ARMEXA

Case Study:
Operator Advances Secure, Scalable Wireless Architecture Through IT/OT Use Case Alignment

A large industrial energy operator engaged Armexa to help define a future-ready wireless strategy capable of supporting reliability, predictive maintenance, mobility, and digital transformation initiatives while maintaining strict IT/OT separation. Through a facilitated wireless use case workshop and the development of a comprehensive high-level solution design, the organization gained a clear, structured roadmap for deploying multiple wireless technologies in a secure, fit-for-purpose manner aligned with operational requirements and cybersecurity best practices.

Industry: Energy / Liquefied Natural Gas

Environment: Large-scale industrial facility with complex IT and OT networks, existing wireless instrumentation, corporate wireless infrastructure, and distributed field operations supporting process control, maintenance, and reliability functions.

Armexa Services:

- Wireless Use Case Workshops
- Industrial Wireless Architecture & Design
- IT/OT Network Segmentation & Security Architecture
- ISA/IEC 62443 Zones and Conduits Development
- OT Cybersecurity Strategy & Roadmapping

Challenges

The organization was undertaking significant reliability and modernization initiatives that required expanded use of wireless technologies across its operational environment. Existing wireless systems had evolved organically over time, resulting in multiple platforms with overlapping capabilities, limited scalability, and inconsistent alignment with future use cases. Key challenges included a lack of documented current and future wireless requirements, uncertainty around appropriate technology selection for different operational needs, concerns about cybersecurity and IT/OT separation, and the risk of deploying wireless solutions that could negatively impact deterministic process control systems.

Our Solution

Armexa facilitated an in-person wireless use case workshop to collaboratively document existing, planned, and desired wireless applications across operations, maintenance, engineering, and IT stakeholders. The engagement focused on establishing clear security objectives, defining data consumers, and aligning wireless use cases with operational criticality. Insights from the workshop were used to develop a high-level wireless solution design that mapped each use case to the most appropriate wireless technology, incorporating ISA/IEC 62443 zones and conduits principles, defense-in-depth security controls, and explicit IT/OT segmentation. The resulting design provided a structured, technology-agnostic framework to guide future detailed engineering, pilots, and phased deployment.

Outcomes & Impact

The project delivered a clear and actionable wireless strategy that reduced uncertainty and risk associated with future wireless investments. The organization gained a consolidated view of wireless opportunities across reliability, safety, mobility, and analytics use cases, along with a defensible rationale for adopting a multi-technology approach. By defining security principles, zones, and data flows upfront, the solution positioned the operator to expand wireless capabilities without compromising process control integrity or cybersecurity posture. The engagement also established a common understanding among IT, OT, and business stakeholders, enabling more efficient decision-making and a scalable path toward modernization.

Why the Client Chose Armexa

For this engagement, the industrial operator selected Armexa because of its ability to bridge operational requirements, cybersecurity rigor, and practical industrial wireless design, without forcing premature technology decisions or compromising OT integrity.

- Operations-Aware Wireless Strategy (Not Vendor-Driven Design)
- Deep OT Cybersecurity and IT/OT Segmentation Expertise
- Proven Ability to Align IT, OT, and Business Stakeholders
- Technology-Agnostic, Scalable Architecture Approach
- Asset-Owner Mindset Grounded in Real Industrial Environments
- Clear, Actionable Deliverables That Reduced Risk

ARMEXA

Ready to talk all things cybersecurity?
Contact us at info@armexa.com

armexa.com

REV0-18-MAR-2026