Re-examining Non-Interference Requirements in CIP Safety Devices for Closed Communication Systems

Arun K Guru
Systems Architect/Principal Engineer
Rockwell Automation
Mequon/USA

Steven Seidlitz
Principal Engineer
Rockwell Automation
Milwaukee/USA

Jim Grosskreuz
Technology Manager, Safety
Rockwell Automation
Milwaukee/USA

Stina Hornstrom
ABB Robotics
Sweden

David Crane
Senior Staff Engineer
ODVA
Michigan/USA

Presented at the ODVA
2026 Industry Conference & 24th Annual Meeting
October 21, 2026
Vilamoura, Portugal

Abstract

CIP Safety is based on the Black Channel concept defined in IEC 61784-3, where the communication path is treated as unknown and potentially faulty, and safety integrity is achieved through end-to-end mechanisms in the Safety Communication Layer (SCL). These mechanisms provide a SIL 3 compatible residual error rate independent of the underlying network and lower protocol layers. However, current applications of IEC 61508-3 standard's non-interference requirements can impose stringent architectural

 ©2026 ODVA, Inc.

constraints when integrating SIL 3 capable CIP Safety stacks into devices whose safety functions require only SIL 1 or SIL 2 to meet application needs.

This paper examines the implications of applying mixed-criticality non-interference rules—originally intended to prevent interference between safety-related and non-safety-related software elements—within a Black Channel communication model. Not only can implementing non-interference measures in both hardware and software be overly burdensome for products not requiring SIL3, but the alternative is just as burdensome. Namely, requiring Systematic Capability (SC) 3 down to the supporting software, operating systems, and hardware will effectively force a full SIL 3 design onto a platform and/or system where the system-level risk assessment simply does not justify such elevated integrity levels.

The recently adopted closed communication system option in CIP Safety resolves this tension. In closed systems where the system integrator controls the complete communication network, responsibility for achieving appropriate Systematic Capability shifts to the integrator—aligning with IEC 61508:2010 system design principles. This enables device developers to integrate CIP Safety onto platforms with SC levels proportional to their individual safety functions, while the integrator ensures overall system integrity. The paper concludes by outlining areas investigated within ODVA, including conformance policy interpretation and guidance.

Keywords

CIP Safety; IEC 61784-3; IEC 61508-3; ISO 13849-1; Non-Interference; Systematic Capability; Closed Communication System; Black Channel; Mixed Criticality;

Definition of terms

Annexture F	IEC61508-2 Annexture F. Techniques and measures for ASICs – avoidance of systemic failures IEC61508- 3 Annexture F. Techniques for achieving non-interference between software elements on a single computer
BSP	Board Support Package
CIP	Common Industrial Protocol
Closed Communication System	Fixed number or fixed maximum number of participants linked by a communication system with well-known and fixed properties, and where the risk of unauthorized access is considered negligible (see IEC 61784-3:2024 Edition 4.1 Section 3.1.6)
Defined Communication System	Defined channel; fixed number or fixed maximum number of participants linked by a fieldbus based communication system with well-known and fixed properties, such as installation conditions, electromagnetic immunity, industrial (active) network elements, and where the risk of unauthorized access is reduced to a tolerated level according to the lifecycle model of IEC 62443 (all parts), using for example zones and conduits (see IEC 61784-3:2024 Edition 4.1 Section 3.1.11)
FMEA	Failure Mode Effects Analysis
FSCP	Functional Safety Communication Profile
IEC	International Electrotechnical Commission
IEC 61508-3	Functional Safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements 2010
IEC 61784-3	Industrial Communication Networks – Part 3: Functional Safety Fieldbuses, Edition 4.1, 2024
Mixed Criticality	A safety system in which producers and consumers of safety data with varying SIL/PL criticalities co-exist.
PID	Unique Producer ID
PL	Performance Level
RTOS	Real Time Operating System
SC	Systematic Capability
SCL	Safety Communication Layer

 ©2026 ODVA, Inc.

