Enhancing functional safety in CAN/CANopen data communication for industrial machines

Thilo Schumann (CAN in Automation)

This abstract underscores the imperative of achieving functional safety in data communication for industrial machines, with a special focus on the CAN (Controller Area Network) and CANopen protocols. These safety-critical systems, including construction machines, mobile cranes, waste collection vehicles, metal presses, and manufacturing shopfloor machinery, necessitate resilient data communication.

Notably, the international standard EN 50325-5, known as CANopen Safety, has provided a robust foundation for such networks. However, as technological advancements continue to shape the industrial landscape, this standard is undergoing revision. The revised standard offers an opportunity to incorporate new insights and lessons learned over recent years.

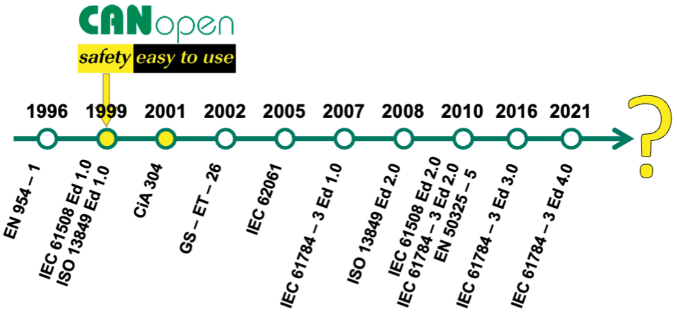
Moreover, it‘s essential to recognize the emergence of new embedded networks and protocols, such as CAN FD (Flexible Data Rate), CANopen FD, and CAN XL. These protocols introduce enhanced features, including increased data transmission speeds and larger data payloads. Nevertheless, their adoption may also necessitate reevaluating functional safety requirements, as they differ from the CANopen Safety standard, which relies on the gray channel approach.

Engineers and practitioners are encouraged to leverage the upcoming revision of EN 50325-5 as a foundational reference to develop updated functional safety requirements. These requirements should not only address the evolving CAN/CANopen landscape but also consider the implications of new protocols like CAN FD, CANopen FD, and CAN XL. This endeavor aims to ensure that industrial machinery continues to operate safely and efficiently in a rapidly advancing technological environment.

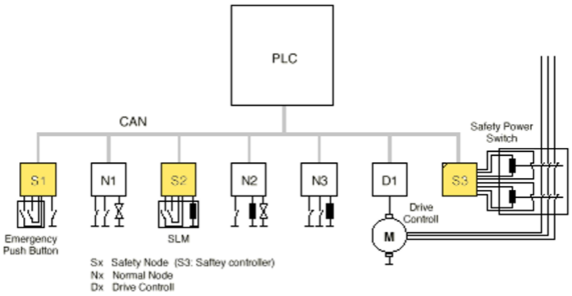
1. Introduction

In industrial environments, where complex machinery and automated systems operate in close proximity to human operators, ensuring safety is paramount. Functional safety, a concept integral to industrial automation, addresses the systematic approach to designing and implementing systems that minimize the risk of hazards resulting from malfunctioning equipment or errors in operation.

Functional safety standards, such as ISO 26262 for automotive systems and IEC 61508 for general industrial applications, provide frameworks for assessing and managing safety risks throughout the lifecycle of a system. These standards emphasize the need for rigorous analysis, design, implementation, and validation processes to achieve the desired level of safety integrity.



Within the realm of industrial automation, embedded communication plays a vital role in facilitating the exchange of data and commands between interconnected devices. This communication enables coordinated operation and control of machinery, enhancing productivity and efficiency. However, in safety-critical applications, such as those found in manufacturing, logistics, and process industries, the reliability and integrity of communication systems are of utmost importance to prevent accidents and protect human life.



One widely adopted communication protocol in industrial automation is CANopen, known for its versatility, efficiency, and interoperability. CANopen facilitates seamless communication between various devices in a networked environment, enabling real-time control and monitoring of industrial processes. However, as safety regulations evolve and become more stringent, there is a growing need to enhance the functional safety aspects of CANopen communication to meet the latest safety standards and directives.

