

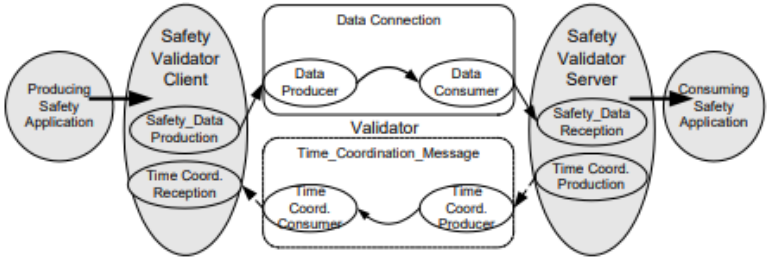
Re-examining Non-Interference Requirements in CIP Safety Devices for Closed Communication Systems

Arun K Guru, Rockwell Automation
Steven Seidlitz, Rockwell Automation
Jim Grosskreuz, Rockwell Automation
Stina Hornstrom, ABB Robotics
David Crane, ODVA

October 21, 2026

Background – CIP Safety and Black Channel

- CIP Safety is based on IEC 61784-3 Black Channel principles.
- The communication path is treated as unknown, faulty, and not safety-trusted.
- The Safety Communication Layer detects corruption, masquerade, delay, loss, repetition, insertion, and related faults.
- Residual communication failure rates remain SIL3-compatible through protocol-level diagnostics.
- CIP Safety's Black Channel model already provides strong end-to-end communication diagnostics.
- The key issue is not residual communication error rate, but how Systematic Capability requirements are allocated.



Single-Cast Safety Function Block Diagram

© 2026 ODVA, Inc.
All rights reserved.

SIL3 FSCP – Faults

For a SIL 3 Functional Safety Communication Profile, or FSCP, the two fault classes require fundamentally different evidence:

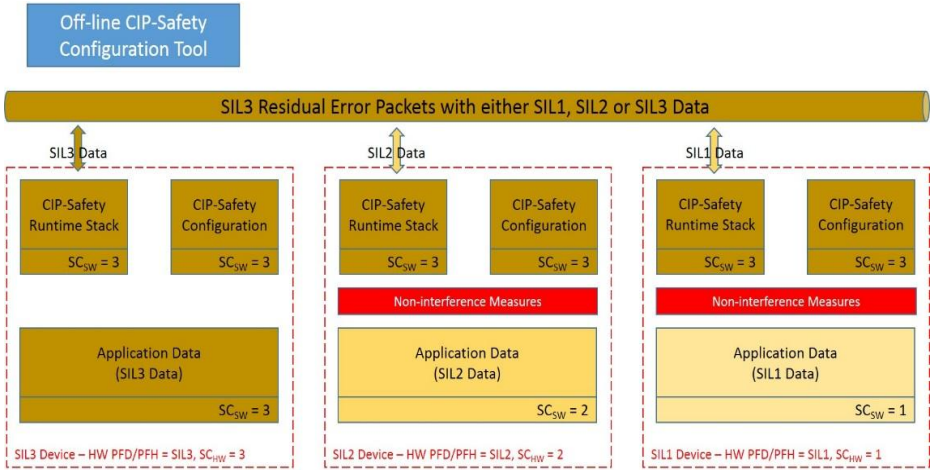
- **Random hardware faults** arise from physical degradation or transient physical effects and occur at unpredictable times. They are addressed primarily through architecture, diagnostics, fault detection, fail-safe reaction, and quantitative residual-error analysis.
- **Systematic faults** are repeatable faults created by specification, design, implementation, configuration, manufacturing, integration, maintenance, or operating-process errors. They are addressed primarily through functional-safety management, lifecycle controls, verification, validation, independence, competence, configuration control, and proven development methods.

FSCP SIL 3 capable, SIL achievement depends on **random hardware integrity, architectural constraints, and systematic capability**.

© 2026 ODVA, Inc.
All rights reserved.

Why This Issue Matters

- A SIL3-capable CIP Safety stack may be integrated into devices whose safety functions require only SIL1/PLc or SIL2/PLd.
- A strict SC3 non-interference interpretation can force SC3 requirements into supporting software, OS, BSP, timing services, and hardware.
- This can increase engineering burden, product cost, latency, and architectural complexity.
- Gateway-style isolation may be unsuitable for robotics and machinery applications requiring direct, time-critical communication.



