Compliance of INSEVIS Products with the Cyber Resilience Act (CRA)

1. Context of the Cyber Resilience Act (CRA)

The Cyber Resilience Act (CRA) is an EU regulation that defines mandatory cybersecurity requirements for products with digital components. The regulation aims to ensure that these products are securely designed, developed, operated, and maintained throughout their entire lifecycle. As a manufacturer of industrial automation technology, INSEVIS expressly supports the objectives of the CRA.
INSEVIS has established an internal vulnerability management and disclosure process that includes a vulnerability reporting infrastructure. SBoms for all products enable vulnerability monitoring on relevant portals. Each product has undergone a threat analysis, and recommendations for achieving CRA compliance have been outlined in the following sections.

2. IT Security and Integration Policy (CRA Compliance)

- **Product Status:** INSEVIS products are classified as legacy products. They include digital elements but do not natively support encryption protocols (e.g., transport encryption via TLS/HTTPS) by default.
- **Compensation Obligation:** To achieve a non-critical risk level in the overall system, the lack of product-specific hardening must be offset by an **isolated and protected system environment**.

3. Mandatory network encapsulation (compensation for lack of encryption)

Since data transmission between INSEVIS components is unencrypted, it is physically possible to intercept and manipulate data packets on the network. The customer must mitigate this risk by implementing the following countermeasures:

- **Physical or logical isolation:** Under no circumstances may the control system be connected directly to a higher-level corporate network (office LAN) or the Internet. It must be operated in a completely isolated OT network segment (VLAN in accordance with **IEC 62443**).
- **Use of Security Gateways:** If communication with external systems is required, the customer must install a dedicated security gateway (e.g., a VPN appliance or an industrial firewall with deep packet inspection) upstream of the controller. The data link must be encrypted (e.g., via IPsec or OpenVPN) on this gateway.
- **Protocol Whitelisting:** On the upstream firewall, only the unencrypted ports that are absolutely necessary for operation (e.g., Modbus/TCP, native fieldbus protocols) should be opened on a device-specific basis. All other network traffic must be blocked.

4. Enhanced physical and logical access controls

Since the component does not have modern identity and access management systems (such as MFA or role-based RBAC), access must be controlled at the system level:

- **Mechanical protection zone:** The control system must be installed in a locked control cabinet with a **protection rating of at least IP54** and a documented key system. Physical access must be restricted to authorized technical personnel..
- **Interface Protection:** Local service interfaces (e.g., serial ports, RJ45 diagnostic ports) must not be routed to the outside. They must remain inside the locked control cabinet.
- **Pre-authentication:** On-site operator stations (e.g., HMIs) that communicate directly with the unencrypted controller must have their own CRA-compliant user management system with password policies to prevent unauthorized command inputs to the controller.

5. Patch Management and Obsolescence Strategy

- **Limited Update Procedure:** For legacy products, firmware updates are primarily intended to address bugs and ensure functional stability. New security features (such as retroactive encryption) are not provided for this generation of hardware.
- **Risk Monitoring:** The customer is required to monitor the security advisories provided by the manufacturer and to adjust the upstream security components (firewalls/gateways) in response to newly identified threats**.**

6. Product Lifecycle and Support Periods (Lifecycle Data)

In accordance with the regulatory requirements of the Cyber Resilience Act (CRA), binding notices and deadlines apply to INSEVIS products. The customer must take this information into account in the risk analysis and operational planning for the overall system:

- **End of Sale (EoS) –**
  (As of this date, the component is no longer available for regular new sales.)
- **End of Life (EoL)**
  (Regular product support will be discontinued. Starting at that time, replacement parts will be available only on a limited basis.)
- **End of Support (EoS) – for Security Updates**
  (The manufacturer will provide critical security advisories and bug-fix updates until this date. After this date, technical support and software patches will no longer be provided. After this date, the entire system must be secured through additional measures taken by the customer, or the component must be replaced.)
- **Safe Decommissioning** with secure deletion of user data via "Factory Reset" for Linux-based devices or "Clear All + Delete IP" for OT devices running INSEVIS firmware.

7. Declaration of Conformity for the Entire System

Please note:

- CRA compliance does not replace system or machine responsibility. The CRA Implementing Regulation applies to the product and not to the entire machine system.
- The operator remains jointly responsible for safe configuration and operation. The customer (system integrator) is advised that compliance with this guideline is an integral part of the risk analysis for its entire system. Failure to comply with the encapsulation requirements will result in the loss of the presumption of conformity of the entire system with regard to the CRA requirements for non-critical system environments.

Erlangen, June 12, 2026

Jörg Peters
Baasansuren Sodnompil
Bastian Süß