This paper explores the intersection of functional safety and embedded communication in industrial automation, with a focus on the CANopen Safety protocol. Specifically, it examines the challenges and opportunities associated with ensuring safety integrity in CANopen networks, particularly in light of new requirements introduced by machine safety directives. By addressing these challenges and proposing enhancements to CANopen Safety, this paper aims to contribute to the advancement of functional safety communication systems in industrial environments.

1.1.1. Introduction to CANopen Safety protocol

CANopen, a widely utilized communication protocol in industrial automation, has been instrumental in facilitating seamless data exchange and control in interconnected systems. However, as industries place increasing emphasis on safety-critical applications, the need for enhanced functional safety within CANopen networks becomes apparent.

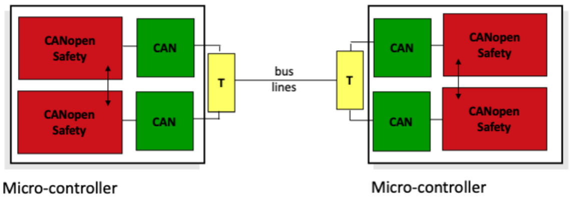
CANopen Safety emerges as a specialized profile within the CANopen protocol suite, dedicated to addressing the stringent safety requirements of industrial applications. Unlike its standard counterpart, CANopen Safety incorporates additional functional safe mechanisms and protocols to ensure the reliability, integrity, and timeliness of communication in safety-critical environments.

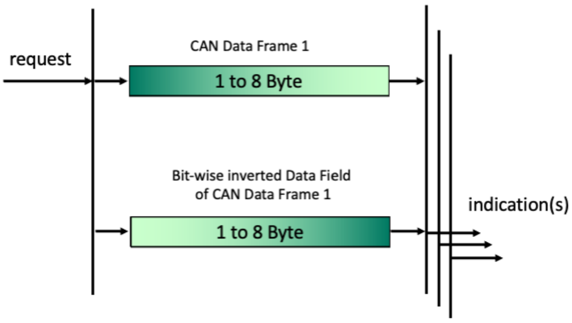
The development of CANopen Safety stems from the recognition that traditional communication protocols, while efficient for general-purpose applications, may fall short in meeting the rigorous safety standards mandated by regulatory bodies and industry directives. As a result, CANopen Safety introduces tailored features and protocols designed to mitigate risks associated with communication failures and data corruption.

By integrating safety-oriented features such as redundant communication and error detection CANopen Safety enhances the resilience of communication networks against potential hazards and failures. These enhancements not only bolster the safety integrity of interconnected devices but also contribute to the overall reliability of industrial systems.

In this paper, we delve into the intricacies of CANopen Safety, exploring its architecture, key features, and advantages over conventional communication protocols. We also examine the challenges and limitations inherent in ensuring functional safety within CANopen networks and propose strategies for addressing these challenges to meet the evolving requirements of machine safety directives.

Through a comprehensive analysis of CANopen Safety, this paper aims to shed light on the critical role of embedded communication in industrial safety and contribute to the ongoing efforts to enhance the safety and reliability of interconnected systems in industrial automation.



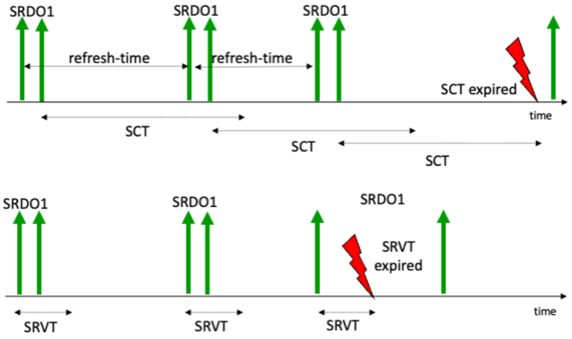


1.2. Statement of the problem: Addressing new requirements in machine safety directives

In recent years, the landscape of industrial safety has undergone significant evolution, driven by advancements in technology, changing regulatory frameworks, and a growing emphasis on safeguarding human operators and assets in industrial environments. As a result, machine safety directives, such as ISO 13849 and IEC 62061, have been revised and augmented to address emerging safety challenges and promote the adoption of state-of-the-art safety measures.