Safety Architectures for Realizing CIP Safety Devices

© 2026 ODVA, Inc.
All rights reserved.

Typical Systematic Faults

Safety requirements faults

- Safety communication threats were incompletely identified.
- Maximum network delay or age was specified incorrectly.
- The maximum number of communicating nodes was omitted.
- Residual error probability was allocated incorrectly.
- Safe-state behavior following timeout was ambiguous.
- Startup, restart, reset, or connection-recovery behavior was unspecified.

© 2026 ODVA, Inc.
All rights reserved.

Typical Systematic Faults

Protocol design faults

- CRC polynomial, initialization, coverage, or concatenation is incorrect.
- Safety CRC does not protect all safety-relevant fields.
- Sequence counter has an unsafe rollover or resynchronization rule.
- Time monitoring admits stale data.
- Connection identifiers do not provide sufficient authenticity.
- **The protocol accepts an unintended producer or consumer.**
- Error handling permits unsafe data to remain valid.
- The assumed maximum fault number is inconsistent with the analysis.
- Fragmentation, reassembly, routing, or gateway behavior is not covered.

© 2026 ODVA, Inc.
All rights reserved.

Typical Systematic Faults

Implementation faults

- Incorrect byte order or CRC implementation
- Race condition between communication and safety application tasks
- Counter updated before message validation finishes
- Timeout implemented with a non-independent or overflowing time base
- **Unsafe data copied before authenticity and integrity checks complete**
- **Compiler optimization exposing an uninitialized value**
- **Diagnostics disabled in a production build**
- **Incorrect handling of duplicate, delayed, or reordered packets**

© 2026 ODVA, Inc.
All rights reserved.

Typical Systematic Faults

Configuration and integration faults

- **Wrong safety network number, connection ID, timeout, or signature**
- Safety device replaced without validating its identity or configuration
- **Standard and safety data objects incorrectly mapped**
- Downloaded configuration not protected by a safety signature
- Incompatible FSCP revisions allowed to establish a connection
- Safety response time calculated without all network and device delays

© 2026 ODVA, Inc.
All rights reserved.

IEC61508 Recommended Steps for Avoiding Systematic Faults

Route 1S developed SIL 3 FSCP implementations require IEC 61508-2 and IEC 61508-3 measures for avoiding and controlling systematic faults.

Key activities include:

- Functional-safety management plan
- Safety requirements specification
- Communication threat and failure analysis
- Architecture and protocol design specification
- Hardware/software partitioning
- Defined coding and design standards
- Bidirectional traceability
- Verification at each lifecycle phase
- Independent review appropriate to SIL 3
- Validation against the safety requirements
- Configuration and change management
- Anomaly management
- Tool qualification or confidence justification
- Competence management
- Functional-safety assessment
- Safety manual and integration constraints

© 2026 ODVA, Inc.
All rights reserved.

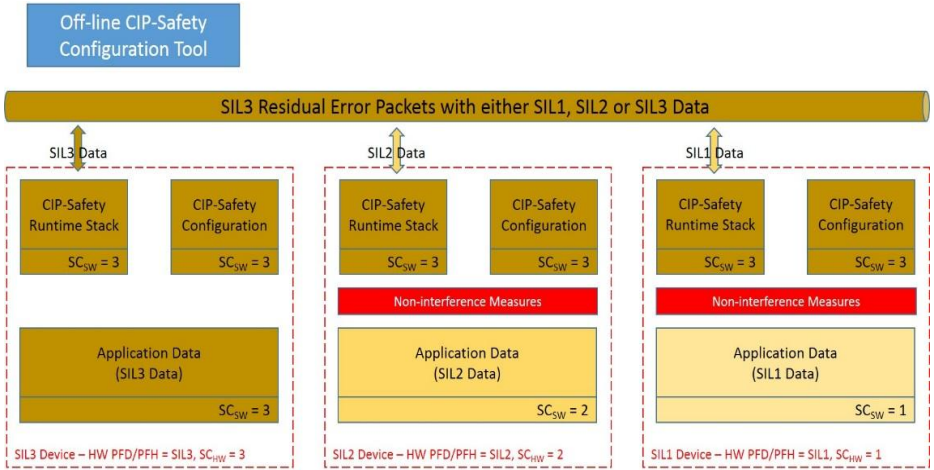
Problem Statement

- There is a mismatch between communication-layer diagnostic strength and device-level Systematic Capability allocation.
- The CIP Safety protocol may provide SIL3-compatible communication error performance even when the application safety function requires less than SIL3.
- Preserving SC3 of the stack through all supporting layers and possible implementations may exceed the system-level risk assessed SC need.
- The practical result can be over-engineering and reduced scalability for lower-SIL/PL devices.

