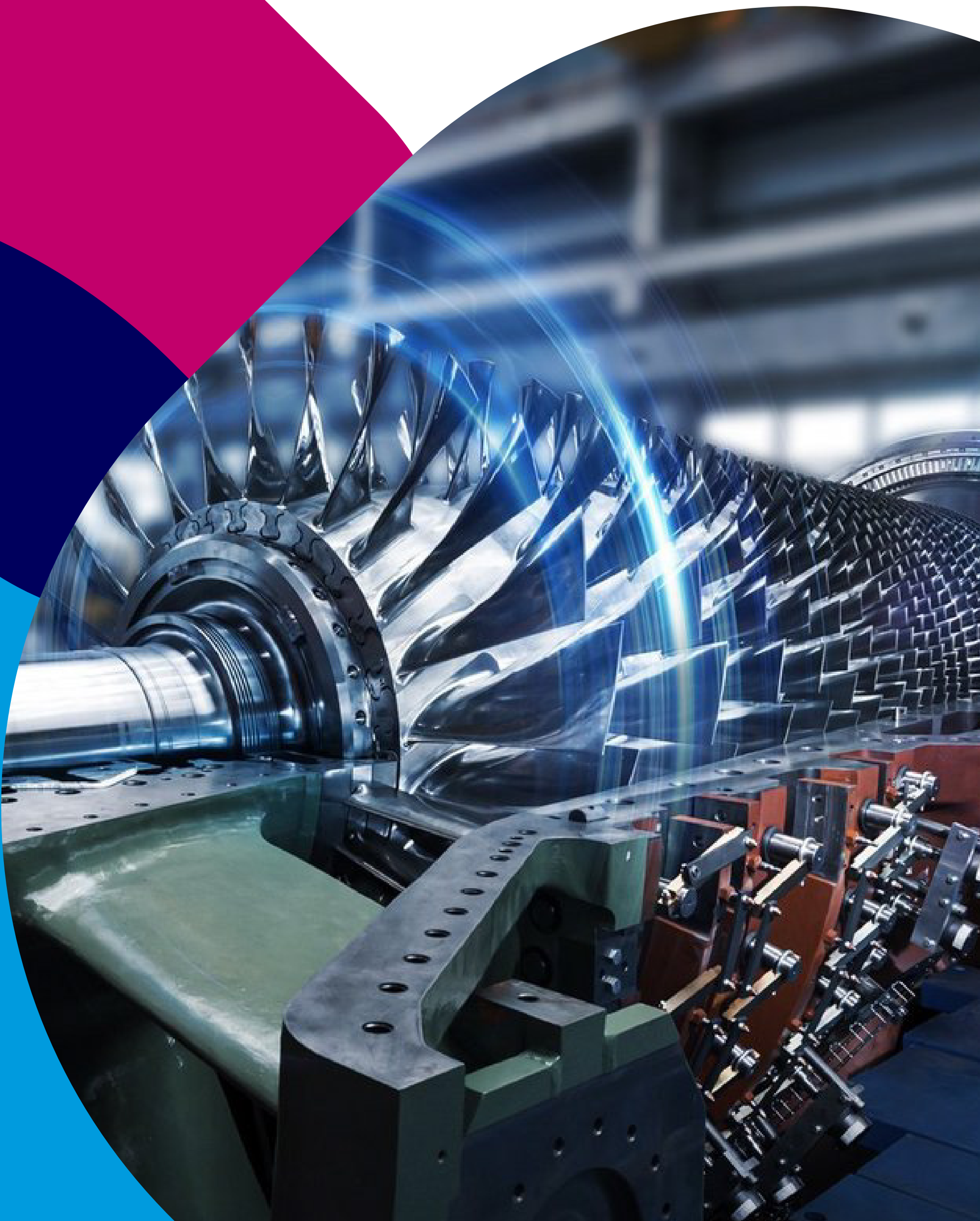
Safeguarding Energy Infrastructure: Ansaldo Energia's Multi-Step Approach to Industrial Cybersecurity



HWG Sababa

ansaldo energia

About Ansaldo Energia

- **170 years of experience with participation in hundreds of projects around the world**
- **Presence in 35+ countries worldwide**
- **Currently employs over 3,300 people**

Introduction

The evolution of safety and security requirements is a natural process for any energy player with a long and storied history. Over the course of a century, such companies experience a dynamic interplay between technological advancements, regulatory changes, and societal shifts that shape their approach to safeguarding operations, assets, and personnel.

