(Source: Adobe Stock)

EU Cyber Resilience Act: The clock is ticking

For manufacturers, importers, and distributors of any hardware and software "with digital elements" there is a countdown running. If your business involves systems using CAN, then the EU Cyber Resilience Act (CRA) is no longer a distant annoyance, it is a reality with fixed deadlines fast approaching.

By December 11, 2027 products "with digital elements" must fully comply to the CRA, but as soon as September 11, 2026 the vulnerability reporting starts.

We heard from several machine builders and integrators who use CAN or mixed-network devices from multiple suppliers that, although they began their CRA compliance work some time ago, they will just barely meet the deadlines. So, if you have not yet started your CRA compliance work for CAN-based products, there's no time to lose.

One common misconception is that the CRA only applies to newly developed products. Well, if that is your perception, you should review the exact wording used in the CRA.

Vulnerability reporting and handling

In September 2026, the vulnerability handling and reporting (Article 14) for affected products, including those that are already on the EU market according to Article 69(3), will become mandatory.

The specific obligations linked to vulnerability reporting and handling follow strict timelines. Depending on the severity of the vulnerability and whether it is actively exploited, you are expected to react within 24 or 72 hours after becoming aware of the incident with a final report due within 14 days or a month, respectively. What "becoming aware" means is currently a point of debate. While some say it is the time at which you receive the report, others will claim that you have to have some reasonable processing time to review and confirm the report first.

What if you get several reports on Friday night? Unfortunately, there is no easy answer, but if you have your processes in place and can provide documentation to demonstrate that you made a reasonable effort to work on the reports in a timely manner, you should at least be in a better legal position.

If in the worst case the vulnerability requires a software or firmware fix, which you aren't able to provide through appropriate mitigations or secure updates, you would have to withdraw your product and issue an advisory to your customers to stop using it.

A disclaimer: We are no lawyers and this is no legal advice, but our CRA interpretation is as follows: Even if you have a product that has been out on the European market for many years already and you become aware of a serious security vulnerability, to avoid potentially harsh penalties you will still have to follow the vulnerability and reporting procedures as they apply to the entire "active use" period. To make matters worse, even declaring a product "end-of-life" may not always free you from all of that burden. Think of "ancient" Windows versions often still used beyond their security update period. If you learn of a new severe vulnerability for a discontinued product and it is still in "active use" then you probably still have to score and report it.

For more details on the specific timelines and terms see Article 14 of the CRA and for details on the CVSS (Common Vulnerability Scoring System) for CAN products see the white paper "EmSA-WP-103", available on our website.

Full CRA compliance by December 2027

Starting in December 2027, the CRA fully applies to all hardware and software products "placed on the EU market" which in EU language refers to individual units made available for distribution or use. Therefore, if after December 2027 you produce a new batch of a product you have been selling the same way for years, still in the eyes of the EU you "place them on the market" and therefore the CRA is in full force. Transitional exceptions only apply to units already delivered to distributors or customers before the deadline.

Obviously, you will not be able to fully claim "security by design" for such products. Nevertheless, you must make a real effort to show (and document) that you have taken all CRA requirements into consideration and that you provide your customers with all details needed to operate your product securely. This includes a risk assessment and detailed documentation on how to prevent potential attack scenarios.

For traditional, CAN CC (classic) nodes this means including a disclaimer, stating that the CAN communication is unprotected and as such does not provide confidentiality or protection from data manipulation. Therefore, when integrating the device into a larger system, adequate additional protection must be carried out and a risk assessment for all components of the larger system is warranted.

Some measures that may follow such an assessment: All logical and physical access points to the nodes and the CAN cabling must be protected. Minimize the use of gateways to other networks. Where such gateways are needed, add firewall functionality ensuring only authorized access gets through. To protect the physical access, ensure that nodes and CAN cabling are well hidden behind locked panels or cabinets.

Risc score still too high?

