GAINING STEAM ON DIGITAL TRANSFORMATION

A Nuclear Power Company Builds One of the Industry’s Most Advanced Cybersecurity Suites

Case Study
One of the more conservative industries in the industrial world—nuclear energy—took a leap towards better protecting critical infrastructure when a major nuclear energy company partnered with Honeywell to upgrade the industrial controls systems (ICS) at its facilities with advanced cybersecurity goals in mind.

In the highly regulated nuclear industry, digital computers and communication networks have been operating for a long time with limited modifications due to strict regulatory requirements. While upgrading the ICS kept getting pushed further down the to-do list, sophisticated operational technology (OT) cybersecurity threats emerged. So, when the nuclear company decided it was time to modernize its systems, the team knew it would not be a small undertaking.

This power company had nuclear units commissioned decades ago, operating on the original digital systems. Honeywell experts were tasked with replacing over 20 different controls systems across three sites and addressing the 500 cybersecurity controls that needed to adhere to multiple regulations.
ASSURING CYBERSECURITY SUPPLY CHAIN INTEGRITY

The team established a secure development and operational environment (SDOE) at a Honeywell facility to help ensure that the new system would not get infected while being built by Honeywell’s industrial cybersecurity experts. Each member of the 70-strong project team was thoroughly trained in the SDOE processes and procedures to uphold the trustworthiness and integrity of the entire system for years of its design, development, validation and the eventual custody transfer to the customer site.

SHAPING THE FUTURE

The operational lifecycle of a control system is often 5-10 years, but many systems have been operating for over 30 years, particularly in the nuclear industry. To make sure the new system stays updated despite it not getting upgraded based on the recommended time frame, the Honeywell experts conducted the customer’s cybersecurity risk analysis and recommendations in a way that helps better protect against cyber threats today and in the future.

Honeywell’s cybersecurity team designed and implemented a one-of-a-kind OT cybersecurity structure to build a control system to help comply with Nuclear Regulatory Commission (NRC) regulations, address long-term lifecycle support, and better manage advanced cyber threats. The new system included multiple third-party components, which all had to pass through the rigorous NRC validation and verification processes.

The customer’s new, modern control system was built with advanced endpoint protection, PCN monitoring, configuration and included efficient change management.

RESULTING VALUE

This new modern system resulted in one of the most advanced systems - for this conservative industry - that was disbursed across multiple sites. This standardized system design was subsequently deployed to replace the numerous, different legacy systems. This project helped the power company address NRC rules, and achieve an NRC-approved platform while helping to maintain cybersecurity resilience into the future.