Interface Driven Security Evaluation for Sensors

The Impact of Sensor Interfaces like SPI, I2C, CAN and others on Cybersecurity Measures

White Paper EmSA-WP-102

Version 1.00
28 July 2025

Jointly authored by

Embedded Systems Academy GmbH
Bahnhofstraße 17
30890 Barsinghausen
Germany

Embedded Systems Academy, Inc.
84 W. Santa Clara St., Suite 700
San Jose, CA 95113
United States

www.em-sa.com

Contents

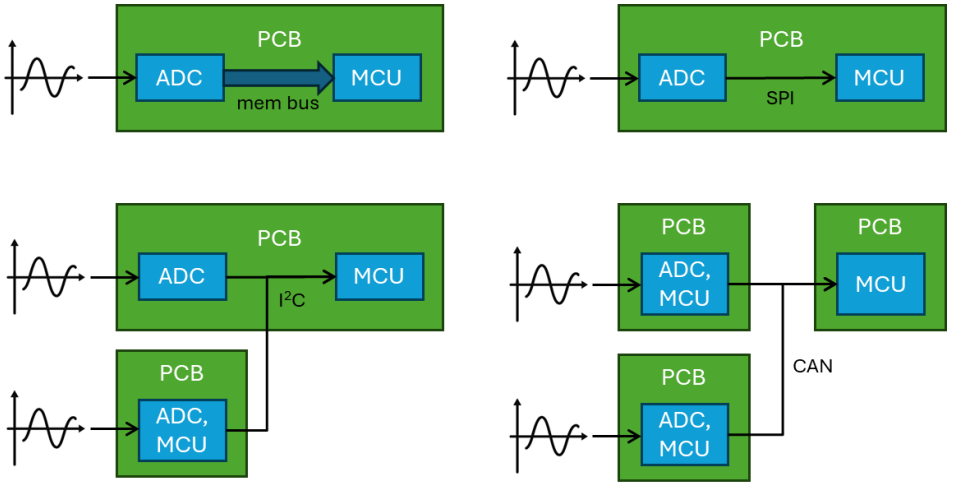
1 Scope and Objective

This document investigates how the choice of communication interface for an embedded sensor affects its EU Cyber Resilience Act (CRA) compliant cybersecurity evaluation and risk assessment. Using an analog sensor (e.g., for a temperature) as a guiding example, the document traces the evolution from a basic ADC (analog to digital) input to a fully networked IoT node. We assess the impact of interface selection on security requirements looking at interfaces from a parallel data memory bus via serial connections to a fully integrated IoT sensor.

This analysis is aligned with the requirements of the CRA, which mandates a risk-based, lifecycle-aware approach to cybersecurity. The goal is to help developers and evaluators judge when and why specific CRA requirements become applicable and when physically enforced security or lightweight security solutions are sufficient.

2 Interface Scenario Options

In this chapter we outline common “data collecting” interfaces typically used with sensors producing an analog value, like a temperature. At some point there is an analog to digital converter (ADC) involved that produces a digital representation of the data measured/collected and that is transferred on to some “processing unit” like a microcontroller (MCU) that works with the data and/or sends it on.



2.1 Parallel Data Memory Bus Interface

This interface is shown top left and is limited to very short distances directly on a PCB. The ADC chip and the receiving processor are in close proximity. Depending on the width of the data interface, typically 8 or 16 data lines and a few control lines are directly connecting the two.

2.2 Serial interface like SPI or I^2C

Many ADC chips are available with a standardized serial interface like SPI or I^2C, shown top right and bottom left. The maximum distance between the sensor producing the data and the processor receiving the data depends on the bitrate in use. SPI communication is typically limited to the same PCB whereas some I^2C implementations can support a distance of 1 meter or more allowing off-PCB communication. Both SPI and I^2C can handle multiple connected devices. SPI requires one additional chip select signal for each device while I^2C is a bus system supporting addressing the connected devices without the need of additional signal lines.

2.3 CAN and other non-IP Fieldbusses

These interfaces typically require an MCU on both the transmitting and the receiving end. While it is possible to use CAN also for on-PCB communication, the more common use case is that each CAN node sits on its own PCB, clearly physically separated from the other nodes.

The Firmware in the MCU collects the data from the ADC, which could also be MCU integrated or connected through a method described in the previous 2 sections, and forwards it via CAN to the next higher control level. Depending on the CAN bitrate this could be tens to hundreds of meters away.

