NEW EUROPEAN CYBER SECURITY REGULATIONS

NIS 2, RED, MR AND CRA AND THE ASEM JOURNEY

ASEM
A ROCKWELL AUTOMATION COMPANY

NEW EUROPEAN CYBER SECURITY REGULATIONS

AGENDA

EXECUTIVE OVERVIEW

A new European regulatory framework
From 2025 to 2028, RED Cyber Security, NIS 2, Machinery Regulation and Cyber Resilience Act will come into force, introducing increasingly strict technical, organizational and product requirements to ensure IT/OT security in industry.

Impact on companies and products
The regulations require risk management, stronger cybersecurity governance, advanced protections in digital and connected products, and the ability to demonstrate compliance through structured processes, certifications and secure updates.

The ASEM journey
ASEM is aligning its processes and products to international standards (ISO 27001, IEC 62443), strengthening its Secure Development Lifecycle, introducing SBOM, improving vulnerability management and collaborating with specialized partners for gap-analysis and security assessments.

Goal
To support customers and partners in the regulatory transition by providing secure, reliable and compliant solutions, reducing cyber risk on machines and plants and ensuring operational continuity.

EXECUTIVE OVERVIEW

NIS 2 is about corporate risk management
in the cybersecurity domain
→ End User ←

the **Machinery Regulation (MR)** is about
cybersecurity in machine physical safety
→ OEM / Integrators ←

the **Cyber Resilience Act (CRA)** is about
digital product cybersecurity
→ Suppliers ←

RED CYBER

RED CYBER SECURITY: WHAT IS IT

The Radio Equipment Directive (RED) – Cyber Security Art. 3.3

Updates the harmonized standards for radio equipment, including cybersecurity requirements for the categories and classes of Internet-connected radio equipment.
With the enforcement of RED Cyber Security (Art. 3.3), all products integrating Wi-Fi or Cellular features must comply with the new security requirements to maintain the CE marking.

RED Cyber Security on ASEM products

ASEM has conducted a full assessment of products with radio interfaces (Wi-Fi/Cellular) to define the compliance path for RED Cyber Security, identifying which devices need to be certified and which ones will be brought to end of life ahead of the new CE rules.

Deadline

- Effective date: August 1, 2025

RED CYBER SECURITY: WHICH PRODUCTS ARE AFFECTED

PRODUCT	STATUS
RK11 / RM11 4G Global	End of Life
RK21 / RK22	RED Certified
HMI40 / HMI50	End of Life - Wi-Fi and/or Cellular variants
BM122 / BM130/ BM131	End of Life
VK3500	RED Certified
ASEM 6300B-JB1AAD **ASEM 6300B-JB1BAD**	RED Certified

RED CYBER SECURITY: CERTIFICATION VALIDITY

RED Cyber certified products fall into two categories:

- Units manufactured before August 1, 2025
  Keep their CE marking without the need for RED Cyber Security certification.

- Units manufactured after August 1, 2025
  Are covered by the RED Cyber Security certification and the Declaration of Conformity (DoC) has been updated to include the new sections required by the regulation.

  The new DoC and the RED Cyber Security Certificate of Compliance are available on the ASEM website for each certified product.

NIS 2

NIS 2: WHAT IS IT

The Network and Information Security 2 (NIS 2)

Aims to improve cybersecurity in companies,
imposing stricter requirements for the protection of corporate networks and data.

Deadlines

- Effective date: January 1, 2025
- Deadline for security measures implementation: October 31, 2026

NIS 2: WHO IS INVOLVED

Who is a NIS 2 entity

A NIS 2 entity, whether Essential or Important, must adopt a structured approach to cybersecurity. NIS 2 is not a product certification, but a risk management-based approach. Security measures must be proportionate to the context, the criticality of the services and the potential impact of incidents.

Who is not a NIS 2 entity

NIS 2 extends cybersecurity responsibility also to the supply chain. Essential and important entities must assess and manage cyber risks coming from software and components used in their systems and plants by OEMs and integrators.

NIS 2: WHAT IS BEING ASKED

When the end-user asks the OEM/integrator:

Are you NIS 2 compliant?

They are not asking for a certification or an ISO checklist. They are actually asking:

If an incident happens,
can you prove that you properly managed
the cyber risk of the solution you provided to me?