Consider adding a security monitoring and logging system (see Figure 1), which by itself can fulfil two CRA requirements. Especially in CAN systems with pre-determined configurations and very predictable timing such monitoring can be used to detect security anomalies such as:

- Unusual number of resets;
- Re-configuration during operation;
- Deviations in the timing patterns.

If reported to the upper control level via a dedicated communication channel, such detections can directly trigger a security alert with appropriate warnings or actions.

See our white paper "EmSA-WP-101" to learn more on how to justify minimal or lightweight security options for CAN systems.

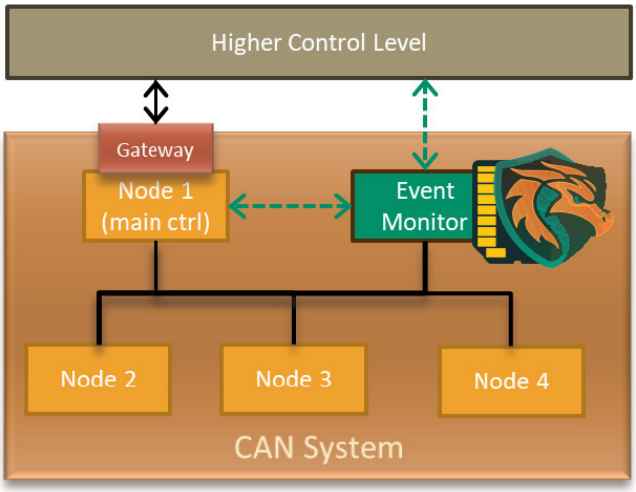

Figure 1: A security event monitor and logger for CAN systems reporting anomalies to a higher control level (Source: Embedded Systems Academy)

How much documentation is required by CRA?

Annex I of the CRA outlines the essential security requirements that must be documented, including how each has been addressed. However, additional requirements are scattered throughout its other articles as well. A big portion of the overall documentation goes to the risk assessment. There is no specific assessment method required, so if you already use risk assessments for safety reasons, it probably makes sense to re-use the method already established. Otherwise, for CAN based systems, we recommend an IEC 62443 aligned risk assessment.

As part of our consulting and training activities we have developed various templates. Together, the ones for documentation have more than 100 (sub)chapters that you need to fill with the specifics relating to your product. Even for a simple CAN-based I/O node the CRA related documentation can easily reach more than 100 pages. However, assuming your production and test processes are already well documented, you will be able to re-use or link to existing documentation.

When and where to use cryptographic protection?

One of the essential CRA requirements is a secure update path, which requires cryptographic protection. The minimal security level generally accepted for the update file is AES-GCM protection (encrypted and authenticated) based on a pre-shared key. Even on many embedded devices with performance constraints this is achievable, especially when update cycles happen in a maintenance mode and not during regular operation.

But how about a fully running system during regular operations? As mentioned earlier, the most straightforward security measure for traditional CAN systems is external protection by restricting physical access as much as possible. It should be addressed first, before considering more complex measures. Still, not every system can be secured this way. Systems in remote or even public locations or with many (trusted?) persons having easy access are especially vulnerable. It might only take a few seconds to attach some hidden CAN wireless interface giving an attacker full CAN-level access and, on an unprotected bus, to almost "everything". Securing the CAN network on the data link layer (ISO/OSI layer 2) itself is challenging. While CAN FD (flexible data rate) has frame sizes large enough that we can reserve a few bytes for security overhead including some authentication tag, CAN CC does not offer any "realistically adequate room" for it.

Therefore, for CAN CC systems it makes more sense to add security at a higher protocol level. The CiA IG06 SIG02 HLP Cybersecurity (IG: interest group; SIG: special interest group) is currently in the process of defining various security-related functions, such as:

- Selection of standardized cryptographic primitives;
- Option to securely read/write security-related (CANopen) object dictionary entries;
- Option to lock/unlock an (CANopen) object dictionary to protect it from unauthorized re-configuration;

Related publications

- EU Cyber Resilience Act: Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024
- EmSA-WP-101: Security Justification for Classical CAN Systems
- EmSA-WP-103: Common Vulnerability Scoring System (CVSS) for CAN

- Option to read an authenticated node identification;
- Recommendations for security event monitoring and logging.

