CYBER RESILIENCE ACT
Mitsubishi Electric's resilience management ensures CE conformity

The Cyber Resilience Act (CRA) requires manufacturers, importers and distributors to implement cybersecurity measures throughout the entire lifecycle of products containing digital elements. In the context of industrial automation, this means products must be developed securely from the outset ('secure by design'), delivered with preset security features ('secure by default'), and any known vulnerabilities must be actively addressed. Furthermore, free security updates must be available throughout the entire lifecycle.

Regulation (EU) 2024/2847 was published on 20 November 2024. Reporting requirements for actively exploited vulnerabilities will take effect on 11 September 2026, with all requirements applying in full from 11 December 2027. This makes cybersecurity a central component of CE conformity.

For operators of networked production facilities, mandatory update and reporting processes will increase predictability and reduce supply chain risks. Going forward, controllers, HMIs and network technology must be powerful, auditable and cyber-resilient. Mitsubishi Electric consistently incorporates CRA requirements into its development, operational and support processes. A Product Security Incident Response Team (PSIRT)

coordinates vulnerability management and publishes countermeasures. As a CVE Numbering Authority (CNA), Mitsubishi Electric can clearly identify and communicate security vulnerabilities transparently. The company also relies on signed firmware updates, role-based access controls and monitoring concepts to protect operations and ensure compliance. All these measures are based on international standards such as IEC 62443-4-2, creating a robust foundation for auditing and verification.

From HMI to PLC: Technical measures for auditable cyber resilience

Mitsubishi Electric's success in implementing these requirements is well-documented. HMIs, such as the new GOT3000 series, use signed firmware updates, restrictive default configurations and role-based user management. PLC systems, such as the new MELSEC MX-F and MX-F platforms, are made resilient to cyberattacks by employing separate engineering and operating networks, encrypted remote access, and defined update processes. Typical evidence includes a complete SBOM (Software Bill of Materials), documented patch processes, log export, and communication of the support period. Comparable principles apply to drives, robots, and engineering software, including secure communication paths, documented lifecycle support periods, and disclosure of known CVEs (Common Vulnerabilities and Exposures). These measures increase resilience to manipulation and support verification in the context of CE marking.

Current threat situation and regulatory pressure

Current developments highlight the relevance of CRA. According to the Dragos Report, the number of ransomware attacks on industrial

organisations increased by over 87 per cent in 2024 compared to 2023, while new ICS-specific malware families were identified. At the same time, Germany is tightening requirements for companies with the NIS-2 Implementation Act. From the end of 2025 onwards, around 29,000 companies will be subject to extended security and reporting obligations, with cybersecurity explicitly becoming a management responsibility. This significantly increases compliance pressure along the industrial supply chain and supplements the CRA requirements.

Greater trust in industrial systems

The CRA creates opportunities for greater transparency and trust in automation solutions. Mitsubishi Electric offers solutions for secure, future-proof production, including secure firmware updates, access controls and monitoring concepts. The company also provides checklists and security advisories to facilitate audit verification. Weekly patch windows for HMIs or PLC engineering via jump hosts according to the bastion principle are practical examples that illustrate the benefits for operations.

Author: Silvia von Dahlen, Marketing Communications Manager

Mitsubishi Electric Europe B.V. Industrial Automation

Further information at:

[Cyber Resilience Act CRA – Cyber security for industry](#)

Sources

Regulation (EU) 2024/2847 *https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

Dragos report: https://www.dragos.com/resources/press-release/dragos-reports-ot-

ics-cyber-threats-escalate-amid-geopolitical-conflicts-and-increasing-ransomware-

attacks

NIS 2 Implementation Act: BSI - Press - NIS 2 implementation: Bundestag passes

cybersecurity law

Images

Image 1: Secure by default and by design. Mitsubishi Electric consistently

integrates CRA requirements into development, operation, and support.

(Source: Getty Images)

Image 2: No chance for ransomware attacks thanks to CRA.

The image(s) distributed with this press release are for editorial use only and are subject to copyright. The image(s) may only be used to accompany the press release mentioned here; any other use is prohibited.

About Mitsubishi Electric Corporation

With more than 100 years of experience in providing reliable, high-quality products, Mitsubishi Electric is a globally recognized leader in the manufacture, marketing, and sale of electrical and electronic equipment for information processing and communications, space development and satellite communications, consumer electronics, industrial technology, energy, mobility and building technology, and heating, cooling, and air conditioning technology. Based on its motto, "Changes for the Better," Mitsubishi Electric strives to enrich society with technology. The company achieved consolidated sales of US$36.8 billion* at the end of the fiscal year on March 31, 2025. It has sales offices, research companies, development centers, and manufacturing facilities in over 30 countries. Mitsubishi Electric has been represented in Germany since 1978 as a subsidiary of Mitsubishi Electric Europe. Mitsubishi Electric Europe is a wholly owned subsidiary of Mitsubishi Electric Corporation in Tokyo.
For more information, visit www.MitsubishiElectric.com.

Amounts in US dollars are converted from yen at a rate of ¥150=US$1, the approximate rate on the Tokyo foreign exchange market on March 31, 2025.

About Mitsubishi Electric Factory Automation Business Group

Mitsubishi Electric offers a wide range of automation and processing technologies, including controllers, drive products, power distribution and control products, spark erosion machines, electron beam machines, laser processing machines, numerical computer controls, and industrial robots, contributing to higher productivity and quality in manufacturing. In addition, extensive service networks around the globe provide direct communication and comprehensive support for customers. The global slogan "Automating the World" illustrates the company's approach to using automation for the benefit of society through the use of advanced technologies, the sharing of expertise, and support for customers as a trusted partner.

For more information on the history of "Automating the World," please visit:

Mitsubishi Electric Industrial Automation

Mitsubishi Electric Europe B.V., Industrial Automation is headquartered in Ratingen near Düsseldorf. It is part of Mitsubishi Electric Europe B.V., which has been represented in Germany since 1978 and is a wholly owned subsidiary of Mitsubishi Electric Corporation, Japan. Its task is to manage sales, service, and support for the Industrial Automation division throughout the DACH region and Benelux.

Further information can be found at de.mitsubishielectric.com/fa

Automating the World

Further information:

de.mitsubishielectric.com

Follow us:

youtube.com/user/MitsubishiFAEU

twitter.com/MitsubishiFAEU

https://www.linkedin.com/showcase/mitsubishi-electric-europe-industrial-automation

https://www.instagram.com/mitsubishi_electric_fa_emea/

Press contact:

Mitsubishi Electric Europe B.V.

Industrial Automation

Silvia von Dahlen

Manager Marketing Communications

Mitsubishi-Electric-Platz 1

40882 Ratingen, Germany

Tel.:

Fax

silvia.von.dahlen@meg.mee.com

www.linkedin.com/in/silvia-von-dahlen