NIS 2: HOW TO DEMONSTRATE RISK CONTROL

The end-user needs assurance that all four areas are covered:

1. Supply Chain Security and Software Development
2. Risk Management and Technical Measures (Access Control and Encryption)
3. Incident and Vulnerability Management
4. Audit, Monitoring and Business Continuity

ASEM provides a dedicated tool for OEMs and Integrators to generate the mitigation report on these four points

MACHINERY REGULATION

MACHINERY REGULATION: WHAT IS IT

The new Machinery Regulation (EU) 2023/1230, also known as Machinery Regulation (MR), replaces the previous Machinery Directive.

It introduces explicit cybersecurity requirements for connected machines.

Reason: a cyber attack can create a physical risk.

NOTE: This is a regulation that directly affects machine safety and the CE marking process.

Deadline

- Effective date: January 20, 2027

MACHINERY REGULATION: WHY CYBERSECURITY MATTERS

Even if the software is not a safety component,
it can become a risk vector, for example:

- Remote access that allows dangerous changes
- Communication with PLC or safety controller
- Unauthenticated or unencrypted protocols

That's why software falls under Annex III requirements

MACHINERY REGULATION: WHAT ANNEX III REQUIRES

The regulation in Annex III includes clauses like Art. 1.1.9 (Protection against tampering) and Art. 1.2.1 (Safety and reliability of control systems) which require:

- That remote connections or connected devices do not create hazardous situations
- That HW and SW are protected from accidental or intentional tampering
- That legitimate or illegitimate changes are detectable and traceable
- That critical software and data are identified and protected

This is not about IT security, but about machine protection

MACHINERY REGULATION: ROLES AND RESPONSIBILITIES

OEMs and Machine Builders

- Remain responsible for the CE conformity of the machine

Integrators

- Must demonstrate that digital components do not introduce risks

What does ASEM do?

- Designs products according to secure-by-design principles
- Ensures: strong authentication, encrypted communications, access management and logging
- Aligns the following products to Machinery Regulation requirements:
  - UBIQUITY, RK2x Router, FactoryTalk Remote Access, Stratix 4300
  - FactoryTalk Optix, OptixPanel, OptixEdge

Cybersecurity becomes part of the technical file.
ASEM provides components designed to support the CE marking process of the machine.

CYBER RESILIENCY ACT

CYBER RESILIENCE ACT: WHAT IS IT

- The Cyber Resilience Act (CRA) is a European regulation that:
  - Introduces mandatory cybersecurity requirements
  - Applies to hardware and software with digital elements
  - Is a necessary condition to obtain and maintain the CE marking

It is a product regulation, not an organizational one

Deadlines

- Vulnerability reporting obligation: September 11, 2026
- Effective date: December 11, 2027

CYBER RESILIENCE ACT: WHO IT APPLIES TO

- The Cyber Resilience Act applies to:
  - Hardware manufacturers
  - Software manufacturers
  - Suppliers of digital products that can be integrated into machines or systems

- The Cyber Resilience Act also:
  - Does not depend on the industrial sector
  - Applies to all connected products

CYBER RESILIENCE ACT: WHAT IT REQUIRES

- The CRA requires that the manufacturer:
  - Develops according to a Secure Development Lifecycle
  - Manage security updates for at least 5 years from the date of sale
  - Ensures software integrity
  - Ensures secure updates
  - Ensures protection from unauthorized access
  - Provides security information (e.g. SBOM)

CRA is therefore both a **product and** a **process regulation**.

Security becomes a continuous obligation, not a one-time check.

CYBER RESILIENCE ACT: REFERENCE STANDARDS

There are no harmonized CRA standards yet,
but the main references are:

- IEC 62443-4-1 for the development process
- IEC 62443-4-2 for product requirements
- ISO/IEC 27001 for governance

The CRA does not invent new concepts,
but makes them mandatory by law

CYBER RESILIENCE ACT: ROLES AND RESPONSIBILITIES

- OEMs must:
  - Use CRA-compliant components and avoid products that are not upgradable or not supported
- Integrators must:
  - Integrate products without weakening their security
    and not introduce configurations that cancel the protections
- What does ASEM do?
  - Designs hardware and software according to secure-by-design principles
  - Applies the Rockwell Secure Development Lifecycle (IEC 62443-4-1) to products relevant for the CRA
  - Integrates: secure updates, software integrity protection, vulnerability management and SBOM

ASEM provides products designed to support customers' CRA compliance.
Cybersecurity becomes a product requirement
and ASEM provides the right building blocks to address it.

