CASE STUDY

Renfe Automates Inventory and Monitoring of Industrial Network Operations and Security

About the Customer: Renfe Operator

Renfe Operator was born in 2005 as a consequence of the segregation of functions of railway infrastructure from the operation of the transportation of people and goods. Later, in 2012, Renfe Operator was established as the head of a group of companies created by Royal Decree to advance the process of liberalization of the railway sector and its opening to competition.

As Renfe Operator is a public entity dedicated to the freight and passenger transport industry, a very important part of its services is closely linked to industrial activity and railway material support infrastructure that combines IT, OT and IoT technologies.

The Challenge: How Does a Global Transport Operator Protect its IT, OT, and IoT Infrastructure?

Although cybersecurity is strategic for any company today, most resources are poured into IT cybersecurity. While IT is a very common source of cyberattacks, this doesn't cover all connected infrastructure in companies with industrial environments.

Renfe's strategic cybersecurity objective is the unity of action in all technological contexts. Working with Nunsys Group as a technological partner, a self-inventory, monitoring and security project was implemented for several industrial networks located in train stations. Renfe aimed to technologically integrate the Nozomi Networks platform with Lunaria from Opscura and the Sirena platform from Nunsys Group.

Company Profile

Industry: Transportation

Employees: 14,000+

Location: Spain

Challenges

- **Unifying the protection** of their IT, OT, and IoT infrastructure
- **Understanding all of the systems and data** in their OT environment
- **Increasing risks** in industrial OT and IoT environments

Results

- **Enhanced security**
- **Reduction in response time** to security incidents
- **More accurate responses** to security incidents

Overlooked and Underserved: Securing OT Environments

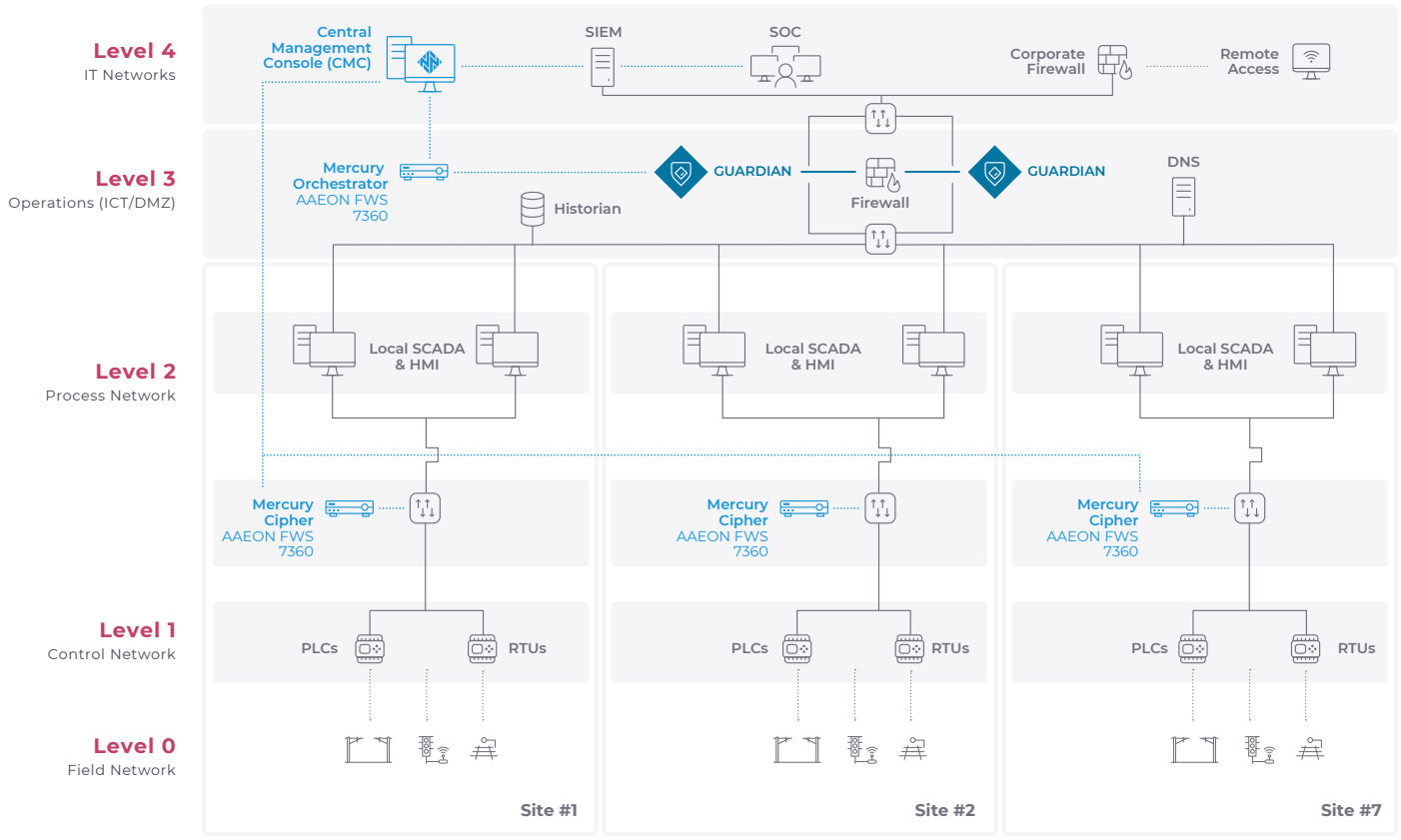
Renfe Aims to Unify OT Security Operations