SI	System Integrator
SIL	Safety Integrity Level

Introduction

Safety communication protocols are often judged by two overlapping but distinct properties: the probability that random communication errors escape detection, and the systematic capability that the software and hardware implementing the safety function are developed and integrated appropriately. CIP Safety has historically emphasized strong end-to-end communication diagnostics through the Black Channel concept. This means that the lower-level communication path, including ordinary network equipment and lower-layer software, is not trusted to be correct; instead, the Safety Communication Layer (SCL) detects corruption, masquerade, delay, loss, repetition, insertion, and other communication faults before unsafe data can be accepted by the receiver in a safety function, pursuant to all the fault modes described in IEC 61783-3: 2024, Edition 4.1.

The following sections discuss a practical question that emerges when this model is combined with non-interference expectations on mixed criticality safety networks with many different safety devices present as shown in Figure 1 and a solution is proposed to address this question. When a CIP Safety runtime stack that is developed to SIL3/SC3 capability is integrated into a device with SIL1/PLc or SIL2/PLd safety functions (as shown in Figure 2), a literal preservation of SC3—as previously required by the CIP Safety specification—can be problematic. It can drive requirements downward into all the rest of the subsystems of a safety product, which may or may not be compliant with SC3. This includes the operating system, board support package, memory management units, timing services, and even the hardware platform. All of this adds disproportionate burden. The result can be increased engineering burden relative to the safety function risk analysis and to the end user in terms of higher product costs.

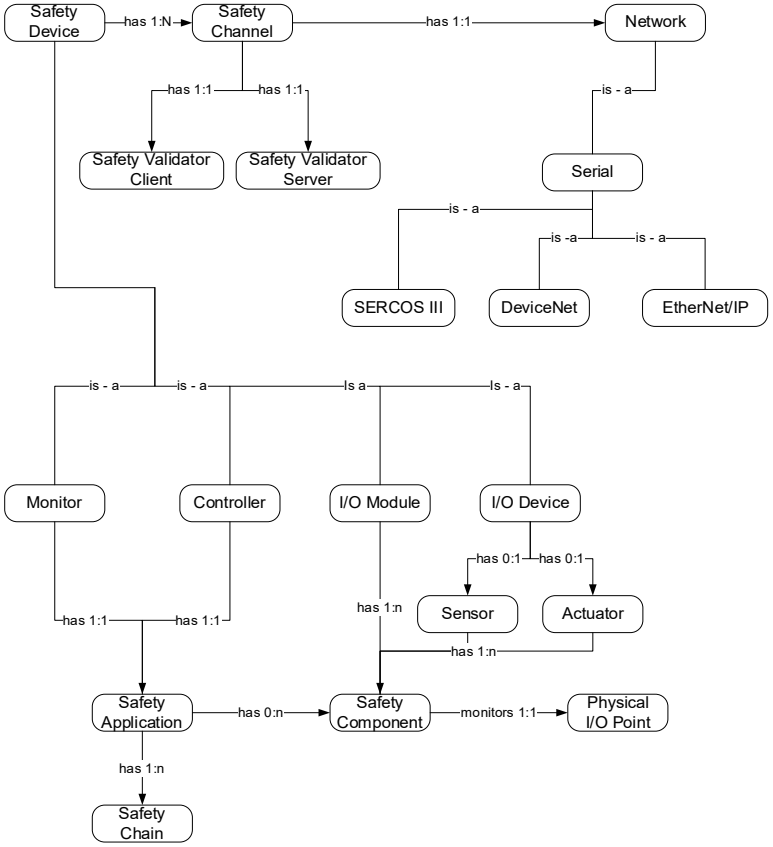


Figure 1: Entity Relationship Diagram of a Safety System

A closed system is where all participating nodes are known, fixed, and controlled. Furthermore, the network is not open to arbitrary devices or traffic such that the risk of unauthorized access is considered negligible. In short, the communication topology and participants are bounded and stable in a closed communication system. IEC 61784-3, however, fundamentally moves the industry away from relying on closed systems toward defined safety communication over a Black Channel (FSCP-based) and removes some of the restrictions in the use of safety devices imposed in the closed systems. The Black Channel approach assumes that the network itself is not trusted, and all safety guarantees must come from the end-to-end safety protocol.