© 2026 ODVA, Inc.
All rights reserved.

Mixed Criticality and Non-Interference

- IEC 61508 mixed-criticality principles require independence between software elements with different safety integrity levels.
- Part -3, Annexure F techniques focus on spatial and temporal independence, memory separation, execution-time control, and shared-resource management.
- **If supporting software provides non-interference, that software must support the highest Systematic Capability it protects.**
- This makes SC3 preservation difficult on SC1 or SC2 device platforms.



© 2026 ODVA, Inc.

All rights reserved.

Closed Vs Defined Communication Systems

- Defined Communication System – IEC61784-3 Edition 4.1

3.1.11
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

- Closed Communication System – IEC61784-3 Edition 4.1

3.1.6
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

[SOURCE: IEC 62280:2014, 3.1.6, modified – transmission replaced by communication]

Proposed Closed-System Interpretation

- Retain SIL3-compatible communication residual error performance for broad CIP Safety compatibility.
- In closed communication systems, evaluate CIP Safety integration according to the SC/PL required by the safety functions.
- The system integrator controls participants, properties, access assumptions, and safety function requirements.
- The lowest SC/PL participating device limits the closed communication system claim.
- Traditional SC3 preservation remains applicable when SC3 is required or when the system is not closed.

© 2026 ODVA, Inc.
All rights reserved.

FMEA Findings

- FMEA evaluated interference scenarios such as wrong Producer ID, wrong rollover count, wrong timestamp, masquerade, data integrity error, timeliness error, and authenticity error.
- Most cases remain safe because the consumer detects CRC, timeliness, or data integrity mismatches.
- Residual dangerous cases require coupled failures: a producer-side overwrite combined with a complementary Black Channel error pattern that escapes diagnostics.

FMEA Analysis of Coupled Error Modes

Failure Scenario	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.	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.

© 2026 ODVA, Inc.
All rights reserved.

Traditional vs. Closed Communication System Paths

- Traditional path: maintain SC3 of the CIP Safety stack within the device integration environment.
- Closed-system path: maintain the required SC/PL of the safety function in the controlled application context.
- Traditional path may require SC3-capable supporting software and hardware.
- Closed-system path allows lower-SC/PL platforms when justified by risk assessment and documented in the safety manual.

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.
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.

© 2026 ODVA, Inc.
All rights reserved.

Certification and Conformance Implications

- ODVA conformance policy was updated to support closed communication systems and ISO 13849 certification paths.
- Support for Closed Communication Systems was integrated into ODVA CIP Safety Specification, Volume 5, Edition 2.28 was certified by TUV Rhineland.
- Vendor Certificates or reports may declare SIL3/SC3 capability or the achieved PL/SIL with closed-system-only restrictions.
- Safety manuals become the primary interface between device developer and system integrator.
- Black-box conformance routines remain unchanged; documentation and inspection requirements are updated.

© 2026 ODVA, Inc.
All rights reserved.

Key Takeaways

- CIP Safety's Black Channel diagnostics remain intact and central to safety value.
- The proposed change concerns proportional allocation of Systematic Capability in closed communication systems.
- Closed-system use enables scalable adoption in controlled machinery and robotics applications with SIL1/SIL2 or PLc/PLd requirements.
- The safety claim must align with the risk assessment and the weakest participating device.
- Safety manuals and system integrator responsibility are essential to maintaining the closed-system assumptions.

© 2026 ODVA, Inc.
All rights reserved.

Conclusions

- A proportional closed-system interpretation preserves the protocol's communication safety strength while avoiding unnecessary SC3 platform burden.
- This approach aligns safety design with actual risk requirements and enables practical CIP Safety deployment across diverse industrial applications.
- Final message: strong protocol, clear safety manual, controlled system boundaries, and integrator-owned system-level responsibility.

© 2026 ODVA, Inc.
All rights reserved.


2026
ODVA
Industry Conference and Annual Meeting