WHAT HAS IEC 62443 TO DO WITH IT?

WHAT HAS IEC 62443 TO DO WITH IT?

- IEC 62443 is the family of international standards for cybersecurity of industrial automation systems (IACS), globally recognized and vendor-neutral

- For the Machinery Regulation (EU) 2023/1230, there is not yet a harmonized standard specific for machine cybersecurity, but IEC 62443 is indicated as the main reference to implement the security controls required by Annex III (Art. 1.1.9 and 1.2.1)

- For the Cyber Resilience Act, the main references are:
  - IEC 62443-4-1 → secure development process (Secure Development Lifecycle)
  - IEC 62443-4-2 → technical security requirements of the product (component level)

IEC 62443 will be, very probably,
the basis of harmonized standards for both CRA and MR

62443-4-2 CERTIFICATION ≠ MACHINERY REGULATION COMPLIANCE

⚠️ Using an IEC 62443-4-2 certified component in a machine
does not automatically make the machine compliant with the Machinery Regulation ⚠️

- The Machinery Regulation requires that cybersecurity
  is part of the overall risk assessment of the machine (Art. 1.1.9, 1.2.1),
  not that IEC 62443-4-2 certified components are used
  - A product with strong authentication is useless if the OEM leaves default credentials.
  - A product with encrypted communication does not protect if the integrator does not enable TLS/SSL.
  - A product with logging is not useful if nobody collects and monitors the logs.

The value is not in the certificate, but in the capability to put the machine builderin the condition to apply the cybersecurity capabilities of the product.

62443-4-2 CERTIFICATION ≠ MACHINERY REGULATION COMPLIANCE

- What really matters is that the supplier provides:
  - 📄 Clear and operational security documentation (hardening guide, security manual)
  - 🔧 Instructions to configure and enable the capabilities: authentication, encryption, access control, logging
  - 📋 Guidelines for the secure integration of the product in the machine or plant
  - 🛡️ Information for risk assessment: which threats the product mitigates, at which security level, and which responsibilities remain on the integrator side
  - 🔄 Vulnerability management and update processes that are accessible and documented

- A good supplier does not just deliver a certificate: it delivers the tools to build a secure machine.
- The responsibility of the CE compliance of the machine remains on the OEM/machine builder, but the component supplier has the duty to make the security capabilities practically applicable, not just declared on paper.

62443-4-2 CERTIFICATION ≠ CRA COMPLIANCE

⚠️ A product certified IEC 62443-4-2
is not automatically compliant with the CRA ⚠️

- IEC 62443 is a voluntary technical standard, the CRA is a mandatory European regulation. The CRA requires additional elements that the 62443 certification alone does not cover

Aspect	IEC 62443-4-2	CRA
Nature	Voluntary standard	Mandatory EU Regulation
Product technical requirements	✅ Covered	✅ Covered (partially aligned)
Vulnerability handling and reporting (24h/72h/14 days)	❌ Not covered	✅ Mandatory (Art. 14)
Post-market monitoring	❌ Not covered	✅ Mandatory
SBOM (Software Bill of Materials)	❌ Not covered	✅ Mandatory
EU technical documentation and conformity	❌ Not covered	✅ Mandatory (Annex VII)
EU Declaration of Conformity + CE	❌ Not covered	✅ Mandatory
Supporto minimo 5 anni	❌ Non previsto	✅ Mandatory (Art. 13(8))

APPENDIX

NIS 2 - ARTICOLI

Supply Chain Security and Software Development
The directive, at Art. 21.2.d and 21.2.e, requires ensuring security throughout the entire supply chain, demanding a rigorous assessment of both supplier reliability and the quality of ICT product development and acquisition processes.

System Hardening, Access Control and Data Encryption
The directive, at Art. 21.2.g, 21.2.h, 21.2.i and 21.2.j, requires securing industrial networks by enforcing strict logical and physical access control policies for assets. This includes the use of multi-factor authentication (MFA) solutions, solid cyber hygiene practices and the use of cryptography to ensure data integrity.

Vulnerability Management and Incident Response
The directive at Art. 23 and at Art. 21.2.b and 21.2.e requires clear procedures for the prevention, detection and management of incidents, including timely reporting of significant vulnerabilities.

Monitoring, Audit and Business Continuity
The directive at Art. 21.2.a, 21.2.c and 21.2.f, requires ensuring the resilience of business activities through risk analysis, continuous system monitoring, implementation of disaster recovery plans and procedures to regularly assess the effectiveness of adopted security measures.