All of the above are defined for both CANopen CC and CANopen FD and limit secure communication with security overhead to a few selected transfers. A combination of these functions significantly lowers the risk scores in a system-wide risk assessment. During the startup process, an entity on the network can verify the authenticity of all connected devices and verify that all configurations are locked before switching to full operation. During operation, security system monitoring may include a cyclic re-check of the authenticated node identification. While an attacker could possibly still introduce individual injected frames, the security monitoring entity would recognize those posing a threat, allowing for an appropriate reaction to such an attack.

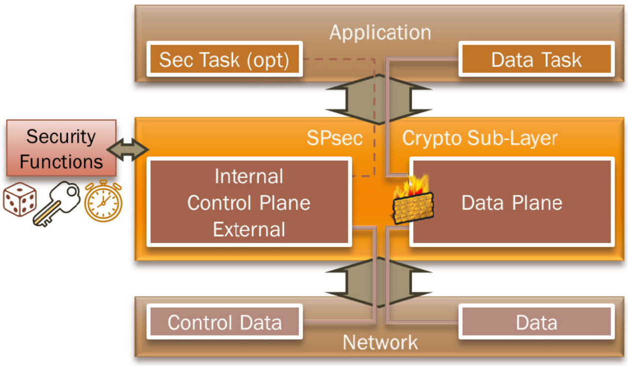

Figure 2: The SPsec crypto sublayer securing all CAN FD communication independent from the application (Source: Embedded Systems Academy)

If an instant reaction is required, like discarding frames that fail authentication, then cryptographic methods indeed need to be applied at the beforementioned lower level. Hochschule Offenburg and we at Embedded Systems Academy have jointly developed SPsec for that purpose – a security system for small-packet networks (see Figure 2). Its mapping to CAN FD supports a crypto sublayer securing all CAN FD communication, including confidentiality and authenticity. In our prototype implementation the maximum payload size per CAN FD frame is set to 48 byte to provide room for security overhead. SPsec for CAN FD is compatible with CANopen and J1939, as well as their FD variants.

Ultimately, the choice of which security measures or mitigations to apply depends entirely on the individual risk assessment. While many manufacturers of individual CAN products may be able to shift much of the security responsibility to the integration level, CRA-compliant documentation is still required. If you're the system integrator, talk to your suppliers early. The more detailed information they give you, ideally beyond what the CRA demands, the easier your system-wide risk assessment and documentation will be. ◀


Authors

Olaf Pfeiffer, Christian Keydel
Emsa (Embedded Systems Academy)
info@esacademy.com
www.esacademy.de

Editorial

"Nothing is as bad as it looks"

The Cyber Resilience Act (CRA) has made some CAN-networked device suppliers nervous. They do not know how to react. Some are moving around, starting to develop security measures. Other are quiet and wait – this is not that bad. A rabbit in front of a snake should also not move fast. Snakes cannot see quite well, but they can recognize movements.

Of course, the CRA requests security audits – no doubts. A system designer should evaluate risk and threat assessments. From these audit results, cybersecurity measures should be selected and implemented. These cybersecurity measures can also be requested from device suppliers.

From talks with German notified bodies, CiA learnt that "nothing is as bad as it looks". They will not be able to certify every CAN-connectable device. They do not have the resources to do so. In many cases, it is sufficient to evaluate the possible attack scenarios and to implement basic cybersecurity measures or none (if not needed). Documentation of security audits should be available as well as optionally implemented measures. In some cases, sophisticated measures might be needed. CiA is working on different cybersecurity measures: CANsec for CAN XL networks and on a generic higher-layer protocol security approach (including for CANopen FD). Additionally, CiA specifies the adaptation of Ethernet-based security measures (e.g., MACsec) for CAN-based networks (Ethernetification of CAN).

My recommendations: Start with security audits and evaluate basic security measures; participate in the security-related CiA technical groups and talk to notified bodies, what they require. Most important seems to be a secure bootloader.

Holger Zeltwanger