

EU Cyber Resilience Act and CAN



(Source: Adobe Stock)

The EU Cyber Resilience Act (CRA) is the first European regulation to set a minimum level of cybersecurity for products comprising digital elements or software. CAN interface implementations comprise digital elements (protocol controllers) and software (e.g., higher-layer protocol stacks and application programs). Therefore, a system-and-application-risk assessment is required.

The CAN data link layer protocols (CC, FD, and XL) as standardized in ISO 11898-1:2024 as well as standardized higher-layer protocols such as CANopen CC/FD (CiA 301/CiA 1301) do not provide intrinsic cybersecurity measures. Cybersecurity measures can be added depending on the required security level (SL) as defined in the IEC 62443 standard series (security for industrial automation and control systems). Therefore, suppliers of CAN-connectable devices, vendors of products based on CAN networks, and CAN network designers need to evaluate, which SL is required by the targeted application.

Since December 11, 2024, the CRA is in force, applies in all EU Member States, and is implemented gradually. Starting June 11, 2026, Conformance Assessment Bodies (CAB) can assess the fulfillments of requirements. Starting September 11, 2026, vulnerabilities and security incidents must be reported to defined authorities within 72 hours. End of 2027, starting on December 11, all CRA requirements must be complied with.

The following CAN-connectable products do not fall under the CRA: free-of-charge open-source software, and nonprofit products. Additionally, medical products, vehicles, in-vitro diagnostic devices, civil aviation as well as marine equipment, and products used in the context of national security (e.g., military equipment) are not in the scope of the CRA, when specific cybersecurity-related EU regulations are in place.

EU regulations for medical device cybersecurity, primarily driven by the Medical Device Regulation (MDR) 2017/745 and In Vitro Diagnostics Regulation (IVDR) 2017/746, require manufacturers to implement "secure-by-design" principles across the entire product lifecycle. Compliance involves risk management for cyber threats, software validation, and adherence to updated MDCG (Medical Device Coordination Group) guidelines and the EU Cyber Resilience Act (CRA).

There are also other regulations in power, which you might need to be complied with, e.g., the U.S. FDA

(Food & Drug Administration) cybersecurity guidance for medical devices (Quality System Considerations and Content of Premarket Submissions). This guidance, issued summer 2025, adds Section VII to address FDA's recommendations regarding section 524B of the U. S. FD&C (Federal Food, Drug & Cosmetic) Act for cyber devices. This document supersedes the final guidance "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions," released September 27, 2023.

CANopen and security

CiA has a long history in developing security measures against unintended misuse as well as intended manipulation of CANopen communication. This covers also unauthorized access to CANopen devices and CANopen networks. There are password options for the CANopen object dictionary access. Furthermore, there will be an authentication signature option in CANopen messages specified, indicating that they are from the right origin and that in case of SDO (service data object) transmission, SDO segments belonging together and that they have not been manipulated. Some CANopen specifications already provide dedicated security measures, e.g., the CiA 710 generic CANopen bootloader or the CiA 417-1/CiA 814-1 CANopen lift bootloader.

According to the OSI (open systems interconnection) model, security controls can be applied to each of the seven OSI layers, depending on the required SL and expected attack scenarios. This is defined in the ISO 7498-2:1989 (Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture) framework. For the CAN XL data link layer, CiA members are developing the CANsec (EU trademark by CiA) approach, a cybersecurity extension specified in CiA 613-2 (CAN XL add-on services — Part 2: CANsec data plane). This CiA technical document is expected to be released this year.

hz

CiA board-of-directors statement

The CiA board of directors, Magnus Hell (Infineon), Christian Schlegel (CHS Consulting), and Holger Zeltwanger, has worked out the following statement, evaluating the EU CRA regulation and impacts on CAN networks:

The nonprofit CiA (CAN in Automation) international users' and manufacturers' group informs its members that products using CAN and placed on the EU markets fall under the European Cyber Resilience Act (EU CRA), unless the relevant cybersecurity aspects are covered by application-specific EU legislation. In most cases, the required risk assessment may be a self-assessment, unless the product is considered critical (as defined in the CRA Annex III).

It remains to be seen, which future standards best reflect the EU CRA requirements. For now, suppliers of CAN-connectable devices are requested by their customers to comply with a dedicated SL (security level) as defined in the IEC 62443 standard series (security for industrial automation and control systems).

CiA is confident that SL 2 can often be reached with minimal effort for CAN networks. Achieving SL 3, requires more advanced security measures involving cryptography at CAN data frame (data link layer entity) or CANopen message (application layer entity) level. CiA's assessment is that CAN networks with restricted and limited physical access usually comply with SL 2 or lower, not needing additional cybersecurity measures. This assumes that gateway functions to other networks and external interfaces are protected by means of firewalls or are made not accessible (e.g., the JTAG interface, named after the Joint Test Action Group).

If restricted and limited physical access is difficult to enforce, cybersecurity measures do not necessarily require cryptography. In CiA's view, a security monitoring entity that scans communication on abnormal behavior, detecting and reporting attack, is an efficient security measure as indicated in the CRA regulation and the IEC 62443 standard series. It reduces overall risks for undetected attacks, having a positive influence on the risk assessment and showing a defense in-depth approach.

If cryptography is necessary, its use can be limited to core functions. While a secure software update mechanism might be mandatory for CRA compliance, in many cases, further use of security functions can be reduced to secure CAN node authentication and device configuration protection (e.g., by means of passwords). Such core security functions are currently under discussion in the CiA SIG (special interest group) HLP (higher-layer protocol) cybersecurity and expected to be integrated into CANopen CC and CANopen FD specifications.

hz