MACHINERY REGULATION – ANNEX III

Art 1.1.9 – Protection against tampering

The machinery or related product shall be designed and constructed in such a way that the connection to it of another device, through any feature of the connected device itself or through any remote device communicating with the machinery or related product, does not lead to a hazardous situation. Hardware components that transmit signals or data, relevant for the connection to or access to software that is critical for the machinery or related product to comply with the relevant essential health and safety requirements, shall be designed so as to be adequately protected against accidental or intentional tampering. The machinery or related product shall collect evidence of a legitimate or illegitimate intervention on such hardware components, where relevant for the connection to or access to software critical for the conformity of the machinery or related product. Software and data critical for the machinery or related product to comply with the relevant essential health and safety requirements shall be identified as such and shall be adequately protected against accidental or intentional tampering. The machinery or related product shall identify the software installed on it, necessary for its safe operation, and shall be able to provide such information at any time in an easily accessible format. The machinery or related product shall collect evidence of a legitimate or illegitimate intervention on the software or of a modification of the software installed on the machinery or related product or its configuration.

MACHINERY REGULATION – ANNEX III

Art 1.2.1 – Safety and reliability of control systems

Control systems shall be designed and constructed so as to prevent hazardous situations from arising. Control systems shall be designed and constructed so that:

a) they can withstand, where applicable, circumstances and risks, intended service stresses and intended or unintended external influences, including reasonably foreseeable deliberate attempts by third parties leading to a hazardous situation;

b) a fault in the hardware or the logic of the control system does not lead to hazardous situations;

c) errors in the control system logic do not lead to hazardous situations;

d) the limits of safety functions are established as part of the risk assessment carried out by the manufacturer and modifications to settings or rules generated by the machinery or related product or by operators, including during the learning phase of the machinery or related product, are not permitted where such modifications could lead to hazardous situations;

e) reasonably foreseeable human errors during operation do not lead to hazardous situations;

f) the logging of data tracking generated in relation to an intervention and of safety software versions uploaded after the placing on the market or putting into service of the machinery or related product is permitted for five years after such uploading, solely for the purpose of demonstrating the conformity of the machinery or related product with this Annex in response to a reasoned request from a competent national authority.

Control systems of machinery or related products with an entirely or partially self-evolving behavior or logic and which are designed to operate with varying levels of autonomy shall be designed and constructed so as to:

a) not cause the machinery or related product to perform actions beyond its defined task and movement space;

b) allow the data related to the safety decision-making process for software-based safety systems ensuring the safety function, including safety components, to be recorded after the placing on the market or putting into service of the machinery or related product, and such data to be kept for one year after collection, solely for the purpose of demonstrating the conformity of the machinery or related product with this Annex following a reasoned request from a competent national authority;

c) allow at any time the correction of the machinery or related product in order to preserve its intrinsic safety.

CYBER RESILIENCE ACT - ARTICLES

Obligation Area	Description of the obligation for the software supplier	Regulatory References
Secure by design	Ensure that the software is designed and developed taking into account cybersecurity principles from the beginning, to minimize the risks of attacks and malfunctions from the time it is placed on the market. The product must not contain known vulnerabilities at the time of delivery. Implement secure default configurations (secure by default).	Art. 13(1); Annex I, Part I (points 1 and 2)
Risk assessment and documentation	Conduct and document a cybersecurity risk assessment of the product, considering its intended and reasonably foreseeable use, the operating environment and the assets to protect. Use the results of the assessment to determine which essential security requirements to apply and how to implement them. Keep this assessment updated over time (e.g. when new threats emerge or the product use changes).	Art. 13(2)-(4)
Due diligence on third-party components	Verify and ensure that included third-party components (software libraries, open source modules, etc.) do not compromise overall security. Responsible integration of open source: if non-commercial FOSS (Free/Open-Source Software) components are used, their security must be assessed and the manufacturer should possibly participate in their community to manage vulnerabilities.	Art. 13(5)