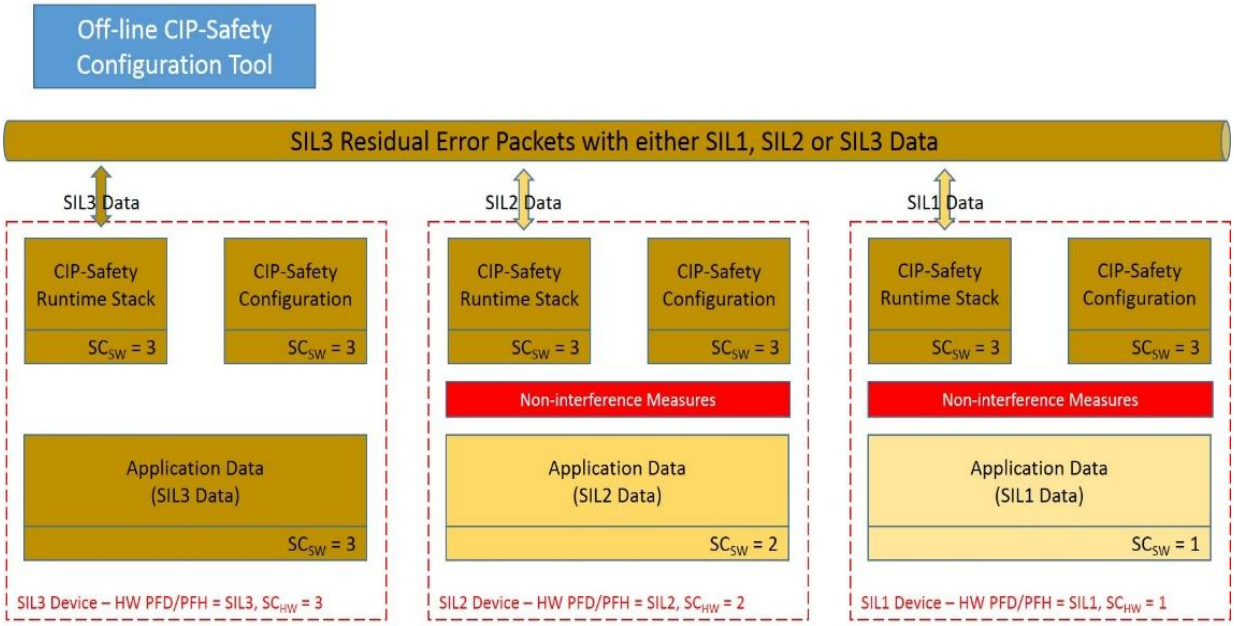


Figure 2: Possible Safety Architectures for CIP Safety

However, for a CIP Safety stack to implement end-to-end safety properly, it itself must have sufficient integrity within a safety product, free from corruption by other safety elements within that same device. Figure 2 shows one of two options to achieve this integrity for a CIP Safety stack. The first column in Figure 2 shows a requirement that all other safety elements within said device also need to achieve SC3. The second alternative is shown in the other two columns, where explicit non-interference measures in both hardware and software would need to isolate the application from interfering and corrupting the CIP Safety stack. Both options can be considered burdensome that adds undue cost to a system of which its risk assessment does not deem SIL3 to be necessary.

This paper re-examines whether such non-interference expectations in the CIP Safety specification as shown Figure 2 should apply differently in devices deployed in closed communication systems. It centers around clarifying two things: communication diagnostics must remain robust, and the responsibility for achieving appropriate system-level SC/PL ultimately rests with the system integrator, who controls device selection and system boundaries in closed networks.

CIP Safety Specifications and Standards Context

Black Channel model and CIP Safety

The Black Channel model assumes that the communication path between producer and consumer is unknown, potentially faulty, and not relied upon for safety. The Black Channel not only encompasses external network devices such as switches and routers, but it also extends within a safety product, too, to include the standard (non-safety) communication layers as well. In the single-cast safety function block diagram shown in Figure 3 below, the Black Channel boundary begins when the producer's Safety Communication Layer forwards the safety payload to the EtherNet/IP stack and ends where the communication enters the consumer's Safety Communication Layer. Software and hardware below that

boundary may therefore be treated as part of the Black Channel rather than as trusted safety mechanisms.

This distinction matters because the communication protocol mechanisms are intended to provide the diagnostic coverage necessary to keep residual communication failures sufficiently low. The current CIP Safety protocol's residual communication failure rates are proven to be SIL3-compatible, meaning the communication error detection mechanisms themselves are not the primary proposed change. The proposed change concerns how systematic capability requirements are allocated when the safety function using the network requires less than SIL3/SC3.

