nanolock

Food & Beverage Industry
CASE STUDY

A world-leading food production company implements NanoLock OT Defender to protect its Programmable Logic Controllers (PLCs).

After just one day, the company benefits from device-level, zero-trust protection with zero impact on PLC performance or functionality.

Profile:	**Multinational food company present in 30+ countries**
Sales volume:	**$15 Billion**
Number of employees:	**Over 100,000**
Number of plants:	**300**

The Company is one of the world's largest food producers known for its 100+ brands and three million points of sale. Across its hundreds of plants, the Company deploys a large, heterogeneous fleet of Programmable Logic Controllers (PLCs), varying in models, technology, and function. It's a massive operation with disparate systems and many moving parts.

The challenge

Managing a diverse fleet of Programmable Logic Controllers (PLCs) and the insider threat

The Company approached NanoLock after a disgruntled employee attempted to tamper with the heat configuration of the ovens, purposely putting the safety of other employees and the entire plant in danger.

The challenge lay in the fact that the production lines in each plant were empowered by OT networks, separate networks, and multi-island PLCs which ranged widely in size, purpose, and age. To program PLCs, the Company deployed in-house programmers as well as various third-party contractors, whose trail could not be followed, tracked or traced back. Most PLCs were not part of an OT network, and programming and support were executed using a physical Engineering Workstation (EWS) – sometimes a third-party laptop which provided services to other companies. Remote access was available on a few of the PLCs only. While the company used different cybersecurity products such as firewalls to protect their network, in the case of PLCs there was no user and password mechanism for restricting access.

The Company wanted to:

- Prevent unauthorized access across all PLC environments
- Deploy a single solution for both legacy and new assets
- Minimize downtime through simple deployment
- Ensure minimal impact on day-to-day PLC operations and the programming process
- Get a clear audit trail at factory & headquarters levels

The solution

A prevention-based approach to PLC security

NanoLock's OT Defender solution ensures that only a few certified users are allowed to program PLCs through the use of a username and password. When finished, the user logs out and no more changes are allowed. All successful and unsuccessful login attempts are monitored and an audit trail is built. When there are subsequent unsuccessful login attempts, NanoLock blocks the system until an authorized administrator re-enables access. In addition, NanoLock sends system usage and abnormal activity alerts to relevant managers where necessary.

Results and benefits

- Quick, cost-effective deployment
- Complements existing cybersecurity measures
- Protects new and legacy PLCs regardless of model or age
- Blocks cyber incidents coming from outside adversaries and third parties
- Blocks incidents coming from trusted sources such as insiders, customers, and human errors
- Avoid catastrophic product recalls

With NanoLock, the Company achieves significantly improved cybersecurity with no impact on the performance and functionality of PLCs, and minimal impact on daily workflows. Plus, it ensures the operational integrity of its PLCs even in the event of a cyber attack.

Our Partners

indra RENESAS ISTARI Atlantica ectacom

Complies With:

ISA NIST enisa NERC CIP

For more information:
info@nanolocksec.com | www.nanolocksecurity.com

nanolock