CYBER RESILIENCE ACT – ARTICLES

Obligation Area	Description of the obligation for the software supplier	Regulatory References
Vulnerability management throughout the lifecycle	• Establish internal processes for the timely discovery, reporting and correction of security vulnerabilities in the product and its components: Actively monitor known vulnerabilities (e.g. CVE) affecting the software or included components, and apply corrections (patches, updates) as soon as available. Adopt a Coordinated Vulnerability Disclosure policy to encourage reports from external researchers and users, and communicate this policy (e.g. provide a contact for security reports). • Maintain security logs and update the risk assessment as needed with new threat/vulnerability information.	Art. 13(6)-(8), (12) & (17); Annex I, Part II (all points)

CYBER RESILIENCE ACT - ARTICLES

Obligation Area	Description of the obligation for the software supplier	Regulatory References
Security updates and user support	• Ensure the availability of effective security updates (patches): Define and declare a support period during which vulnerabilities will be fixed and security updates provided. This period must take into account the expected useful life of the product and be at least 5 years unless the estimated product life is shorter. (For long-lived industrial software, it is advisable to provide even longer support, given the multi-year use in production plants.) • Make patches available in a timely, free and possibly automated way. Allow the user to be notified of updates and to install them easily (preferably over-the-air). Make sure that security updates are separate from any feature updates, so that the user does not have to purchase functional upgrades just to get security fixes. • Keep published security patches downloadable for at least 10 years from their release (even beyond the end of support, if support is < 10 years). • If a substantially modified new version of the software is released, ensure security (CRA-compliant) at least for the latest version; users of previous versions must be able to migrate to the latest version for free, without hidden costs (e.g. not charging additional licenses just because the patch needs to be installed on a new release). • Consider making previous software versions available in public archives (and warn users of the risks of using unsupported versions).	Art. 13(8)–(11); Annex I, Part II (points 6–9)

CYBER RESILIENCE ACT - ARTICLES

Obligation Area	Description of the obligation for the software supplier	Regulatory References
Technical documentation and conformity	Prepare the technical documentation (see Annex VII) before placing the product on the market, including the risk assessment and a description of how the product meets the security requirements. Subject the product to a conformity assessment (e.g. internal production control or, if it falls under "critical products", also EU-type examination or certification) according to the procedures indicated in Art. 32. Draft and provide the EU Declaration of Conformity and affix the CE marking before sale. Keep the technical documentation and declaration of conformity for at least 10 years after the product sale (or for the duration of support, if longer).	Art. 13(4), (12)-(14); Art. 13(20)
User information and support	• Provide end users with clear information about product security and its safe use: Accompany the software with usage instructions and security information (Annex II), including the specifics of the guaranteed support period (indicating the end-of-support date). Instructions must be clear and understandable, and remain available for at least 10 years from the product release. • Specify at the time of purchase (e.g. on the packaging, website or documentation) until when the product will receive security updates (e.g. "Support guaranteed until MM/YYYY"). Also, if possible, send notification to users when the support period is about to expire, so they are aware the product will no longer receive patches. • Clearly indicate the manufacturer's contact data (name, headquarters, email, website) on the product, packaging or documentation, and establish a single point of contact (e.g. a dedicated email address, a portal, etc.) where users can quickly reach out, especially to report security issues (vulnerabilities).	Art. 13(15)-(19); Annex II

CYBER RESILIENCE ACT - ARTICLES

Obligation Area	Description of the obligation for the software supplier	Regulatory References
Vulnerability and incident reporting	• In case of discovery of a critical security flaw already being exploited (vulnerability under active exploitation) or a serious cyber incident affecting the product: Within 24 hours of discovery, send an early warning through the designated ENISA/CSIRT platform, reporting at least the type of issue (e.g. exploited 0-day vulnerability, or cyber-attack incident). • Within 72 hours, provide a detailed notification with more precise information about the nature of the vulnerability/incident, the corrective actions taken and the mitigation measures recommended to users. • Provide a final report – within 14 days (for vulnerabilities) or 1 month (for incidents) – describing the vulnerability/incident, its severity, causes and impacts, and the corrective measures adopted (e.g. patch released). • Promptly inform product users about the vulnerability or incident and the actions they need to take (e.g. apply a security update, change configurations, isolate the system from the network, etc.). • If the manufacturer does not warn users in time, the coordinating CERTs can themselves disclose the existence of the threat. • Collaborate with authorities (ENISA, CSIRT, market surveillance) providing any additional information or follow-up reports upon request. • N.B.: These notification obligations come into force before the others: from September 11, 2026, also for products already on the market.	Art. 14(1)-(8); Art. 14(8); Art. 13(21)

THANK YOU

ASEM

A ROCKWELL AUTOMATION COMPANY