Beyond CAN, a variety of other fieldbus systems such as Modbus RTU and Profibus are commonly used in industrial applications. Like CAN, these interfaces are not IP-based and typically use serial or differential signaling lines. Most of these protocols require dedicated interface hardware or protocol converters, often integrated into microcontrollers or gateway devices.

For the scope of this document we focus on CAN as a representative for this category.

3 Security Implications

From a security evaluation standpoint, memory bus, SPI, I²C, and CAN interfaces share many common characteristics.

3.1 No Direct Internet Access

None of these interfaces provide or imply direct Internet access. Any such external connectivity can only be introduced through the addition of a gateway or similar interface. Once a gateway is added, it forms a clear trust boundary. The responsibility for securing any Internet access rests entirely with this gateway.

Regardless of the local security mechanisms implemented between the gateway and the ADC or sensor, they cannot prevent compromise if the gateway itself is breached, as full access is already granted. A compromised gateway with full access rights to the sensor will retain that access, rendering any downstream security measures ineffective in preventing misuse. Therefore, in risk assessments concerning Internet-based threats, the only relevant targets are Internet-connected access points or gateways. The technology or protocol used on the local, non-IP side of that interface (whether memory bus, SPI, I²C, or CAN) becomes irrelevant in this context.

In a CAN system with an Internet-connected gateway, the cyber risk associated with that gateway exceeds the combined risk of all physical access-based attacks.

3.2 Physical Attacks

What remains then is the evaluation of physical attack vectors. These are scenarios where an attacker gains either time-limited or even unlimited physical access to the system. In such cases, the attacker may have access to not only the local interface lines but also to debugging ports, and may attempt side-channel attacks. Such a physical access scenario significantly narrows the attack surface. While Internet-based attacks can target large numbers of devices simultaneously that share common hardware and software, physical attacks are limited to one system at a time.

When comparing the local interfaces in the context of physical attacks, the key differences lie in the ease of signal access, interpretation, and manipulation. Attacks on a memory bus require a high degree of determination and technical capability. In contrast, for I²C and CAN, off-the-shelf tools exist that can passively interpret traffic or even inject and manipulate data on the bus. This means that the critical factor in evaluating risk is how physically accessible the signals are. Are they confined to a printed circuit board

within a sealed device? Or are they routed through exposed wiring in a field environment? And how many individuals have potential access to these points?

3.3 Attacker Capabilities & Motivation

The IEC 62443 standard defines four security levels where the effectiveness of physical access limitations depends on the attacker's motivation and resources. For Security Level 4, attackers are assumed to have significant capabilities, such as those associated with nation-state actors (e.g. a secret service).

While physical access protection of a CAN system might be sufficient to reach Security Level 2, it will be insufficient to protect from attacks at Security Level 3 and 4.

Another challenge in CAN system security is the transfer of high-level attack capabilities to lower-level attackers. A market exists for portable CAN intrusion tools that, to some extent, are legally available. These tools are often marketed with slogans like: “Lost your car keys? No problem. Just connect to a few wires behind the headlight and unlock and start your vehicle, no key needed.” Only in the fine print is it stated that such tools must be used exclusively on your own vehicle.

Such devices enable attack techniques typically associated with highly capable adversaries (Security Level 3 or 4), yet they are accessible to individuals with only Security Level 2 skills or motivation. This disconnect between assumed attacker profile and available tooling complicates risk-based decisions.

4 Access Limitations and Mitigations

4.1 Deeply Embedded

In a well-protected CAN-based system where cables are fully enclosed (like within sealed machinery) and access is tightly controlled and limited to a small number of authorized personnel, no additional security measures are needed on I^2C or CAN level. This is consistent with the evaluation applied to memory bus interfaces, for which security mechanisms are generally not considered necessary under physically enclosed conditions.

4.2 Partly Exposed

A more vulnerable case arises with partially exposed CAN systems. For example, a construction machine parked in public might have CAN wires accessible behind removable parts such as headlights. Or in a building automation scenario, CAN cables might be located behind cover plates of switches or buttons. In such cases, a single prebuilt CAN intrusion device, such as those already used in automotive hacks, could be used to compromise all machines or installations of the same type.

4.3 Selection of Mitigations

To address these risks, simple yet effective countermeasures include the use of time-determined CAN messaging combined with communication monitoring. Injection or replay attacks would alter message timing and could be detected.

For higher assurance, a system-specific authenticated communication object, such as a cryptographic heartbeat, can be introduced. This allows regular integrity verification without encrypting the entire CAN traffic.