1.2.1. Emerging Safety Challenges

The proliferation of automation and interconnected systems in industrial settings has led to new safety challenges that traditional machine safety directives may not fully address. For instance, the increasing complexity of machinery and processes introduces additional points of failure and potential hazards, necessitating enhanced safety mechanisms and risk mitigation strategies.



Furthermore, the integration of advanced technologies, such as collaborative robots (cobots), autonomous vehicles, and Industrial Internet of Things (IIoT) devices, presents unique safety considerations that require tailored solutions. These technologies introduce new modes of interaction between humans and machines, raising concerns about operator safety, cybersecurity, and system resilience.

1.2.2. Revised Safety Standards and Directives

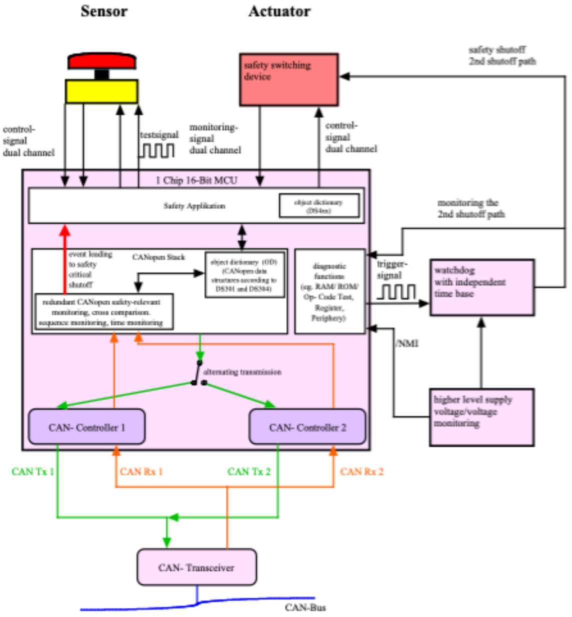
In response to these evolving safety challenges, regulatory bodies and standards organizations have revised existing machine safety directives and introduced new requirements aimed at raising the bar for safety performance and compliance. For example, ISO 13849, which specifies safety-related parts of control systems, has been updated to incorporate additional validation and verification requirements, as well as provisions for cybersecurity and functional safety integration.

Similarly, IEC 62061, which pertains to the safety of machinery control systems, has undergone revisions to align with the latest developments in safety technology and best practices. The revised standard emphasizes the importance of systematic risk assessment, safety integrity level (SIL) determination, and the implementation of safety functions to achieve the desired level of safety performance.

1.2.3. Challenges in Compliance and Implementation

While the revisions to machine safety directives are intended to enhance safety performance and promote best practices, they also present challenges for manufacturers, integrators, and end-users seeking to achieve compliance. Meeting the new requirements often requires investment in additional resources, expertise, and infrastructure, which may pose financial and logistical constraints for organizations.

Moreover, ensuring compatibility and interoperability between existing systems and newly implemented safety measures can be a complex and time-consuming process. Integrating safety-critical components, such as emergency stop systems, safety interlocks, and safety-rated communication protocols like CANopen Safety, requires careful planning and validation to prevent unintended consequences and ensure seamless operation.


Sensor
Actuator
safety switching device
safety shutoff 2nd shutoff path
control-signal dual channel
testsignal
monitoring-signal dual channel
control-signal dual channel
1 Chip 16-Bit MCU
Safety Application
object dictionary (DS4xx)
monitoring the 2nd shutoff path
event leading to safety critical shutoff
CANopen Stack
object dictionary (OD) (CANopen data structures according to DS301 and DS304)
redundant CANopen safety-relevant monitoring, cross comparison, sequence monitoring, time monitoring
diagnostic functions (eg. RAM/ ROM/ Op- Code Test, Register, Periphery)
trigger-signal
watchdog with independent time base
/NMI
alternating transmission
higher level supply voltage/voltage monitoring
CAN- Controller 1
CAN- Controller 2
CAN Tx 1
CAN Rx 1
CAN Tx 2
CAN Rx 2
CAN- Transceiver
CAN-Bus

2. Background

In the realm of industrial automation and automotive engineering, ensuring the safety of complex systems is paramount. Functional safety standards provide the framework and guidelines necessary to systematically assess and mitigate safety risks throughout the lifecycle of a product or system. Two prominent standards in this domain are ISO 26262 and IEC 61508.

