Security Justification for Classical CAN Systems

Justification for Using Lightweight or Non-Cryptographic Security Measures

White Paper EmSA-WP-101

Version 1.00
15 May 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 reviews the security requirements and implementation decisions for a CAN system based on classical CAN using frames with a maximum payload of 8 bytes. It is intended for auditors evaluating the system's compliance with industry-standard security frameworks, particularly BSI TR-02102 and IEC 62443. The document provides a justification for employing non-cryptographic security mechanisms and potentially only lightweight cryptographic mechanisms in the internal CAN network while maintaining an overall secure architecture.

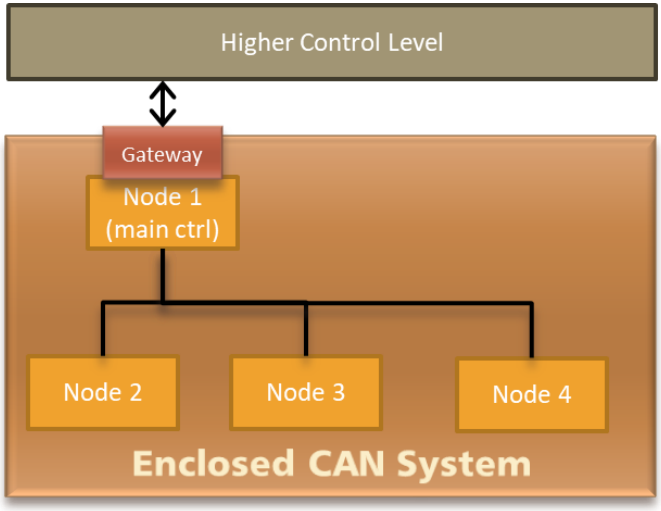
This document addresses only selected CRA requirements for which non-standard or reduced measures are justified and does not attempt to demonstrate full CRA compliance.

Nr.	Security Requirement
1	Cyber risk assessment, security by design
2a	Deliver without vulnerabilities
2b	Secure default config, reset to default
2c	Fix vulnerabilities with security updates
2d	Protect from unauthorized (user) access
2e	Protect confidentiality of data: at-rest, in-transit
2f	Protect integrity of code, config, data: at-rest, in-transit; report corruption
2g	Personal data minimization
2h	Protect availability, system resilience
2i	Minimize own negative impact
2j	Minimize attack surfaces / interfaces
2k	Minimize impact of an incident, defense in depth
2l	Protected cybersecurity event log
2m	Decommission, remove all data

This document focuses on the highlighted security requirements 2b, 2e, 2f, 2h, 2j, 2k and 2l.

2 System Overview

The control system comprises a main control unit that communicates with multiple embedded devices over a classical CAN, J1939 or CANopen network and has a second communication channel to a higher control level. The communication with the higher control level is not in the scope of this document.

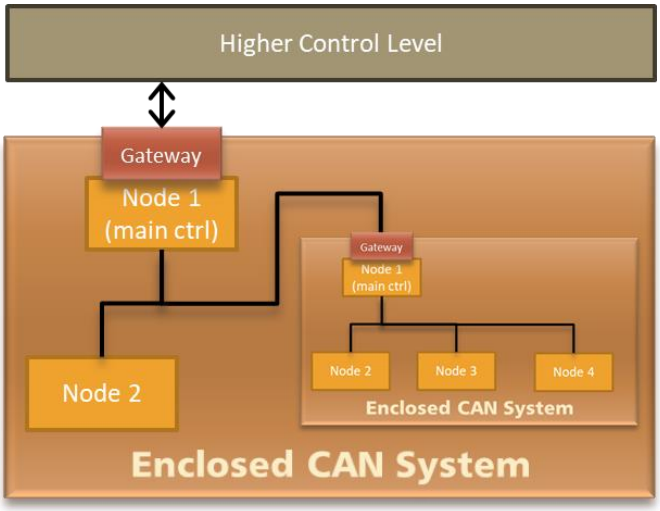


The communication consists of service, network management and process data communication. Process data communication is frequent and has real-time requirements. Service data communication is infrequent and typically happens during system startup or maintenance. Network management communication includes system startup commands, emergencies or alerts and heartbeats.

The internal CAN network is deeply integrated into the machinery and is entirely enclosed, with all cables, connectors, and devices concealed behind locked service hatches and inaccessible without dismantling secured covers. This setup significantly restricts unauthorized physical access and effectively protects against tampering through physical isolation.

