CLAROTY

CASE STUDY

RAIL TRANSPORTATION

Rail Rapid Transit System Rolls Through Digital Transformation Challenges with Support from Claroty

With more than 20 lines that span nearly 1,500 kilometers, this mass rapid transit system transports billions of passengers a year across urban and suburban districts. Like regional and national rail systems, rapid transit systems consist of a series of specialized industrial networks for railway electrification, signaling, and communications – but also rely on an extensive building management system (BMS) to support station and tunnel ventilation, lighting, and physical security. For operational efficiency and security reasons, the rail operator needed visibility and control across all these networks while maintaining compliance with rigorous, international safety integrity level (SIL) standards.

Challenges

- **Connectivity and digitization**. Passengers now expect timely, reliable updates on the status of train arrivals and schedules. Vendors need access to OT, IoT, and IIoT assets to monitor performance and service systems. Data from devices and processes need to be available in the cloud for analysis that informs decisions and drives operational efficiencies. However historically, OT systems and devices have been designed with isolation in mind — not to connect and communicate with IT systems and the internet.

- **Visibility**. Response and remediation of system failures is difficult because the rail operator has zero visibility into their industrial networks. A power outage or closed-circuit television camera (CCTV) malfunction could be a fix for a technician, an incident a cybersecurity specialist needs to investigate, or an act of vandalism to report to local police.

- **Maintaining SIL standards**. The railway sector differs from many other industrial sectors in two main ways: 1) it is deemed to be critical national infrastructure – rolling stock must remain operational all the time, and 2) it must ensure the safety of passengers and cargo. As such, compliance with SIL-1 up to SIL-4 standards is mandatory depending on safety risks associated with each function, system or component. Third-party equipment introduced into the industrial network, including cybersecurity devices, must be able to work completely divided from systems that are safety-critical, or integrate in a way that doesn't affect those systems and trigger the need for recertification.

- **Legacy OT assets**. This rapid transit system dates back several decades with vast kilometers of networks that are always evolving with new junctions, tracks, and stations. The multiple layers of legacy OT systems that comprise these networks were designed for a lifespan of about 25 to as many as 50 years. The volume and variety of vendors, products, and protocols (many of which are proprietary), along with a lack of security controls, adds further complexity to modernization efforts.

CUSTOMER QUOTE

"Threats targeting national critical infrastructure are on the rise, so our rail system is in the crosshairs. Plus, with unmanned metro trains in our near future, we need to expand automation and connectivity, securely. We can't spend years trying to apply IT security approaches that aren't effective and put our safety compliance at risk. We were impressed with Claroty's passive integration with switches, firewalls, and data diodes and their ability to provide us immediate asset visibility and continuous threat monitoring with no impact to our SIL certification."

The Solution

To secure their expansive, heterogenous OT environment and safely connect with IT systems, the rail operator selected Claroty as its partner, utilizing the following components of The Claroty Platform:

- **Continuous Threat Detection (CTD)** for full spectrum OT, IT, and IoT visibility, continuous security monitoring, and real-time risk insights with zero impact to operational processes, underlying devices, and SILs.
- **Secure Remote Access (SRA)** to safeguard indusrtrial networks from threats introduced via unmanaged and unmonitored access by remote users, including third-party vendors and employees.
- **Enterprise Management Console (EMC)** to simplify management at scale, consolidating data from Claroty products and providing a unified view of assets, activities, and alerts across multiple networks, tracks, and stations. The Claroty Platform also integrates seamlessly via the EMC with IT security infrastructure.

Outcomes

Full visibility and asset profiling to understand exposure to cyber risk. The rail operator has telemetry and, thus, visibility to quickly determine if suspicious activity is happening on any of their industrial networks or devices – even in aging systems that utilize proprietary protocols. They can monitor for threats and identify risks due to unpatched vulnerabilities in high-priority assets or misconfigurations, allowing them to act faster to mitigate risk and assure continued operations of critical processes.

Digitization without breaking security. Claroty integrates with data diode units – including the Siemens Data Capture Unit – that control the flow of information from industrial assets out to IT systems without impacting SILs. The rail operator can confidently connect to systems to communicate travel updates to riders, collect data from IoT and OT assets for storage and analysis in the cloud, and open new connectivity vectors — including with automation systems that support unmanned metros.

Connectivity for remote parties. Equipment manufacturers can seamlessly access systems remotely to service equipment, while security teams have granular control over remote sessions — specifically the ability to manage the who, what, and when of access to devices and systems. The rail operator can also outsource services to companies that specialize in specific operational areas such as preventative maintenance, reducing rolling stock downtime, increasing service quality, and gaining efficiencies.

About Claroty

Claroty is the industrial cybersecurity company. Trusted by the world's largest enterprises, Claroty helps customers reveal, protect, and manage their OT, IoT, and IIoT assets. The company's comprehensive platform connects seamlessly with customers' existing infrastructure and programs while providing a full range of industrial cybersecurity controls for visibility, threat detection, risk and vulnerability management, and secure remote access—all with a significantly reduced total cost of ownership.

Claroty is backed and adopted by leading industrial automation vendors, with an expansive partner ecosystem and award-winning research team. The company is headquartered in New York City and has a presence in Europe, Asia- Pacific, and Latin America, and deployments on all seven continents. For more information, visit www.claroty.com.