Automating the World

Surge in Manufacturing Attacks Demands Smarter Production Controllers

Ratingen, Germany - 20th of October, 2025

[Source: Mitsubishi Electric Europe]

A global study by Telstra and Omdia found that 80% of manufacturing firms experienced a significant increase in security incidents or breaches last year, while only 45% are adequately prepared in their cyber security posture. This trend highlights the growing vulnerability of production environments as they become more connected and digitised.

According to the same study, manufacturers affected by a cyber attack reported issues costing between $200,000 and $2 million per incident.

Let's take a more detailed look. Ransomware attacks on industrial sectors grew by 87% year-on-year with manufacturing accounting for 69% of all incidents, according to Dragos' February 2025 report. With manufacturing being the most targeted industry for four consecutive years according to IBM's X-Force 2025 Threat Intelligence Index, industrial security undoubtedly has become a critical concern.

The connection of information technology with operational technology in manufacturing has introduced new security challenges. While traditional security approaches can address many of these issues, the evolving threat landscape has created a need for robust cybersecurity measures embedded directly into automation products themselves.

"With the increasing reliance on IoT connectivity including Machine-to-Machine communication and Human-Machine Interfaces too, the central components of the industrial 'nervous system'—the controllers—must now serve as critical guardians of information security," said Daniel Sperlich, Strategic Product Manager for Controllers in the EMEA region at Mitsubishi Electric. "Our latest MX Controllers have been developed to meet these evolving security requirements while maintaining the precision and reliability essential to manufacturing operations."

DDoS and Ransomware: Twin Threats to Production Continuity

The threats facing manufacturing extend beyond ransomware. Distributed Denial of Service (DDoS) attacks have emerged as a significant concern, with a report by Zayo Group revealing that the manufacturing sector has seen a 257% increase in attack size between 2023 and 2024. These attacks target production systems and can cause substantial operational disruption.

"The manufacturing sector is facing a convergence of threats," explained Daniel Sperlich. "Ransomware directly targets intellectual property and operational data, while DDoS attacks aim to disrupt production by overwhelming network infrastructure. Both can result in costly downtime that manufacturers simply cannot afford."

The financial impact of these attacks is substantial. According to the Zayo Group report, the typical DDoS attack lasts 39 minutes and costs businesses approximately €5,350 per minute, resulting in average losses of nearly €210,000 per incident. For manufacturing operations with just-in-time production schedules and complex supply chains, even brief disruptions can have cascading effects throughout the production process.

Zero-Downtime Security: The Controller's Critical Role

A key challenge in manufacturing cybersecurity is maintaining security without compromising availability. As Omdia's research indicates, the greatest financial impact from cyber incidents occurs when they affect production control systems.

"Manufacturing operations do not permit downtime like traditional IT infrastructure," noted Sperlich. "Routine cybersecurity patching or incident response simply aren't options in many production environments. Security needs to be built into the fundamental architecture of industrial systems."

Effective security for manufacturing environments requires multiple layers of protection that operate without disrupting production processes. This includes secure-by-design components, network segmentation, access controls, and continuous monitoring capabilities. Mitsubishi Electric's MX Controllers integrate these security principles while maintaining the operational performance critical to manufacturing environments.

What sets modern industrial controllers apart in terms of security is their ability to protect both operational technology (OT) and information technology (IT) environments while maintaining continuous production. The MX Controllers establish a secure boundary between these environments, helping manufacturers implement effective cybersecurity measures without interrupting operations.

Secure-by-Design: The New Standard for Industrial Control Systems

The manufacturing industry is responding to these challenges with increased investment in cybersecurity measures and greater attention to security standards in industrial control systems. This includes adopting security frameworks designed for industrial environments and implementing defence-in-depth strategies that protect critical production assets.

"The security landscape for manufacturing will continue to evolve as threat actors develop new techniques," adds Daniel Sperlich. "Manufacturers need to adopt security solutions that can adapt to these changing threats while maintaining the operational reliability that production environments require."

The MX Controllers address these evolving security challenges through several key features aligned with international security standards and IEC 62443-4-2 certification. These include encrypted communications to prevent eavesdropping and unauthorized access, and comprehensive user authentication that allows access and operation permissions to be set for different users based on their roles. This approach enables separate asset management for different stakeholders, such as end users and machine manufacturers, while maintaining a secure operational environment.

Additionally, the upcoming feature: controller's built-in OPC UA server and client functions allow for secure connectivity between operational systems and IT infrastructure, addressing one of the most significant vulnerabilities in manufacturing environments—the boundary between production systems and business networks.