The 20th century alone saw a transition from predominant physical security measures - including access control, guards, perimeter protection - and basic safety training to advanced electronic security systems and standardized safety regulations. This century ushered in the digital era, thus introducing cybersecurity concerns: protection against cyber threats, data breaches, and hacking emerged as key priorities. At the same time, safety training became more advanced, ergonomic practices were integrated, and adherence to rigorous regulations intensified.

Counting hundreds of power plants since the first one was founded back in 1923, **Ansaldo Energia** has also navigated the dynamic landscapes of security, safety, and cybersecurity, constantly adapting its strategies to meet the ever-changing demands of a modernizing world.

Nowadays, the integration of digitalization and connectivity into industrial environments clamors for a holistic approach to security, encompassing physical security measures, comprehensive safety protocols, continuous training initiatives, compliance with regulatory standards, as well as vertical cybersecurity measures and solutions.

“The industrial sector is strongly embracing digital transformation and the concept of Industry 4.0, leading to an increasing connectivity and convergence between IT and OT. Not so long ago, there were very few OT systems connected to the network; today, almost all of them are” **commented Stefano Santucci, CIO at Ansaldo Energia**, *“Managing security effectively in the OT environment requires specialized knowledge and a comprehensive approach in order to address the specific challenges, vulnerabilities and risks”.*

The project

When it comes to such large industrial enterprises with years of history and a complex environment, defining an effective cybersecurity strategy is not only about implementing technologies, but requires the careful formulation of a comprehensive action plan encompassing multiple steps. Leveraging a well-established and successful partnership, Ansaldo Energia turned to **HWG Sababa** for this complex project.

Step 1. Empowering Plant Engineers with Industrial Cybersecurity Training

In the final stage of the first collaboration with Sababa Security to secure the energy giant's IT infrastructure, Ansaldo Energia had considered it essential to integrate into the project a specific training on industrial cybersecurity, aimed at providing engineers with all the necessary tools to develop, manage and integrate products in a secure and compliant way. Among the almost 100 participants, some have become a real reference point in the company for OT security.

“This OT training was a real success, and not only because of the high-quality content and the great competence of the experts who delivered it, but also because it made all the operators begin to consider our Cyber Security Operation (CSO) team as a competence center for industrial security”, **explained Marco Grillo, Deputy General Manager at Ansaldo Energia** *“Given the results, our intention is to carry out this type of training on a regular basis, especially after the introduction of the NIS 2 Directive. Customers are asking us to comply with cybersecurity requirements on a daily basis, so I would like the training to be an ongoing process, especially for those who work in the plants”.*

Step 2. Micro-Segmentation Strategy to Minimize Risks

Ansaldo Energia's second step towards safeguarding against cyber threats was **implementing micro-segmentation**. The process - which lasted about 3 months - had the ultimate goal of dividing the network into smaller, isolated segments, each containing a specific production machinery, which couldn’t communicate with others on the same network. This phase saw a joint effort between Ansaldo Energia, HWG Sababa and digipoint, with the most complicated part being the evaluation of the network traffic that could be allowed for each individual machine.