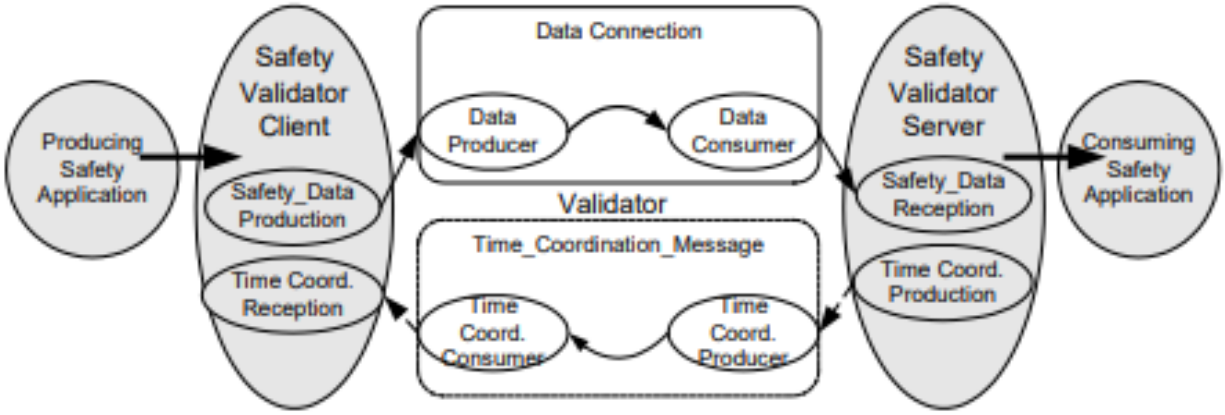


Figure 3: Single-Cast Safety Function Block Diagram

Mixed criticality and non-interference in IEC 61508
IEC 61508 mixed-criticality principles require adequate independence when software implements functions of different safety integrity levels. Annex F (IEC61508-2 and IEC61508-3) techniques focus on independence in spatial and temporal domains, such as memory separation, execution-time control, and shared-resource management. The attached analysis highlights a crucial implementation consequence: if a BSP, RTOS, hypervisor, memory manager, timer service, or equivalent supporting software provides the non-interference service, that supporting software must be capable of supporting the highest systematic capability that it is protecting.

For a CIP Safety stack certified or developed at SC3, preserving SC3 by non-interference on an SC1 or SC2 platform can therefore become infeasible without upgrading the supporting software and hardware environment. In the strictest interpretation, the stack's systematic capability is not preserved by merely placing it on a lower-SC platform with aspirational separation; the separation mechanism itself becomes a safety-related supporting mechanism. The maximum SIL/PL for any safety function is limited by the device with the lowest SIL/PL capability participating in the network.

Problem Statement
The problem is a mismatch between communication-layer diagnostic strength and device-level systematic capability allocation. A CIP Safety stack may produce SIL3-compatible residual error performance for communication faults, yet the application safety function may only require SIL1 or SIL2. If preserving SC3 of the stack requires SC3 non-interference throughout supporting software and hardware as required previously in the CIP Safety specification, the device developer may be forced into a platform integrity level that exceeds the system risk assessment.

A member inquiry into Safety SIG prompted discussions about practical consequences of the current approach. These include increased development effort, over-engineering, higher costs, and reduced performance. Gateway-style isolation adds latency, and the approach becomes unsuitable for robotics and machinery applications where PLd/SIL2 requirements are common. In the most partitioned architecture, a separate SC3 hardware module may be required merely to host the CIP Safety stack, even when the safety function does not require SIL3.

Technical Analysis

Why the issue is not the Black Channel residual error rate

The Black Channel approach already assumes that lower communication layers may fail. Relaxing the device-level non-interference expectation in a controlled closed system does not mean relaxing the CIP Safety protocol's end-to-end diagnostics. The proposed closed-system approach retains the techniques used to detect communication errors and continues to use SIL3-compatible communication residual error calculations for reliability prediction. The residual communication error model therefore remains intact; what changes is the systematic capability that may be claimed for the overall safety function that is to be integrated into a network of safety devices. The Safety SIG did not want to create two or three formats of protocol meant for different SIL needs.

