QUANTINUUM | Honeywell

CASE STUDY:

Smart Grids Face Smart Cyber Threats

Transitioning to efficient, reliable, and protected smart grids using Quantinuum's **Quantum Origin**

EXECUTIVE SUMMARY

- Case study for CIOs and CTOs on the transition to efficient and reliable smart grids
- Honeywell demonstrates support for customers Environment, Social, and Governance (ESG) strategies
- Smart grids introduce outsized risk of cyberthreat to critical infrastructure
- Honeywell deploys Quantinuum's Quantum Origin for smart grid protection

Introduction

Traditional, centralized energy systems are being replaced by distributed smart grids. A system of industrial-scale generation plants supplying energy to local consumers is now complimented by an increasing number of distributed producers, equipped with smart meters to exchange energy with a smart grid. For example, a solar-paneled roof or a fully charged electric vehicle may feed energy into the grid at peak times.

The proliferation of micro renewable energy sources will reduce excessive dependence on legacy fossil fuel generation. At a neighborhood level, wind turbines and solar panels will connect to novel forms of energy storage to reduce or eventually eradicate the reliance on centralized and highly polluting coal power stations.

Honeywell plays a crucial role in this transition and, consequently, supports the ESG goals of its customers. Honeywell Smart Energy & Thermal Solutions is one of the leading innovators supporting industrial automation across utilities as well as sectors that depend on thermal solutions. The need for practical and impactful sustainability underpins their technical solutions.

The foundation of this energy transition is the smart grid and its associated smart metering operational and data integrity infrastructure. Unlike the traditional grid, smart grids rely on a blend of operational technology (OT) and information technology (IT). The OT handles the movement of energy, while IT is used for operations and resiliency.

These changes introduce efficiency and reliability, but they also add vulnerability to the system. A cyber-attack on highly connected critical infrastructure can have a devastating impact, including widespread outages and even risk to human life.

One area of critical focus is the cryptographic systems that protect the smart meter networks. A weakness in this layer would allow devastating attacks to be released undetected into the smart grid, impacting critical infrastructure.

With nation-state level cyber-attackers deploying increasingly sophisticated tools - such as AI - Honeywell recognized they must do everything technically possible to strengthen the encryption keys and certificates that secure their smart meter products.

Hardening smart meters with Quantum Origin

As governments ramp up preparations for the arrival of powerful quantum computers, innovators like Honeywell are embracing quantum computing solutions to enhance cybersecurity.

Quantum Origin is an advanced quantum random number generator (QRNG) developed by Quantinuum. It generates random, patternless digital data, which is the raw ingredient used to create encryption keys. Powered by Quantinuum's world-leading quantum computers, Quantum Origin allows Honeywell to generate encryption keys that are proven to be unpredictable.

The scientific concepts behind Quantum Origin date back to the 1960s and recently led to the award of the Nobel Prize in physics. By combining this fundamental quantum science with a unique deployment methodology, Quantum Origin strengthens encryption systems, far exceeding the minimum bar required by industry standards.

The decision to harness Quantinuum's Quantum Origin product as a source of proven high-quality randomness reflects Honeywell's commitment as a leader in industrial automation technology to keeping critical infrastructure many steps ahead of potential threats. This move is not just about enhancing security; it's about ensuring reliability and future-proof trust in the systems that underpin modern infrastructure.

"Honeywell is committed to deploying best-in-class security to protect our customers' critical systems. Quantum Origin's quantum-enhanced random number generation is crucial input to our cryptographic strategy, helping us generate encryption keys far stronger than standard public key cryptography."

Matthew Bohne,
VP & Chief Product Security Officer at Honeywell

Why Honeywell chose Quantum Origin

ENHANCED PROTECTION

Quantum Origin provides the strongest foundation against encryption threats, enhancing operational and data security for Honeywell customers.

EASE OF INTEGRATION

Honeywell integrated Quantum Origin into its existing infrastructure, allowing for easy deployment at scale.

INNOVATIVE LEADERSHIP

By choosing Quantum Origin, Honeywell solidifies its position as a leader in industrial automation and secure energy solutions.

Securing the future of energy transition

To meet ambitious ESG goals, organizations need smart technology that keeps OT and IT systems secure.

The switch to distributed smart grids will enable a transformation of the energy ecosystem, making ESG goals more attainable. But this will only be successful if the technology can be deployed in a resilient and secure manner.

By using Quantum Origin, Honeywell is leading the way in smart grid security and guiding the industry on a path to a more sustainable and automated future.

QUANTINUUM
QUANTUM ORIGIN

Quantum Origin is the only software-deployed solution delivering provable quantum randomness.

Designed for flexibility across diverse environments, including IoT (Internet of Things), air-gapped systems, and high-security infrastructure.

Learn more about how Quantum Origin can strengthen your cybersecurity infrastructure by getting in touch with our team:
sales@quantinuum.com

quantinuum.com/products-solutions/quantum-origin