Security under control(ler)

As manufacturing cyber threats intensify, production controllers have emerged as the critical defensive cornerstone in industrial security strategies. These systems now serve as active guardians protecting the integrity of entire production environments, not merely operational components. By implementing robust controllers at the heart of operations, organisations transform vulnerable points into defensive assets, ensuring both operational continuity and data protection in today's hostile digital landscape.

Sources:

1. https://www.telstrainternational.com/content/dam/shared-component-assets/telstra-international/global/news-research/research/secure-manufacturing-the-challenges-of-it-ot-convergence/WP_IT-OT-security-convergence_manufacturing_digital.pdf
2. https://www.dragos.com/ot-cybersecurity-year-in-review/#anchor-report
3. https://zayoeurope.com/wp-content/uploads/2024_2H_Zayo_DDoS_Insights_Report_v3.pdf
4. https://www.ibm.com/thought-leadership/institute-business-value/report/2025-threat-intelligence-index

About Mitsubishi Electric Corporation

With more than 100 years of experience in providing reliable, high-quality products, Mitsubishi Electric Corporation (TOKYO: 6503) is a recognised world leader in the manufacture, marketing, and sales of electrical and electronic equipment used in information processing and communications, space development and satellite communications, consumer electronics, industrial technology, energy, transportation, and building equipment. Mitsubishi Electric enriches society with technology in the spirit of its "Changes for the Better." The company recorded a revenue of 5,521.7 billion yen (U.S.$ 36.8 billion*) in the fiscal year ended March 31, 2025.
For more information, please visit www.MitsubishiElectric.com

*U.S. dollar amounts are translated from yen at the rate of ¥150=U.S.$1, the approximate rate on the Tokyo Foreign Exchange Market on March 31, 2025.

About Mitsubishi Electric Factory Automation Business Group

Offering a vast range of automation and processing technologies, including controllers, drive products, power distribution and control products, electrical discharge machines, electron beam machines, laser processing machines, computerised numerical controllers, and industrial robots, Mitsubishi Electric helps bring higher productivity – and quality – to the factory floor. In addition, its extensive service networks around the globe provide direct communication and comprehensive support to customers. The global slogan "Automating the World" shows the company's approach to leveraging automation for the betterment of society, through the application of advanced technology, sharing know-how, and supporting customers as a trusted partner.

For more about the story behind “Automating the World” please visit:

www.MitsubishiElectric.com/fa/about-us/automating-the-world

Factory Automation EMEA

Mitsubishi Electric Europe B.V., Factory Automation EMEA has its European headquarters in Ratingen near Dusseldorf, Germany. It is a part of Mitsubishi Electric Europe B.V. which has been represented in Germany since 1978, a wholly owned subsidiary of Mitsubishi Electric Corporation, Japan. The role of Factory Automation EMEA is to manage sales, service, and support across its network of local branches and distributors throughout the EMEA region.

For more information, please visit emea.mitsubishielectric.com/fa

About e-F@ctory

e-F@ctory is Mitsubishi Electric's integrated concept to build reliable and flexible manufacturing systems that enable users to achieve many of their high-speed, information-driven manufacturing aspirations. Through its partner solution activity, the e-F@ctory Alliance, and its work with open network associations such as the CC-Link Partners Association (CLPA), users can build comprehensive solutions based on a wide-ranging "best in class" principle.

In summary, e-F@ctory and the e-F@ctory Alliance enable customers to achieve integrated manufacturing but still retain the ability to choose the most optimal suppliers and solutions.

**e-F@ctory and iQ Platform are trademarks of Mitsubishi Electric Corporation in Japan and other countries.*

**Other names and brands may be claimed as the property of others.*

**All other trademarks are acknowledged*

Follow us on:

YouTube	youtube.com/user/MitsubishiFAEU
X	twitter.com/MitsubishiFAEU
LinkedIn	https://www.linkedin.com/showcase/mitsubishi-electric-europe-factory-automation-emea/
Instagram	https://www.instagram.com/mitsubishi_electric_fa_emea/

Press contact:
Mitsubishi Electric Europe B.V.
Factory Automation EMEA
Anna Sendecka
Anna.Sendecka@mpl.mee.com

Story/Editor:
Tigers Ltd.
Artur Kosior
Q22, Jana Pawła II 22
Warsaw, PL, 00-132
Tel.: +48 663 525 108
artur.kosior@tigers.pl
www.tigers.pl

Distribution/Circulation:
MEPAX
Jessica REITMAIER
Tel.:+34(0)695202002
j.reitmaier@mepax.com
www.mepax.com