EVALUATING THE COVERAGE OF DIVERSE CIP SAFETY MECHANISMS & ITS INTEGRATION IN HIGHLY DYNAMIC INDUSTRIAL ENVIRONMENTS

Riya Rahul Shah, Senior Functional Safety Lead
Shyam Sundar Pal, Firmware Architect
Utthunga Technologies

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

1. Abstract

The emergence of Industry 4.0 has accelerated the adoption of reconfigurable and software-defined manufacturing systems. These systems rely increasingly on programmable controllers, distributed input/output devices, industrial Ethernet networks, and dynamically integrated safety functions. Functional safety communication profiles such as CIP Safety apply the black-channel principle defined in IEC 61784-3 [2]. Under this principle, standard communication infrastructure may be used to transport safety-related information, provided that an independent end-to-end safety communication layer detects or controls the assumed communication errors.
CIP Safety is specified in Volume 5 [1] of the ODVA CIP Networks Library and standardized as Functional Safety Communication Profile 2/1 in IEC 61784-3-2 [2]. It uses safety Cyclic Redundancy Checks (CRCs), timestamps, rollover counts, time-expectation monitoring, producer and consumer identification, redundant data encoding, cross-checking, and connection supervision. Collectively, these mechanisms address communication failures [7] such as message repetition, loss, insertion, incorrect sequence, corruption, delay, unintended coupling, increased data age in bridges, and addressing errors.

This paper evaluates the coverage provided by these mechanisms within the CIP Safety producer–consumer model through Communication Failure Mode and Effects Analysis (Communication FMEA) [4]. The assessment considers unicast and multicast connections, the required Extended Format, and the deprecated Base Format where legacy compatibility remains relevant. The Communication FMEA yields integration assumptions that are subsequently evaluated against product-level implementation faults, including memory corruption, partial DMA overwrite, timestamp-processing errors, scheduling faults, incorrect configuration handling, and corruption occurring before cyclic redundancy check (CRC) generation or after message validation. Product level FMEA thereby supports traceability and validation of those integration assumptions.

The analysis demonstrates CIP Safety provides strong detection of communication-channel errors. To support complete product or system safety, the paper serves as a guidance for root-cause identification, diagnostic granularity, system availability, internal non-interference, semantic validation of process values, and allocation of the complete system reaction time. The paper therefore proposes an assessment methodology that maps communication FMEA, product FMEA [4], Functional Requirement Specification identifiers, and applicable test evidence. The methodology also evaluates system-level architectural controls alongside the protocol and its interface requirements, including fault-injection testing, to provide illustrative examples for product developers, safety assessors, and standards working groups (WGs).

2. Keywords

Availability; Black-channel principle; CIP Safety; Closed communication system; Communication failure classes; Communication FMEA; Cyclic Redundancy Check; Extended Format; Functional safety; Integration faults; Multicast; Product FMEA; Residual error; SC3; Single-cast; System reaction time.

 ©2026 ODVA, Inc.

3. Definition of terms

Availability
The ability of a system or safety communication connection to remain operational when required. Availability is distinct from safety: a system can enter a safe state correctly but still have poor availability because of frequent nuisance trips or unnecessary connection terminations.

Base Format
A legacy CIP Safety message-encoding format using separate integrity checks for different message sections. Volume 5, Edition 2.28 [1], deprecates Base Format and requires Extended Format. Originators may optionally retain Base Format for backward compatibility.

Black-Channel Principle
A functional safety communication approach in which the underlying transmission system is not relied upon to perform safety functions. End-to-end safety mechanisms implemented by the safety producer and consumer detect or control communication errors introduced by the intervening network.

CIP
Common Industrial Protocol. An object-oriented industrial communication protocol used by networks including EtherNet/IP, DeviceNet, and ControlNet.

CIP Safety
A functional safety communication extension to CIP. It adds end-to-end safety mechanisms such as Safety CRCs, timestamps, identifiers, redundant data encoding, time expectation, and connection supervision over a standard CIP communication system.

Closed Communication System
A communication system with a defined set of participants, controlled access, and known communication characteristics. Under Volume 5, Edition 2.28 [1], devices intended solely for closed systems may declare an applicable Systematic Capability or Performance Level. The lowest device capability limits the closed system.

Communication Failure Class
A category of errors that may occur during message transmission. Examples include repetition, loss, insertion, incorrect sequence, corruption, delay, unintended coupling, increased data age, and addressing errors.

CRC
Cyclic Redundancy Check. An error-detection value calculated from selected data fields and transmitted or stored with those fields. The receiver recalculates and compares the CRC to detect corruption. A valid CRC establishes consistency of the protected encoding, but not necessarily the physical correctness of the process value.