FMEA of possible interferences

An FMEA tool was used to explore lowered systematic capability interference scenarios. These included wrong Producer ID (masquerading a higher SIL device's ID), wrong rollover count, wrong timestamp, masquerade, data integrity error, timeliness error, and authenticity error. Many cases remain safe because the safety layer in the consumer detects a CRC error, timeliness, or data integrity mismatch. Residual dangerous cases arise under specific scenarios with coupling of multiple errors as shown in Table 1: For example, a producer-side overwrite of Producer ID occurring simultaneously with a complementary Black Channel error pattern that escapes the diagnostic mechanism on the consumer side or when a consumer-side Producer ID overwrite occurring simultaneously with a similar error on the producer side. When this occurs, the residual failure rate depends on the over-write rate (in the producer and/or consumer), the communication error rate (in the receiver), and the CRC residual probability (of the protocol) which are hard to quantify without level higher systematic measures. SIG felt it is better to conservatively analyze such failure modes using qualitative methods. It should be noted that the current CIP Safety protocol does not account for announcing the SIL/PL capabilities of a producer explicitly unlike other protocols. Table 1 summarizes the FMEA logic used to separate safe detected cases from residual-dangerous coupled cases.

Table 1: FMEA Analysis of Coupled Error Modes

Scenario class	Example	Primary diagnostic	Residual-risk interpretation
Standalone producer-side overwrite	PID or rollover count overwritten, but message reaches intended consumer without additional corruption.	Safety-related CRC, expected identifier, rollover and context checks.	Normally detected or harmless when safety data remains correct and consumer context is unchanged.
Coupled data - integrity error	Safety data corruption complements the producer-side over-write pattern on the consumer side.	CRC and data integrity assurance.	Residual dangerous rate is bound by over-write rate, bit error probability over safety data length, and CRC residual probability.
Coupled timeliness error	Out-of-sequence data with a rollover/timestamp pattern that appears valid in the consumer context.	Timestamp, Network Time Expectation, rollover sequence checks.	Residual dangerous rate is tied to overwrite rate, timeliness error rate, valid time window, and CRC residual probability.
Coupled authenticity / masquerade error	Message is misdirected or masquerades as another valid producer and happens to match context.	Connection authentication, unique identifiers, SNN, and CRC encoding of identity-dependent data.	Residual dangerous rate depends on authenticity error rate, valid context coincidence, and CRC residual probability.

Architectural consequences of strict SC3 non-interference

A strict SC3-requirement can transform an integration task into a platform redesign. If an SC3 stack is placed on an SC2 BSP/OS and SC2 hardware, the supporting mechanisms that enforce temporal and spatial independence are not themselves SC3. Consequently, such integration without non-interference does not guarantee isolation of the SC3 boundary of the stack; so, the platform must be upgraded, or the stack must be isolated on separate SC3 hardware. For time-critical robot or machine applications, gateway isolation adds latency and another safety communication path, undermining the value of direct safety communication with the end device.

Proposed Solution for Closed Communications Systems

Proposed interpretation is a proportional systematic capability model for closed communication systems:

- The CIP Safety runtime stack and protocol mechanisms remain developed and assessed for SIL3-compatible communication residual error performance when intended for broad CIP Safety compatibility.
- In a closed communication system, the integration of the stack, configuration handling, and application data path may be evaluated according to the SC/PL required by the safety functions and documented in the safety manual.
- The safety system integrator is responsible for selecting devices and maintaining a closed system whose participants, properties, access assumptions, and safety function requirements are controlled.
- The weakest participating node or device, by SC/PL, determines the maximum SC/PL claim for the closed communication system and the safety functions using it.
- When SC3 is required or when the system is not closed, traditional SC3 preservation/non-interference requirements remain the applicable path.

The strongest objection to the closed-system interpretation is that it moves burden from the device supplier to the communication system integrator. That concern is legitimate: the integrator must be safety-competent, must control the assumptions that make the system closed, and must ensure the selected devices are suitable for the intended safety functions. However, this allocation is also consistent with the system-design logic of functional safety; the required risk reduction belongs to the safety function and its application context, not automatically to the highest-capability communication component available. Furthermore, there must also be organizational measures in place to ensure the system remains closed throughout the lifecycle of the system, and not just from initial commissioning at a production site. Future system integrators will need to be aware of this system configuration and not allow for mixed criticality changes to creep into the system based on future maintenance or updates.

