OCTOBER 2024

Engineering IoT Industry 4.0 R&D
EIIR TREND

Futurize OT Cybersecurity of A Heavy Engineering Plant Quickly & Cost-Effectively

Cybersecurity Assessment & Implementation at Heavy Engineering Plant, Hazira

Author: Pareekh Jain, CEO EIIRTrend

Client Realized OT Cybersecurity is Necessary for Competitive Advantage

The client, a $6.5B+ heavy engineering conglomerate, operates a 750-acre manufacturing facility at Hazira, India featuring a 1.6 km waterfront and a highway. Hazira facility is equipped to manufacture extra-large and very heavy equipment for power projects, chemical, refinery, petrochemical & fertilizer industries, which can be shipped out via waterways. The Modular Fabrication Facility (MFF) at Hazira, one of the largest of its kind in South Asia, is capable of manufacturing several large modules simultaneously with an annual fabrication capacity of 50,000 MT.

As part of their digital transformation initiative, they aim to connect all machines and prioritize OT cybersecurity to ensure efficient, secure production and differentiate themselves in the market. Their digitalization strategy focuses on real-time data collection and processing from machines for improved analysis and optimization.

However, vulnerabilities in their legacy OT network present security risks, particularly as they adopt digital factory concepts. Cybersecurity, machine connectivity, and data transfer are key priorities. Client Leadership emphasizes delivering high-quality products manufactured in a secure environment, leveraging this focus on security as a competitive advantage.

To address this, the client seeks an end-to-end cybersecurity solution that meets both IT and OT requirements while being adaptable to future technologies.

LTTS Was Selected As A Specialized Industrial OT Cybersecurity Partner

LTTS was selected for its OT cybersecurity expertise, particularly in manufacturing, its vendor ecosystem, and product engineering capabilities. Its subject matter expertise, domain experience, and strong OEM partnerships aligned with the client's needs.

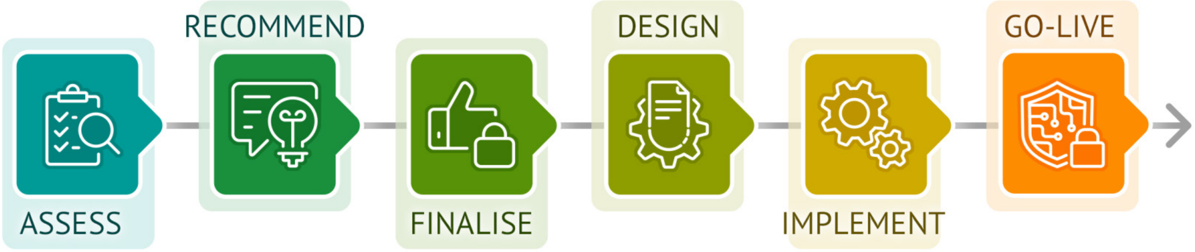
Among various management consulting, IT service, and engineering firms, LTTS stood out through a rigorous and independent evaluation process.

The knowledge of the plant ecosystem enabled LTTS to propose tailored solutions that met the client's requirements. LTTS provided a detailed walkthrough of these solutions, designed for different volumes and partners, and the final decision was based on the client’s specific criteria.

Comprehensive Six Step Industrial OT Cybersecurity Engagement Methodology Was Used By LTTS

LTTS first assessed the "As-Is" state and made recommendations for the "To-Be" state. The client and LTTS jointly finalized these recommendations, after which the project moved into the execution phase. LTTS then designed the solution based on the finalized recommendations, implemented it, and successfully brought it live.

Exhibit 1: Six Step Industrial OT Cybersecurity Methodology



Source: LTTS

Assess As Is State:

LTTS began by assessing the "As-Is" state, gaining a clear understanding of the operational technologies, systems, assets, and networks supporting the client's infrastructure. It conducted a thorough evaluation of their plant, providing a comprehensive overview of how these assets are currently connected across various processes and machines, identifying inherent vulnerabilities in their operations.

LTTS also analyzed the current connectivity of machines, the volume and nature of data being transferred, and potential communication pitfalls or challenges that could arise during their planned digitalization efforts.

Recommend To Be State:

LTTS recommended cybersecurity solutions and preventive measures for both the network and process control systems. LTTS team performed a thorough vulnerability assessment, understood the client’s challenges, and proposed various options for the "To-Be" state. It highlighted that security should be an overlay on top of connectivity, offering the client multiple connectivity options, including WiFi 6, Private 5G, and traditional three-tier core switching architectures. For each option, it provided a detailed analysis of the pros and cons.

Additionally, LTTS emphasized OT and asset visibility, traffic communication protocols, and how these changes align with the client’s evolving data collection needs. It also referred to various cybersecurity standards to ensure best practices. The client wanted to reduce capital expenditures without relying on multiple sensors, which influenced LTTS recommendations.

Finalize:

LTTS evaluated various products and assessed the feasibility of the solution implementation. The client had different perspectives on emerging technologies, such as SD-WAN, Private 5G, and LoRaWAN, all of which were considered from a connectivity standpoint.

In consultation with the client, LTTS finalized the solution and security requirements. The client ultimately chose a three-tier architecture. LTTS recommended implementing a PaloAlto Network IOT Security, offering a 360-degree threat view with asset visibility, network analysis, advanced detection and response capabilities for both OT and IT assets across the organization.

