Cyber Resilience Act (CRA) at WEG

Industrial Motors

Commercial & Appliance Motors

Automation & Systems

Energy

Transmission & Distribution

Coatings

Cybersecurity and Digital Resilience

Driving efficiency and sustainability

Summary

1. Overview

In an increasingly digital and interconnected era, industrial infrastructures are becoming heavily dependent on integrated automation devices, such as frequency drives, programmable logic controllers (PLCs), human-machine interfaces (HMIs), industrial gateways, distributed control systems (DCSs), and other connected technologies. In this context, cybersecurity is no longer an option; it has become an essential requirement for ensuring the safe, reliable, and continuous operation of industrial systems.

As cyber threats continue to evolve, becoming more sophisticated and targeted, traditional and purely reactive security approaches have proven insufficient. New attack techniques emerge every day, requiring manufacturers, system integrators, and industrial operators to adopt proactive and resilient measures to protect their assets.

The increasing exposure of critical infrastructures to the Internet has led governments and regulatory bodies to establish cybersecurity regulations aimed at strengthening system resilience, that is, the ability to recover from cyberattacks, adapt to an evolving threat landscape, and continuously improve defense mechanisms while minimizing operational impacts and preserving business continuity. Achieving resilience requires not only the implementation of robust security controls but also the capability to anticipate, detect, respond to, and recover from cybersecurity incidents effectively. In this context, adopting a strong cyber resilience strategy is no longer a competitive advantage; it has become a business necessity for protecting industrial and mission-critical operations.

Several jurisdictions around the world have introduced regulations specifically addressing the security of industrial systems. In the United States, the NERC CIP standards establish stringent requirements for the protection of automation and control systems used in critical infrastructure. In the European Union, both the NIS2 Directive and the Cyber Resilience Act (CRA) impose direct cybersecurity obligations on manufacturers of digital products, including industrial automation equipment.

These regulatory initiatives are built upon internationally recognized standards and frameworks, such as the ISA/IEC 62443 series, the NIST Cybersecurity Framework, the ISO/IEC 27000 family of standards, and specialized guidelines such as IEC 62351, which focuses on securing industrial communication and automation protocols. Adopting these references enables organizations to mitigate significant cybersecurity risks, strengthen the security of automation devices, and enhance the resilience of industrial operations against sophisticated threats, ensuring the continuity of essential services and the integrity of the data and systems involved.

2. Beyond IT: The New Frontier of Cybersecurity

Traditionally, the term "cybersecurity" refers to the set of measures adopted to protect computer systems and networks against unauthorized access and malicious attacks. However, when applied to the context of industrial automation and energy technologies, the concept expands significantly. In these environments, cybersecurity encompasses practices aimed at ensuring the reliability, integrity, and availability of control and automation systems, principles commonly known in Information Technology (IT) as the "CIA" triad (Confidentiality, Integrity, and Availability).

In industrial environments, these measures are essential to prevent a wide range of risks, including the leakage of sensitive information, physical damage to equipment or systems, data corruption, and operational disruptions. Such incidents can compromise not only operational efficiency but also the safety and security of critical processes.

In traditional IT environments, confidentiality is typically considered the highest priority, followed by integrity and availability. In Operational Technology (OT) environments, however, this order is reversed: availability becomes the primary concern, followed by integrity and then confidentiality. This distinction exists because maintaining the continuous, safe, and reliable operation of industrial systems is often more critical than preventing unauthorized access to information. Any interruption to industrial processes may result in production losses, equipment damage, environmental impacts, or even risks to human safety.

3. Cyber Resilience Act (CRA)

The Cyber Resilience Act (CRA), formally referred to as Regulation (EU) 2024/2847, represents the European Union’s first horizontal regulatory framework specifically focused on the cybersecurity of products with digital elements. Its purpose is to establish a consistent level of security across the European market by requiring manufacturers to incorporate Security by Design and Security by Default principles, implement structured vulnerability management processes, and ensure the availability of security updates throughout the entire product lifecycle.

The regulation entered into force on December 10, 2024, initiating a transition period during which manufacturers, importers, and distributors must adapt their processes, products, and governance structures to meet the new requirements. An important milestone will occur on September 11, 2026, when the requirements for reporting actively exploited vulnerabilities and severe security incidents become mandatory, requiring formal mechanisms for monitoring, response, and communication with the competent authorities of the European Union.

As of December 11, 2027, the CRA will become fully applicable. By that date, all products covered by the regulation must demonstrate compliance with the essential cybersecurity requirements, maintain appropriate technical documentation, operate effective vulnerability management processes, and complete the necessary conformity assessments to obtain CE marking before being placed on the European market.

For manufacturers, the challenge extends beyond regulatory compliance. The CRA requires the establishment and maintenance of ongoing organizational capabilities related to product security, including secure development practices, continuous vulnerability monitoring, incident response coordination, security update management, and cybersecurity governance throughout the entire product lifecycle. For this reason, practical preparation should begin well before 2027, ensuring that processes, tools, and responsibilities are fully established when the requirements become mandatory.

4. Building a Resilient Future

Our mission of **"Continuous and sustainable growth while maintaining simplicity"** reflects our commitment to delivering technologies and solutions that promote a more efficient, connected, and sustainable world. This vision also guides our efforts to create digital and industrial environments that are safer, more resilient, and better prepared for future challenges.

We recognize that **cybersecurity** is essential to ensure the reliability, availability, integrity, and resilience of digital products, systems, and solutions. In an increasingly integrated industrial landscape, cyber protection must be considered continuously throughout the entire product lifecycle, from conception and development to operation, maintenance, updates, and support.

In this context, we are evolving our cybersecurity strategy based on two complementary pillars: on one hand, the progressive adoption of **Security by Design** and **Security by Default** principles in the requirements and functionalities of our products and solutions; on the other hand, the consolidation of a structured secure development process, with continuous maturity improvement in vulnerability management practices, incident response, and support for reliable operation throughout the entire product lifecycle.

In light of the entry into force of the **European Union's Cyber Resilience Act (CRA)**, we would like to inform you that we are actively engaged in the development and implementation of a structured **Vulnerability Management Program**, with the objective of fully complying with the requirements established by this regulation within the timelines defined for its application.

Among the main areas of activity of the cybersecurity team in relation to the CRA are:

- Publication of a single, dedicated point of contact for vulnerability reporting.
- Execution and coordination of the vulnerability management process.
- Coordinated response to cybersecurity incidents.
- Transparent communication with customers, partners, authorities, and other stakeholders.
- Continuous improvement of practices related to coordinated vulnerability disclosure.
- Risk management for connected products, third-party components, and industrial digital ecosystems.
- Strengthening operational and cyber resilience throughout the product lifecycle.

Our commitment goes beyond regulatory compliance. We strive to develop technologies that support safer, more resilient, efficient, and sustainable operations, contributing to the digital trust required for the industry and society of the future. This evolution considers regulatory requirements, recognized standards, and widely accepted best practices in the field of cybersecurity for connected products and industrial environments.

Every WEG project, product, and solution embodies our commitment to continuously advancing reliability, innovation, and cyber resilience, supporting our customers and partners in an increasingly connected and digital world.

The scope of solutions offered by the WEG Group is not limited to the products and solutions presented in this catalog.
To learn more about our portfolio, contact us.

For WEG's worldwide operations visit our website

www.weg.net

+55 47 3276.4000
cybersecurity@weg.net
Jaraguá do Sul - SC - Brazil

Code: 10014764152 | Rev: 00 | Date (m/y): 06/2025.