If the sensor data has high value, for instance in a chemical process involving a proprietary recipe, state-of-the-art cryptographic protection including encryption and authentication should be applied to ensure conformance with Security Level 3 protection objectives.

For a more detailed list of non-cryptographic and lightweight security measures, see our white paper: EmSA-WP-101 Security Justification for Classical CAN Systems.

5 Alignment with Standards and Regulations

The security evaluation approach presented in this document aligns with the principles and expectations set out in the following standards and regulations:

5.1 IEC 62443

IEC 62443 provides a comprehensive framework for securing industrial control systems. This document follows its core concepts, particularly:

- **Zone and conduit model:**
  Local interfaces such as memory bus, SPI, I²C, and CAN can be placed in trusted zones if physical access is restricted.
- **Security Levels (SL1–SL4):**
  The evaluation method reflects the SL concept, where the required protective measures depend on the attacker's capability and motivation.
- **Defense-in-depth:**
  Interface exposure is assessed within a layered model, supporting decisions on whether additional controls such as monitoring or authentication are necessary.
- **Omitted measures:**
  The justification of omitted measures for low-exposure interfaces follows the secure design and justification requirements from 62443-4-1 and 62443-4-2.

5.2 ISO/IEC 27001 and 27005

ISO/IEC 27001 and 27005 provide a structured framework for establishing, maintaining, and continuously improving information security through risk management. While these standards are not specific to embedded systems, they offer valuable guidance when sensor data forms part of a larger information system or enterprise architecture. In the context of this document, ISO/IEC 27005 supports:

- A structured risk assessment methodology, which complements CRA's risk-based requirements.
- The classification of assets, threats, and vulnerabilities, including those associated with physical interfaces.
- Justification for the chosen level of mitigation, especially when opting for lightweight or physically enforced security.
- For sensor systems integrated into broader IT or OT infrastructures, applying ISO/IEC 27001 ensures that security risks related to interface exposure are addressed consistently with organizational policy and lifecycle controls. This also strengthens alignment with CRA which requires documented risk assessments and conformity justification.

5.3 EU Cyber Resilience Act (CRA)

The CRA mandates a risk-based, lifecycle-focused approach to cybersecurity for all products with digital elements. This includes embedded sensors with communication interfaces. This document supports CRA compliance by:

- Providing justification when CRA Annex I security requirements (e.g. secure communication, access control) do not apply, based on physical enclosure and interface classification.
- Identifying when risk becomes non-negligible due to partial exposure, triggering the need for technical mitigation.
- Supporting conformity assessment and internal documentation (Art. 20/21 CRA) with clear rationale based on interface types and system integration context.

6 Summary & Conclusion

The choice of interface technology for embedded sensors has a direct impact on the applicable cybersecurity requirements under the EU Cyber Resilience Act (CRA) and related standards. However, this impact is not determined by the interface like memory bus, SPI, I²C, or CAN, but by the level of exposure it has.

Interfaces without direct Internet connectivity can be considered part of a trusted zone, as long as their physical access is restricted and the system design clearly defines a trust boundary. In such cases, minimal or no additional security measures are justified, unless high security levels need to be reached.

If the interface signals become (intentionally or unintentionally) externally accessible, it becomes a potential attack surface and must be assessed accordingly. Depending on the required security level one or multiple mitigations should be applied.

Property	Memory Bus	SPI	I²C	CAN
Signal Length	<10 cm / PCB	<30 cm / PCB	~10 cm – 2 m	~0.5 – 500 m
Number of Wires (Typical)	16 dat + ctrl	3 + select	2	2
Ease of Sniffing (if exposed)	Hard	Medium	Easy	Easy
Ease of Injection/Manipulation	Hard	Medium	Easy	Easy
Hot-Plug Friendly (to attack unit)	No	No	Limited	Yes
Attack Detection Support	None	None	None	Possible by SW
Cryptography Usable	No	No	No	Limited
Max SL (Physical only)	SL3	SL2	SL2	SL2
Max SL (Lightweight Crypt)	n/a	n/a	n/a	SL3

The table above shows a summary of the security related properties of each interface. Green cells indicate properties with a positive (security) effect.

- Shorter signal length translates to a literally smaller attack surface.
- For serial busses diagnostic devices are usable for sniffing or injections.
- CAN allows for several software-based detection methods to identify injection or replay attacks.
- Cryptographic methods can be applied on CAN but are limited by frame size and bandwidth.

For a more detailed list of non-cryptographic and lightweight security measures, see our white paper: EmSA-WP-101 Security Justification for Classical CAN Systems.