quantum Computing: Technology Update Across the Energy Industry. EPRI, Palo Alto, CA: 2022. 3002025371.

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATION(S) BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCUMENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

REFERENCE HEREIN TO ANY SPECIFIC COMMERCIAL PRODUCT, PROCESS, OR SERVICE BY ITS TRADE NAME, TRADEMARK, MANUFACTURER, OR OTHERWISE, DOES NOT NECESSARILY CONSTITUTE OR IMPLY ITS ENDORSEMENT, RECOMMENDATION, OR FAVORING BY EPRI.

EPRI PREPARED THIS REPORT.

THE FOLLOWING ORGANIZATIONS, UNDER CONTRACT TO EPRI, PREPARED SECTIONS OF THIS REPORT:

PRANAV GOKHALE	INFLEQTION
ALASH GOIPORIA	INFLEQTION
MARK MCGUIRE	INDEPENDENT CONTRIBUTOR

About EPRI

Founded in 1972, EPRI is the world's preeminent independent, non-profit energy research and development organization, with offices around the world. EPRI's trusted experts collaborate with more than 450 companies in 45 countries, driving innovation to ensure the public has clean, safe, reliable, affordable, and equitable access to electricity across the globe. Together, we are shaping the future of energy.

CONTACT INFORMATION

For more information, contact the EPRI Customer Assistance Center at 800.313.3774 (askepri@epri.com).

EPRI RESOURCES

EPRI members interested in engaging in and supporting this effort should contact EPRI for further discussion.

Jeremy Renshaw, ***Technical Executive, Sr***
704.595.2501, jrenshaw@epri.com

Technology Innovation

Product ID 3002027693 July 2023

EPRI
3420 Hillview Avenue, Palo Alto, California 94304-1338 USA • 800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com