2.1. ISO 26262

ISO 26262, titled „Road vehicles – Functional safety," is an international standard that addresses the functional safety of electrical and electronic systems within vehicles. Developed specifically for the automotive industry, ISO 26262 outlines requirements and processes for managing safety risks associated with the implementation of electronic systems in vehicles.

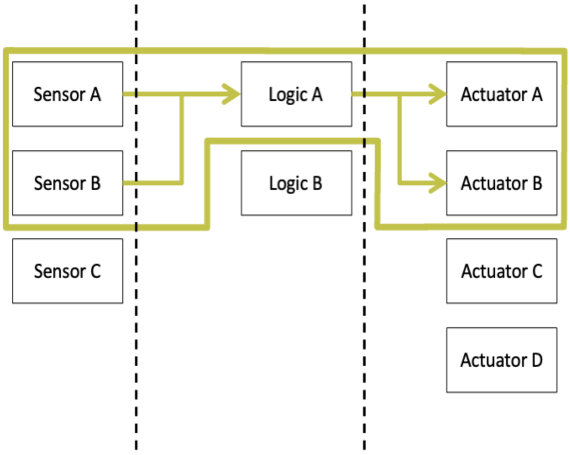
The standard defines various safety integrity levels (SILs), ranging from ASIL A (least stringent) to ASIL D (most stringent), based on the severity of potential hazards and the probability of exposure. ISO 26262 emphasizes a systematic approach to safety, encompassing requirements specification, design, implementation, integration, verification, and validation of safety-related systems.

Key elements of ISO 26262 include hazard analysis and risk assessment (HARA), functional safety concept development, safety requirements specification, and validation and verification processes. The standard also prescribes specific techniques and methodologies for achieving functional safety, such as fault tree analysis (FTA), failure modes and effects analysis (FMEA), and safety integrity level (SIL) determination.

2.2. IEC 61508

IEC 61508, titled „Functional safety of electrical/electronic/programmable electronic safety-related systems," is a generic international standard applicable to various industries, including automotive, aerospace, process control, and machinery. Unlike ISO 26262, which is tailored for automotive applications, IEC 61508 provides a broader framework for managing functional safety across different sectors.

IEC 61508 follows a lifecycle approach to functional safety, encompassing requirements specification, design, implementation, operation, maintenance, and decommissioning of safety-related systems. The standard emphasizes the identification and mitigation of systematic and random failures that could lead to hazardous situations.



Central to IEC 61508 is the concept of safety integrity levels (SILs), which are assigned to safety functions based on their criticality. SILs range from SIL 1 (lowest integrity) to SIL 4 (highest integrity), with each level corresponding to a specified level of risk reduction. The standard provides guidance on the selection of appropriate safety measures and techniques to achieve the required SIL for a given safety function.

2.3. Introduction to CANopen protocol and its applications in industrial automation

In the landscape of industrial automation, where efficiency, interoperability, and reliability are paramount, communication protocols play a pivotal role in facilitating seamless data exchange and control among interconnected devices. One such protocol that has gained widespread adoption in industrial environments is CANopen.

3. CANopen Protocol

CANopen, based on the Controller Area Network (CAN) protocol, is a robust and versatile communication protocol designed for distributed control systems and automation applications. Originally developed by CiA (CAN in Automation), CANopen provides a standardized communication framework that enables interoperability among various devices, such as sensors, actuators, controllers, and human-machine interfaces (HMIs).

At its core, CANopen defines a set of communication profiles and an object dictionary that specify standardized data formats, message structures, and network management functions. This standardized approach simplifies the integration of disparate devices from different manufacturers into a cohesive and interoperable system, thereby reducing development time and costs.