Product information systems and OT systems (which have long lifespans) do not have the focus in operational environments that they do in IT environments. This secondary role has made it a burden to evolve operational environments towards a level of maturity equivalent to that of IT. Often, the exact number of these OT systems that are connected, and even data information, is unknown. This lack of knowledge can lead to risk, particularly in an OT environment's level of patching. With the growth of industrial IoT solutions, these risks will increase considerably.

To solve this problem, Nunsys proposed the Sirena (Security Information and Risk analysis Extending Industrial Network Applications) platform, which allows asset owners to inventory and subsequently monitor all these devices, in addition to showing the results of events, critical or not, in an accessible way with natural language.

Prior to this project, Renfe's CISO had the necessary infrastructure and services around them to detect threats with early warning systems (through the corporate SIEM platform), and a complete CERT team for the company's entire IT/OT environment.

PURDUE Tiered Architecture

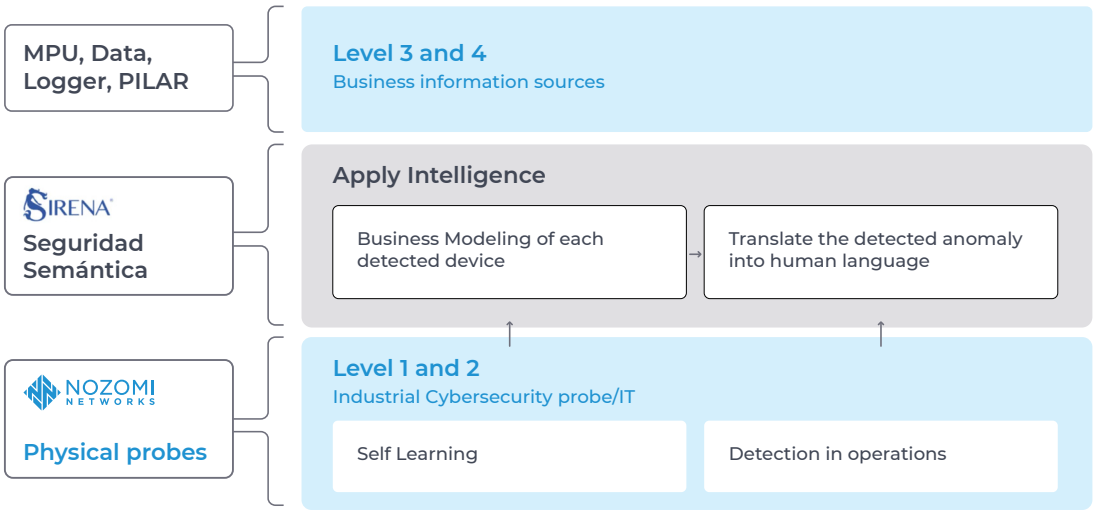


The Solution: Renfe looks to Nozomi Networks, Nunsys Group and Opscura

Security Infrastructure Organization

Renfe trusted Nunsys to organize this service as a technical Industrial Security Office, as support for the already established practice of cybersecurity in the OT technological context. Renfe's security infrastructure was organized as follows:

1. **Traffic Capture, Sending and Receiving Platform:** Equipment in each station and in the Data Processing Center of probes with the functions of capturing, sending and receiving remote traffic by 3G/4G or TCP/IP. This equipment has advanced cybersecurity functionalities such as PKI, authentication, encryption and local log collection, as well as the capacity to expand functionalities in the future by incorporating new requirements for access and monitoring of the industrial network. This is the Lunaria technology from Opscura.
2. **Traffic Analysis and Event Correlation:** Highly available equipment to these OT environments (industrial protocol traces, complex queries) and parameterization of existing platforms. Sirena implements Semantic Security applied to operations environments, using business information (risk analysis or CMMS systems associated with the IT/OT network) for quick decision-making. This makes it possible to provide greater functionality to the existing industrial cybersecurity probes (in this scenario, Nozomi Guardian and Mercury) and display the information that each user profile requires in a more complete, simple and straightforward way, using natural language. This allows a considerable reduction in response time to security incidents and a more accurate response from CyberSOC.