LTTS chose this solution for its ability to quickly discover and assess devices, providing comprehensive visibility across OT and IT assets using ML and crowdsourced telemetry. It enables easy segmentation, least privilege access, protection from known and unknown threats, and supports Zero Trust Security with contextual segmentation, continuous trust verification, security inspection, and 5G security.

Design:

LTTS designed the solution, finalized the deployment architecture, and created the solution design document. The design's key features include Zero Trust Security, future-proofing, asset visibility, vulnerability identification, network traffic analysis, and remediation capabilities.

Implement:

LTTS installed the solution, including all prerequisite components and configurations. While it was a commercial off-the-shelf (COTS) solution, it required fine-tuning to meet the client’s specific needs. LTTS implemented the solution, validated the system and assets, mapped the criticality, and adjusted detection rules based on the client’s environment for optimal threat detection.

Go Live:

The solution successfully went live after acceptance testing and sign-off. LTTS completed the knowledge transfer process and provided detailed handover documentation.

Complex Engagement Challenges Were Effectively Addressed By LTTS

Challenges of Retrofitting OT Cybersecurity in an Old Brownfield Plant

The plant is over 30 years old, with many aging machines. Retrofitting such an old plant with cutting-edge technology is difficult. Many machines operate as standalone units with limited or no connectivity, posing a challenge in bringing them into a connected, secure environment.

The plant has a mix of CNC machines and other equipment with minimal data connectivity. These legacy systems lack real-time data transmission capabilities, complicating the process of integrating them into modern, secure networks. Additionally, the plant employs multiple IoT devices for real-time data collection, which adds to the complexity. The challenge is further compounded by the scale of the project, covering three plant locations, 43 shop areas, 372 machines, 1,900 assets, and 150 IoT stations, creating a highly heterogeneous environment.

Solution:

LTTS adopted a layered approach to avoid overwhelming the system from day one. The initial focus was on protecting the boundaries where most communication occurs with the enterprise network, ensuring visibility and control over data entering and leaving the plant.

LTTS's deep knowledge of machines, the types of data they collect, and the security considerations needed by the client helped mitigate the challenges of this heterogeneous environment. This expertise allowed LTTS to design a solution that effectively addressed the unique security needs of the plant.

Challenge of Future-Proofing with 5G Enablement Without Heavy CapEx

The client faced uncertainty regarding their preferred technology requirements, especially when considering future advancements like 5G, while wanting to avoid heavy capital expenditures.

Solution:

LTTS designed the solution with future architecture in mind, offering multiple options to the client. While the future is uncertain, LTTS incorporated current technologies that support future needs, such as 5G-enabled firewalls, eliminating the need for additional investments in firewall infrastructure later on.

The solution aligns with the client's future requirements, considering the eventual need to refresh their L1 and L0 devices. As these devices are upgraded with superior controllers over time, they will seamlessly fit into the existing ecosystem. The implemented architecture is robust and future-ready.

Client Achieved Industrial OT Cybersecurity Outcomes

Fast & Cost-Effective Solution

LTTS delivered maximum return on investment (ROI) and optimized protection while saving capital expenditure (CapEx). The solution reduced total cost of ownership by saving 15 times the usual deployment time through sensor-less technology and 20 times the effort with automated policy creation. Quick and efficient implementation of Zero Trust OT Security eliminated the need for additional sensors and separate software subscriptions.

Visibility

The solution provided full, secure visibility into the OT environment, offering complete oversight of assets, data flows, and the ability to centrally monitor OT network traffic.

OT Security and Zero Trust Access

OT perimeters and devices were secured through granular segmentation and Zero Trust access protocols. The deployment was streamlined to accommodate various stages of digital transformation, from partially air-gapped systems to fully modern, 5G-enabled equipment.

Advice for Industrial Enterprises on Their OT Cybersecurity Journey

- Begin your OT cybersecurity efforts early in your digitalization process. OT cybersecurity should not be an afterthought but an integral part of both planning and implementation.
- Carefully select partners with expertise in OT cybersecurity, product engineering, and a deep understanding of the manufacturing ecosystem.
- Focus on comprehensive planning, keeping future needs in mind. Consider different technology options to ensure the solution is scalable and adaptable.
- Remember, the most expensive solution is not always the best. Explore alternative approaches to find cost-effective, efficient solutions.

LTTS Capabilities and Value Creation in OT Cybersecurity

With more than two decades of experience providing industrial automation and cybersecurity solutions, LTTS offers a wide range of OT Security services to help clients secure their operational technology (OT) environments.

LTTS offers a full range of industrial/OT cybersecurity assessment services, including consulting and advisory services, asset identification, profiling, and inventory, development of security roadmaps, assessment and mitigation reporting, network architecture review, and vulnerability identification and managed OT SOC.

LTTS leverages its deep domain and engineering knowledge, strong partnerships, and experience in deployment of new technologies to deliver solutions that meet the specific needs and challenges of different applications, from the heavy process industries to discrete manufacturing and critical infrastructure.

As a leading engineering firm for the process industries and other sectors, LTTS brings a wealth of engineering, process, and application knowledge to the world of OT security services.

In this engagement, LTTS's strong project management, in-depth solution knowledge, and R&D through a next-gen lab ensured timely project completion and client satisfaction. By leveraging domain expertise, OT cybersecurity knowledge, and assessment templates, LTTS efficiently delivered cost-effective, tailored solutions.