“This proactive approach holds immense importance for Ansaldo Energia. Indeed, like many other energy players, Ansaldo operates legacy systems that cannot be easily upgraded due to compatibility concerns. The isolation provides a security layer even for these older systems, safeguarding them from modern cyber threats”, **commented Diego Lusso Cybersecurity Analyst at HWG Sababa**, *“Moreover, with micro-segmentation, the potential pathways for lateral movements are drastically reduced, preventing the spread of potential attacks to other parts of the network and minimizing risks”.*

Step 3. ISA/IEC 62443 Assessment

Security is not solely a technological challenge, but it delves into organizational processes, user behaviors, policy frameworks, and procedures. This is why Ansaldo Energia and HWG Sababa agreed that assessment would be a key step in their multi-step project.

With the aim of gaining insight into the current security posture and identifying areas of improvement, HWG Sababa's team conducted an audit against ISA/IEC 62443 - a widely recognized standard that focuses on establishing a framework for cybersecurity in industrial automation and control systems.

"After identifying the objectives and the scope of the activity, we established the audit criteria based on the requirements of the ISA/IEC 62443" **explained Irene Parodi, Cybersecurity Analyst at HWG Sababa** *"We interviewed many of Ansaldo Energia's stakeholders, inspected every corner of the factory, verified the application of policies and procedures, identified vulnerabilities and prioritized them based on their potential impact and risk. The whole audit lasted about 2 months".*

At the end of the activity, HWG Sababa's team prepared a comprehensive report that outlined findings, observations, and suggestions for improvements. Based on this, together with Ansaldo Energia's stakeholders, they developed a roadmap of corrective actions to be implemented, addressing organizational, policy, and procedural aspects.

Step 4. Navigating Technical Solutions

While working on the corrective actions identified within the ISA/IEC 62443 assessment, the energy giant turned its gaze to the market to find vertical security solutions that would best protect their production plants and ensure greater prevention and detection of threats.

After extensive research and testing - with the support of HWG Sababa - Ansaldo's choice fell on two major players in the industrial sector, **Radiflow** and **TXOne Networks**. While Radiflow's products were deployed to analyze the OT traffic and assess risks, TXOne Networks' solutions were selected to increase the security of obsolete and non-upgradeable workstations, as well as to protect critical communications with industrial IPS. The icing on the cake is the continuous monitoring of all implemented solutions through HWG Sababa's Security Operations Center.

Balancing operational continuity with seamless integration of cybersecurity measures proved to be a multi-faceted challenge that required careful planning and execution.

"The most tricky part was conveying the message internally that the implementation of such solutions would not affect operations. The key is to view security, safety, compliance, and operational continuity as interconnected components that together contribute to the resilience and success of the organization" **commented Ivan Monti, CISO & Head of IT Infrastructure Operations at Ansaldo Energia** *"Fortunately, cybersecurity is now a well-established concept among our OT operators, especially after the training they attended, so this helped us overcome the initial apprehension in a short time".*

Results and next steps

Despite the ambition and complexity of the project, the objectives initially set were successfully achieved, further consolidating the relationship between the energy giant and HWG Sababa.

Moreover, having in mind that cybersecurity is not a one-time procedure, but a continuous process that evolves in step with threats and technologies, Ansaldo Energia already has a clear idea of what the next moves will be.

“With HWG Sababa, we have so far focused on securing our production facilities, but now we are actively working on monitoring the security of power plants and turbines that we supply to our customers around the world”, **explained Ivan Monti, CISO & Head of IT Infrastructure Operations at Ansaldo Energia** *“The next step will be to bring the security of older power plants and gas turbines to the same maturity level of the most recent ones, especially in view of the new regulations and requirements in the industry”.*

A further objective is to set up a cyber demo room within Ansaldo Energia's Generator Test Room, where the quality of internally produced generators is tested. Since its structure and automation have many similarities with the plants of Ansaldo's customers, it has been selected as a suitable testbed to show - through dedicated dashboards - the security countermeasures that can be taken to protect power generation systems.

HWG Sababa

ansaldo energia

Follow us on:

in

www.hwgsababa.com
contacts@hwgsababa.com