The inherent features of CANopen, including its high-speed data transmission, deterministic communication, and support for multi-master and peer-to-peer communication, make it well-suited for real-time control and monitoring applications in industrial automation. Additionally, CANopen‘s flexibility allows for the implementation of complex network topologies, ranging from simple point-to-point connections to large-scale distributed control systems.

3.1. Applications in Industrial Automation

The versatility and reliability of CANopen have led to its widespread adoption across various sectors of industrial automation, including manufacturing, automotive, robotics, logistics, and process control. In manufacturing environments, CANopen is commonly used for machine control, motion control, and data acquisition applications, where real-time communication and precise synchronization are essential.

In automotive manufacturing, CANopen facilitates the integration of diverse subsystems, such as robots, conveyors, and assembly stations, into a unified production line, enabling seamless coordination and control of manufacturing processes. Similarly, in logistics and material handling applications, CANopen is utilized for vehicle control, warehouse automation, and inventory management, optimizing throughput and efficiency.

Moreover, CANopen finds applications in safety-critical systems, where the reliability and timeliness of communication are paramount. For instance, in machine safety applications, CANopen Safety protocol ensures the integrity of communication in safety-critical networks, enabling the implementation of advanced safety functions, such as emergency stop, safe motion, and safe monitoring.

4. CANopen Safety Protocol

4.1. Overview of CANopen Safety

In the realm of CANopen Safety, a key feature involves employing redundant communication methods. This redundancy is achieved by transmitting data in two consecutive messages over the same wire. However, these two messages are not identical. In the second message, the data is bitwise inverted, and it is transmitted using a different CAN identifier. Moreover, to ensure the effectiveness of this redundancy, there‘s a stringent timing requirement. The data must be transmitted periodically, and both messages must be received within a specified timeframe. This approach enhances the reliability and integrity of communication in safety-critical environments, aligning with the stringent requirements of machine safety directives.

4.2. Challenges and Limitations

CANopen Safety presents certain challenges when implementing it within devices. Serving as a white channel solution, it is directly integrated onto the communication processor. This characteristic renders it highly suitable for straightforward sensors and actuators, particularly those with single chip implementations. However, the complexity increases when dealing with more intricate and sophisticated implementations involving multiple application processors and microcontrollers.

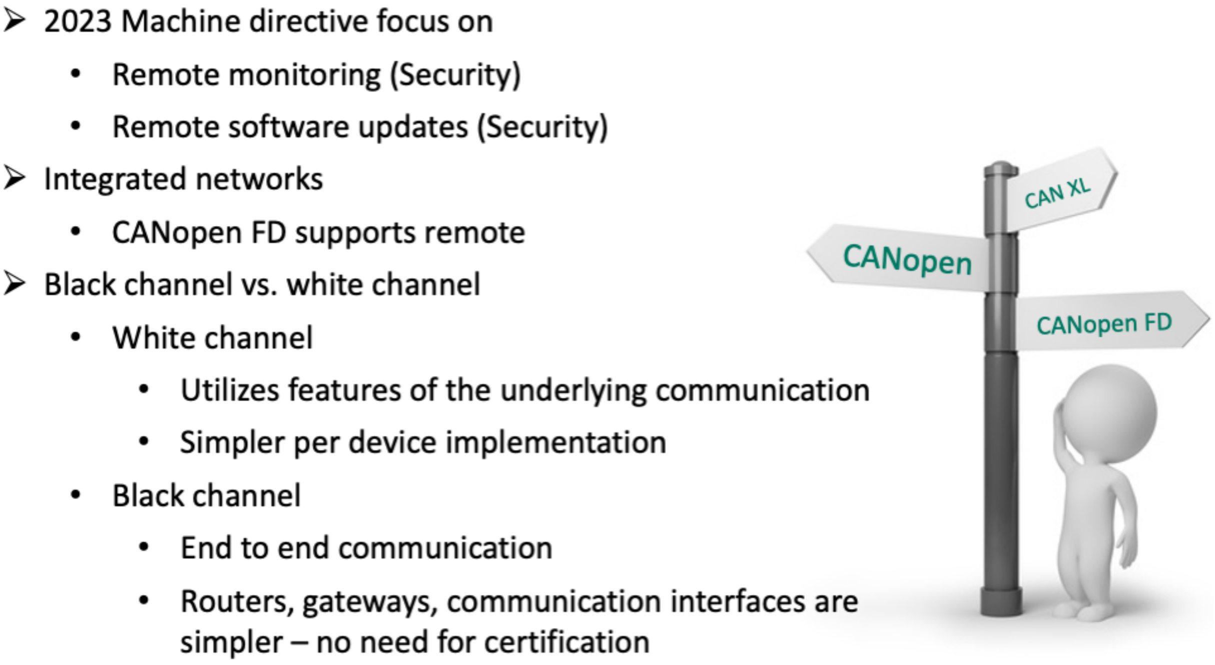
The implementation process as a whole must adhere to the stringent requirements for safety-critical systems and undergo assessment by notified bodies. Implementors must possess expertise in safety-critical implementations, as relying solely on pre-certified modules proves challenging. This is because the software module‘s implementation must align precisely with the provided hardware implementation to ensure compliance with safety standards. Therefore, meticulous attention to detail and thorough verification processes are essential to successfully integrate CANopen Safety into devices within industrial automation settings.