3. **Connection with Business Platforms:** A platform with tailored functionalities to automatically label assets based on patterns, label alarms, present results in natural language, integrate with a risk analysis platform and integrate with CMDB/CMDB software to enrich business information, assets and inclusion of alerts in the corporate SIEM, as well as business dashboards. All with the Sirena Technology from Nunsys Group.



The Results: Renfe Increases Security and Improves the Speed of Decision-Making

Industrial Safety Operation

The current Renfe-CERT 24x7 team is reinforced by the Nunsys CyberSOC in the investigation of incidents for OT environments (industrial protocol traces, complex queries) and paramaterization of existing platforms. It is worth highlighting the contribution of Sirena, which implements Semantic Security applied to operations environments. To do this, it uses business information (risk analysis or CMMS systems associated with the IT/OT network) for quick decision-making. This makes it possible to provide greater functionality to the existing industrial cybersecurity probes (in this scenario, Nozomi Guardian and Mercury) and display the information that each user profile requires in a more complete, simple and straightforward way, using natural language. This allows a considerable reduction in response time to security incidents and a more accurate response from CyberSOC.

Industrial Safety Management

Nunsys holds periodic support meetings on industrial cybersecurity with the RENFE-CERT team and with the cybersecurity government area, sharing information, experience and capabilities, identifying anomalous traffic, analyzing changes in the infrastructure and communication between supposedly isolated networks, actions of third parties (providers) and incremental loading of business information on the platforms to improve daily management.

This service seeks to increase security in Renfe's OT environment, and improve the speed of decision-making by monitoring engineers, or by a technical profile, not cybersecurity, that requires real-time information on any anomaly in the operation.

nunsys GROUP

About Nunsys Group

Nunsys Group participates in the consortium awarded the Incibe challenge to create a CyberSOC for Healthcare valued at €1.8MM, which allows it to develop cutting-edge national technology. In addition, it has extensive experience in this type of technologies, having anticipated the needs of the sector and creating a unique bundle of solutions that work together: OPSCURA + NOZOMI NETWORKS + SIRENA + ERIS-CERT.

Learn more at **nunsys.com**

Nozomi Networks protects the world's critical infrastructure from cyber threats. Our platform uniquely combines network and endpoint visibility, threat detection, and AI powered analysis for faster, more effective incident response. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

NOZOMI NETWORKS

nozominetworks.com