The proposed approach as shown in Figure 4 also improves scalability. Today, device developers may be discouraged from adding CIP Safety to PLd/SIL2 machinery or robotics platforms because doing so can require a broad SC3 platform redesign. A closed-system path permits adoption where the safety function claim is lower, provided the system integrator accepts the corresponding responsibilities and the device documentation makes the closed-use limitation explicit.

 ©2026 ODVA, Inc.

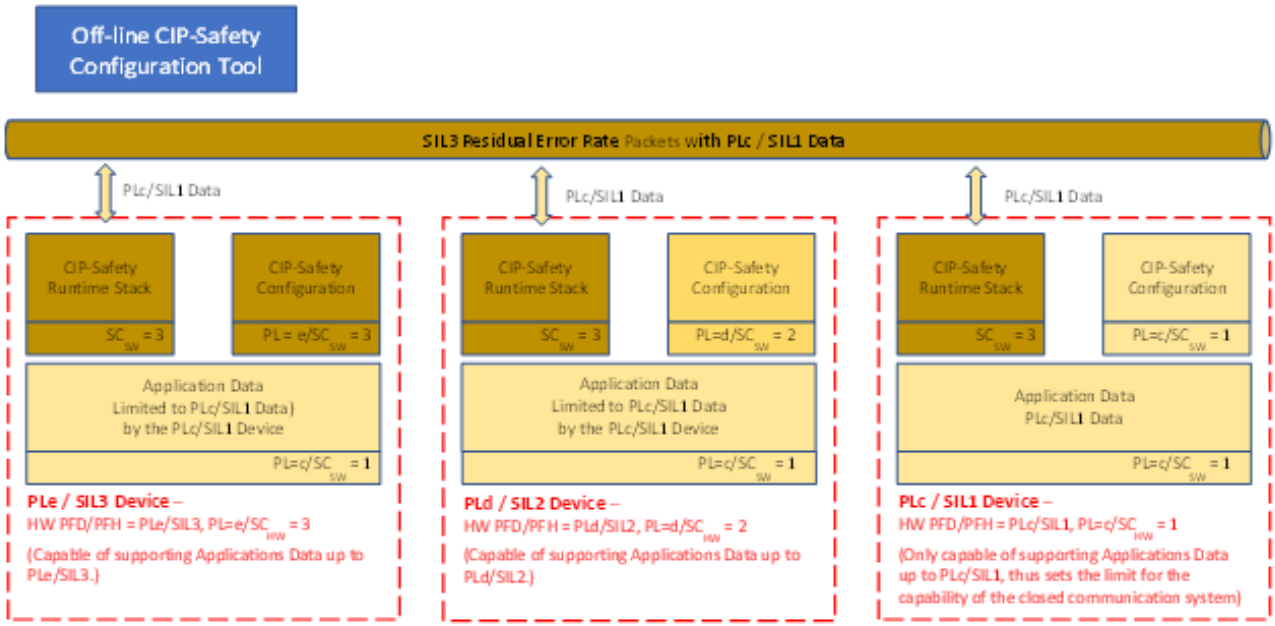


Figure 4: Proposed Safety Architecture for Devices to be Used in Closed Communication Systems

The published specification enhancement adopts the IEC 61784-3 definition of a closed communication system: a fixed number or fixed maximum number of participants with well-known and fixed properties, where the risk of unauthorized access is considered negligible. In such systems, the communication environment is not open-ended; the integrator controls the participating devices, the intended use, and the system-level safety function assumptions.

In the 2.28 Edition of published CIP Safety Volume 5, this closed-system option enables the CIP Safety protocol and device integration to be evaluated according to the required SC/PL for the application, based on risk assessment. Table 2 summarizes the differences in how the CIP Safety stacks are to be integrated into devices meant for use in the traditional and closed communication systems. The device safety manual must identify whether the device is solely for closed communication systems, state the SC/PL for such devices, and instruct implementers that the lowest SC/PL device determines the SC/PL limit of the closed communication system and the safety functions using it.