4.2.1. Limitations of existing CANopen Safety protocol in meeting new requirements of machine safety directives

Despite its advantages, the existing CANopen Safety protocol faces certain limitations when it comes to meeting the evolving requirements of machine safety directives. These limitations stem from various factors, including protocol design constraints, technological advancements, and the changing landscape of industrial safety standards.

4.2.1.1. Limited Support for Advanced Safety Functions

The current CANopen Safety protocol may lack support for advanced safety functions mandated by new machine safety directives. For example, requirements for



- 2023 Machine directive focus on
  - Remote monitoring (Security)
  - Remote software updates (Security)
- Integrated networks
  - CANopen FD supports remote
- Black channel vs. white channel
  - White channel
    - Utilizes features of the underlying communication
    - Simpler per device implementation
  - Black channel
    - End to end communication
    - Routers, gateways, communication interfaces are simpler – no need for certification

safe motion control, safe monitoring, and functional safety integration may exceed the capabilities of the existing protocol. Without adequate support for these advanced safety functions, manufacturers and integrators may face challenges in achieving compliance with the latest safety standards.

4.2.1.2. Scalability and Flexibility Constraints

CANopen Safety protocol may exhibit scalability and flexibility constraints, particularly in large-scale distributed systems or applications with diverse safety requirements. As industrial automation systems evolve and expand, the need for scalable and flexible safety communication solutions becomes more pronounced. The existing protocol may struggle to accommodate the increasing complexity and diversity of safety-critical applications, leading to limitations in meeting the new requirements of machine safety directives.

4.2.1.3. Inadequate Cybersecurity Measures

In an era of increasing connectivity and digitalization, cybersecurity has emerged as a critical concern in industrial safety. The existing CANopen Safety protocol may lack robust cybersecurity measures to protect against cyber threats, such as unauthorized access, data manipulation, and denial-of-service attacks. Without adequate cybersecurity measures, CANopen Safety networks may be vulnerable to security breaches, compromising the integrity and safety of industrial systems.

4.2.1.4. Compliance Challenges with SIL Certification

Meeting the SIL certification requirements specified in machine safety directives can be challenging for CANopen Safety implementations. Achieving SIL certification involves rigorous assessment and validation of the safety-related functions within a system, which may be difficult to achieve with the existing protocol. Manufacturers and integrators may struggle to demonstrate compliance with SIL certification requirements, hindering the adoption of CANopen Safety in safety-critical applications.

5. Conclusion

In conclusion, several improvements are needed to ensure that CANopen Safety protocol meets the requirements of machine safety directives. By enhancing support for advanced safety functions, implementing robust cybersecurity measures, obtaining SIL certification, and improving scalability and flexibility, the protocol can better address the evolving needs of safety-critical applications and facilitate compliance with the latest safety standards. By prioritizing these improvements, manufacturers and integrators can develop safer and more reliable industrial automation systems that comply with machine safety directives.

Thilo Schumann
CAN in Automation
Kontumazgarten 3
DE-90429 Nuremberg
headquarters@can-cia.org
www.can-cia.org