2.1 Cascaded System

Complex control systems may use several such CAN systems as subsystems. In such a case, the subsystem uses classical CAN, J1939 or CANopen also on the next higher control level.



The justification in this document also applies to the control level incorporating a subsystem using classical CAN, J1939 or CANopen communication.

Examples for such subsystems are a electrical power bank with multiple batteries and a charge/discharge controller or an engine driven power generation pack.

3 Security Objectives

In alignment with IEC 62443 and BSI TR-02102, the following objectives are addressed:

- Defence in depth and least privilege
- Protection against unauthorized physical access
- Authentication of nodes
- Integrity of communication between devices
- Timely detection of anomalous activity

4 Rationale for Non-Cryptographic Measures

The use of multiple non-cryptographic measures justifies limiting the cryptographic methods.

4.1 Physical Access Control

- The CAN network is not externally exposed. All wiring is internally routed and physically secured behind locked panels.
- Tampering would require unauthorized access to service compartments, which is restricted under normal operational and service conditions.

IEC 62443-3-3 Reference:
SR 1.1 (Physical access control)

4.2 Denial of Service (DoS) Considerations

- For systems using CAN or CANopen, physical tampering – such as cutting or shorting the bus – constitutes a Denial of Service (DoS) and cannot be prevented by cryptographic means. In such embedded environments, traditional zoning and redundancy offer limited benefit due to the small number of interdependent nodes; loss of even a few devices may render the system inoperable.
- The primary defence against DoS in this context is physical access control. Given that all wiring is secured behind locked service hatches, unauthorized tampering is difficult and can be detected through physical inspection or timing anomalies.

IEC 62443-3-3 Reference:
SR 7.2 (Fail securely),
SR 5.2 (Zone boundary protection)

4.3 Confidentiality Not Required

- No data transmitted over the CAN network requires confidentiality. Data is either operational control data or status information that has no exploitable value in isolation.

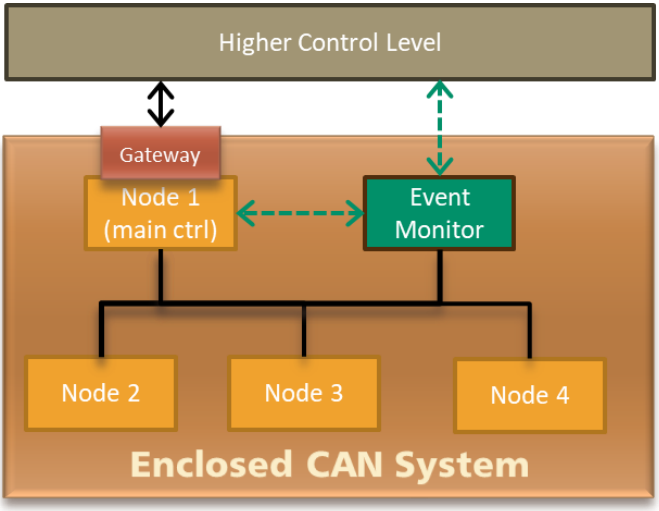
IEC 62443-3-3 Reference:
SR 3.4 (Use of encryption based on confidentiality needs)

4.4 Minimizing and Securing External Interfaces

- Every interface or gateway to other networks enforces state-of-the-art cryptographic security (e.g., TLS, SSH, or similar protocols).
- The number of such interfaces or gateways must be kept to a minimum, in this use case the only external access point is through the main control unit, which enforces state-of-the-art cryptographic security (e.g., TLS, SSH, or similar protocols).
- No matter the security level applied to internal communications, compromise of the main control unit results in full access to all network traffic and any security mechanisms in place, rendering additional internal protections ineffective against such a breach.

IEC 62443-3-3 Reference:
SR 3.1 (Communication integrity),
SR 4.2 (Use of secure protocols for external communications),
SR 7.6 (Least functionality)

5 Cybersecurity Event Monitoring and logging



A security event monitor detects and reports anomalies to the main control unit. This can be an individual hardware or a task of the main control system. The information reported is the base for an auditable log of security events.