Table 2: Contrasts The Two Integration Paths

Dimension	Traditional SC3 non-interference path	Closed communication system path
Primary objective	Maintain SC3 of the CIP Safety stack within the device integration environment.	Maintain the required SC/PL of the safety function in a controlled closed communication system.
Supporting software implication	OS/BSP/resource-management software providing independence must support the highest SC being protected.	Supporting software is assessed according to the required SC/PL of the closed-system application context.
Hardware implication	Lower-SC hardware may not preserve SC3; separate SC3 hardware may be required.	Hardware capability must meet the closed-system safety function claim; the lowest node limits the claim.
Integrator responsibility	Lower burden: certified SC3-compatible devices reduce system-level selection burden.	Higher burden: integrators must control participants, properties, access, safety manuals, and risk analysis. The closed system must be maintained throughout the entire safety lifecycle of the system, not just at the time of commissioning

Best fit	Open/general CIP Safety deployments and SIL3 safety functions.	Controlled machinery/robot cells where the risk assessment requires SIL1/SIL2 or PLc/PLd and the network is closed.

Certification, Safety Manual and Conformance Implications

The ODVA conformance policy was updated to support closed communication systems and ISO 13849 certification paths. A certificate or associated report may declare either SIL3/SC3 capability or the achieved PL/SIL together with an explicit restriction that the device is intended solely for closed communication systems. Safety manuals become the key interface between device developer and integrator: they must state closed-system-only use throughout the entire safety lifecycle of the system, SC/PL capability, and the rule that the lowest SC/PL participant limits the closed communication system. Updated Edition 2.28, Volume 5 that included support for closed communication systems, has also been certified by TUV for compliance with safety standards.

The conformance impact is primarily a white-box documentation and inspection impact rather than a Black Channel protocol test impact. The black-box conformance routines remain the same, and safety manual instructions are updated to verify the new requirements.

Conclusion

CIP Safety's Black Channel model and end-to-end diagnostics remain central to its safety value. The question addressed in this paper is whether SC3 non-interference requirements should always propagate down into every supporting software and hardware layer when the application safety function does not require SC3 and the communication system is closed. This paper shows that a proportional answer is valid: for open systems and SIL3 claims, maintain SC3 preservation expectations; for closed communication systems, allow the integration claim to align with the risk-assessed SC/PL of the safety functions, with the system integrator responsible for maintaining the closed-system assumptions.

This interpretation preserves the communication residual error model while reducing disproportionate design burden in controlled machinery and robotics applications. It also creates a clearer certification narrative: the protocol remains strong, the device safety manual declares the closed-system constraints and SC/PL, and the integrator limits system claims according to the weakest participating device. By aligning safety design with actual risk requirements, this approach enables practical, scalable CIP Safety deployment across diverse industrial applications.

Acknowledgements

The authors gratefully acknowledge the contributions of Erik Jonsson of ABB Robotics, and Xiaobo Peng of Rockwell Automation to the SIG discussions on this subject

References

[1] ODVA, The CIP Networks Library, Volume 5: CIP Safety, Ann Arbor: ODVA, Inc., 2005-2026.
[2] IEC 61784-3:2024, Edition 4.1 Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions.
[3] IEC 61508-2:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
[4] IEC 61508-3:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements
[5] ISO 13849-1:2023, Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design.

****

The ideas, opinions, and recommendations expressed herein are intended to describe concepts of the author(s) for the possible use of ODVA technologies and do not reflect the ideas, opinions, and recommendation of ODVA per se. Because ODVA technologies may be applied in many diverse situations and in conjunction with products and systems from multiple vendors, the reader and those responsible for specifying ODVA networks must determine for themselves the suitability and the suitability of ideas, opinions, and recommendations expressed herein for intended use. Copyright ©2026 ODVA, Inc. All rights reserved. For permission to reproduce excerpts of this material, with appropriate attribution to the author(s), please contact ODVA on: TEL +1 734-975-8840 FAX +1 734-922-0027 EMAIL odva@odva.org WEB www.odva.org. CIP, Common Industrial Protocol, CIP Energy, CIP Motion, CIP

Safety, CIP Sync, CIP Security, CompoNet, ControlNet, DeviceNet, and EtherNet/IP are trademarks of ODVA, Inc. All other trademarks are property of their respective owners.