If a separate hardware device is used, it reports the events to the main control unit using a separate serial communication channel. This communication is secured by a combination of TLS-PSK (Transport Layer Security based on pre-shared keys, RFC 4279) and cTLS (Compact TLS, RFC 9147). If supported by the hardware, the event monitor can also directly report to the higher control level using a state-of-the art secure communication channel.

5.1 Monitoring and Anomaly Detection

In CAN systems, the following security related events can be detected, reported and stored in a secured, auditable security event log:

- Any unknown communication attempts.
- Any communication attempts to devices not part of the system.
- Any communication related to configuration, if known, recognize allowed/unallowed reconfigurations.
- Any communication related to bootloader activation or device re-programming.
- For all time-bound communication, validate timings.

Such a setup is especially effective if all process communication is configured to use exact cycle times (e.g. every 100ms).

In these cases, the dedicated security event monitor checks for communication outside expected timing windows. Any unexpected message injection (e.g., from a physically connected rogue device) is flagged and reported to the main control unit.

IEC 62443-3-3 Reference:
SR 6.1 (Audit/logging of security events),
SR 6.2 (Detection of security-relevant events)

6 Selected Cryptographic Measures

With the non-cryptographic measures in place, the cryptographic measures can be limited to the protection of code updates, configurations and device ID authentication. This is all part of service data communication where data is often segmented, and it is easier to apply authentication tags. The real-time critical process data is not secured, here only the non-cryptographic methods are used for protection.

6.1 Cryptographic Primitives and Tag Sizes

- The default cryptographic hash function used is HMAC-SHA-256. In resource constrained systems HMAC-Blake2s may be used.
- Devices use a pre-shared 256 bits / 32 bytes key installed by system integrator in a secure environment.
- Keys are stored securely in non-volatile memory.
- Re-keying requires physical access or firmware reflashing.
- Firmware updates are encrypted by AES-128.
- Firmware updates use a separate pre-shared key only known to the manufacturer, alternatively using state-of-the-art public/private key protection.
- No dynamic key exchange / agreement.
- Nonces used are 64 bits and are a random value.
- The message authentication tag is truncated to 64 bits for protection of configurations and device ID authentication.
- This selection is consistent with BSI TR-02102 guidance for cryptographic methods in constrained embedded systems.

IEC 62443-3-3 Reference:
SR 2.1 (Authorization enforcement),
SR 3.1 (Communication integrity),
SR 4.1 (Use of strong cryptography),
SR 4.3 (Key management)

6.2 Secure Bootloading

- All embedded devices on the CAN network implement a secure bootloading process.
- Firmware images are digitally signed by manufacturer and verified by devices prior to execution to prevent unauthorized code from being loaded.

- Firmware updates require physical access and are authorized through a cryptographic challenge-response mechanism, ensuring updates originate from trusted sources.
- This guarantees the system starts from a known and trusted software baseline, reinforcing the integrity of all subsequent authenticated communications.

IEC 62443-3-3 Reference:
SR 4.1 (Use of strong cryptography),
SR 4.3 (Key management)

6.3 Device ID Authentication

- The main control unit can authenticate all connected devices. Either one-time on start-up or at intervals. Intervals range depending on security requirements.
    - Identification data for an auditable security event log would only be polled a few times per hour.
    - Identification data for a control unit to evaluate the security health of a system would need to be polled more frequent, possibly every minute or even a few times per minute.
- The authentication of the device ID is based on a cryptographic random challenge and response mechanism.

IEC 62443-3-3 Reference:
SR 2.1 (Authentication enforcement),
SR 2.2 (Account management for components),
SR 2.3 (Use of unique identifiers)

Other References:
ISO/IEC 27001 Annex A.12.4 (Event logging)

6.4 Configuration Integrity and Access Control

- Configurations are either statically defined at build time (hardcoded or read-only) or dynamically locked and protected by the main control unit.
- If a lock/unlock mechanism is used for configurable parameters, it uses a cryptographic random challenge and response mechanism.
- The security monitor maintains awareness of all expected configuration states and will detect and flag any attempt to alter them.

IEC 62443-3-3 Reference:
SR 7.6 (Least functionality),
SR 1.2 (Use control),

SR 6.2 (Detection of security-relevant events),
SR 1.4 (Control system configuration integrity)

7 Alignment with Standards and Regulations

7.1 IEC 62443

- The architecture implements a zone-and-conduit model, with the CAN bus operating within a highly secured zone.
- The main control unit acts as a security perimeter enforcing authentication, anomaly detection and logging, and integrity validation.
- The design supports a layered defence strategy, fulfilling defence-in-depth principles.

7.2 BSI TR-02102

- The selected hash-based authentication aligns with BSI's recommendations for lightweight cryptographic primitives in constrained environments.
- Physical security and network segmentation are acceptable compensating controls where confidentiality is not required.

7.3 EU Cyber Resilience Act

- A system specific security risk assessment is still required. With the measures in place, the risk score is significantly lower as without the measures.
- The design supports a layered defence strategy, fulfilling defence-in-depth principles.

8 Conclusion

Given the system's architecture, physical protections, monitoring mechanisms, and controlled external interface, the implementation of non-cryptographic security measures for the CAN network is both justified and compliant with the intent of IEC 62443 and BSI TR-02102 and the EU Cyber Resilience Act. The risk of internal message tampering is mitigated through physical barriers, device ID authentication, and timing-based anomaly detection, ensuring an appropriate balance between security and system resource constraints.

9 Table: IEC 62443-3-3 Requirements Coverage

SR	Requirement Title	How This Is Addressed
SR 1.1	*Physical access control*	CAN network is physically protected inside machinery, behind locked service hatches. Unauthorized access requires physical tampering, making it a key defence layer.
SR 1.2	*Use control*	Configurations are locked/hardcoded, and access to modify is controlled via HMAC based cryptographic challenge-response.
SR 1.4	*Control system configuration integrity*	The system ensures configuration integrity through fixed setups and anomaly detection that flags unauthorized changes.
SR 2.1	*Authentication enforcement*	Devices are continuously authenticated using a HMAC based cryptographic challenge-response scheme with shared secrets and nonces.
SR 2.2	*Account management for components*	Each device is uniquely identified and authenticated. Accounts are effectively represented by device IDs.
SR 2.3	*Use of unique identifiers*	Device IDs are used as unique identifiers in the authentication protocol.
SR 3.1	*Communication integrity*	Process data message integrity is protected by monitoring anomalies in message timing.
SR 3.4	*Use of encryption based on confidentiality needs*	Confidentiality is not required for data on internal CAN communications; hence, no encryption is used.
SR 4.1	*Use of strong cryptography*	The system uses HMAC-SHA-256 or HMAC-Blake2s with 256-bit keys and 64-bit truncated tags, compliant with BSI TR-02102 for constraint systems.
SR 4.2	*Use of secure protocols for external communications*	TLS-PSK and cTLS are used for all external interfaces, ensuring encrypted and authenticated communication.

SR 4.3	*Key management*	Keys are installed securely during system integration, stored in protected memory, and only updated via physical access or firmware reflashing.
SR 5.2	*Zone boundary protection*	The system is segmented such that the main control unit is the only gateway to external networks, enforcing a secure zone boundary.
SR 6.1	*Audit/logging of security events*	A dedicated security event monitor logs and reports anomalies to the main control unit.
SR 6.2	*Detection of security-relevant events*	The system continuously monitors message timing and configuration states to detect anomalies such as frame injection or unauthorized config changes.
SR 7.2	*Fail securely*	The system relies on physical protection; if the CAN bus is cut or disabled, the impact is equivalent to component failure.
SR 7.6	*Least functionality*	The CAN network and external interface offer only essential functions. All unnecessary services and ports are disabled or omitted.

10 Table: CRA Requirements Coverage

SR	Requirement Title	How This Is Addressed
1	Defence in depth	The design supports a layered defence strategy, fulfilling defence-in-depth principles.
2b	Secure default config, reset to default	Default configurations are hardcoded or locked and can be reset securely by the main control unit.
2c	Fix vulnerabilities with updates	Secure bootloader allow installation of security updates.
2d	Unauthorized access protection	Physical access to the CAN network is restricted by mechanical barriers; interfaces are protected.
2f	Protect integrity (data manipulation)	The integrity of device ID authentication messages and configurations are protected via HMAC. Process data messages are protected by physical security and anomaly detection.
2j	Minimize attack surface	Number of interfaces to other networks is limited, only main control unit acts as gateway.
2l	Cybersecurity Event Log	Security events such as message injection or timing anomalies are detected and reported by the security monitor, the main controller stores them in an auditable security event log.
2c	Fix vulnerabilities with updates	Secure bootloader allow installation of security updates.