Extended Format
The required CIP Safety encoding format that incorporates enhanced CRC coverage and rollover-count protection. Extended Format may allow an isolated invalid packet to be dropped and counted before the configured fault threshold causes connection termination.

FMEA
Failure Mode and Effects Analysis. A structured method for identifying potential failure modes, their causes, local and system-level effects, existing controls, safety reactions, evidence, and residual risks.

FRS
Functional Requirement Specification identifier. The FRS prefix is used in CIP Safety Volume 5 [1] to identify normative protocol requirements and support traceability between safety mechanisms, implementation requirements, and verification activities.

Integration Fault
A fault introduced when the CIP Safety implementation is combined with hardware, operating software, device applications, memory, Direct Memory Access, clocks, communication drivers, or other standard functions. Such faults may occur outside the direct coverage of the communication protocol.

Multicast
A communication arrangement in which one safety producer transmits safety data for consumption by multiple safety consumers. CIP Safety supplements the common production with consumer-specific time-coordination or time-correction activities.

Product FMEA
An FMEA addressing faults within a safety product, including hardware, firmware, memory, processing, configuration, interfaces, diagnostics, and safe-state control. It complements communication FMEA, which primarily considers faults introduced during transmission.
Residual Error
An error that remains undetected or uncontrolled after the specified safety mechanisms have been applied. Residual communication error is normally evaluated probabilistically and contributes to the dangerous failure rate allocated to the safety communication subsystem.
Safe State
A defined condition in which the controlled equipment presents an acceptable level of risk after a safety fault. The safe state is application-specific and may involve de-energizing outputs, stopping motion, closing a valve, or inhibiting further operation.
Safe-State Reaction Time
The maximum permitted time from the occurrence or detection of a fault until the affected safety function reaches its defined safe state. It forms part of the complete system reaction time and includes communication, logic-processing, and actuator response.
SC3
Systematic Capability 3, as defined by IEC 61508 [3]. SC3 indicates that the development and integration processes provide systematic-fault control suitable for safety functions up to SIL 3[3]. An SC3 communication stack does not automatically make the complete integrated product SC3.
Single-Cast
A point-to-point safety connection between one safety data producer and one safety data consumer. Time coordination allows the producer's timestamps to be evaluated relative to the consumer's time base.
TST
Test Specification or test identifier used to trace a safety requirement to a corresponding conformance or verification test.
Volume 5
Volume 5 [1] of the ODVA CIP Networks Library, titled "CIP Safety." It specifies the CIP Safety protocol, safety objects, device behavior, connection establishment, configuration, diagnostics, timing, and device-profile requirements.

4. Problem Statement

CIP Safety applies the black-channel principle to detect communication faults between safety producer and consumers and to transition affected functions to a defined safe state when valid, timely communication can no longer be demonstrated. Its protocol mechanisms, flexible integration model, and suitability for safety architectures up to SC 3 make it a practical choice for industrial products. Adoption at system level nevertheless requires more than protocol compliance. Integrators must configure timing parameters, interpret fault behavior, and coordinate CIP Safety with product architecture, diagnostics, and process constraints—while working within fixed protocol limits and without delaying or weakening the mandatory safety reaction. The core problem addressed in this paper is therefore not inadequate fault detection in CIP Safety, but the lack of structured, system-level guidance to balance safety integrity, operational availability, and demonstrable compliance during product integration.

4.1.1. List of bottom-up requirements and assumptions on design for integration at system level:

CIP Safety applies the black-channel principle to detect communication errors introduced between the safety producer and consumer. The protocol therefore cannot, by itself, detect an incorrect value generated before that value enters the safety communication layer, nor can it detect incorrect configuration. The standard highlights these assumptions and related interface requirements in several sections, which integrators may overlook during system design.

4.1.2. Unspecified linkage to common cause failure analysis (CCFA):

CIP Safety employs diverse mechanisms—including CRCs, timestamps, connection-specific identifiers, and actual/complement cross-checking—to address common-mode and common-cause failures. These features do not justify omitting CIP Safety features from product- or system-level common-mode and common-cause failure analysis.

4.1.3. System level requirements traceability to overall safe state, safety reaction time:

Parameters such as the Expected Packet Interval (EPI), Timeout Multiplier, Network Time Expectation (NTE), Ping Interval and asynchronous application behavior directly influence network supervision and reaction time. For multicast connections, the maximum number of consumers also influences time-coordination scheduling and the minimum permitted ping interval.

This relationship is particularly important in high-speed machinery. Network congestion, burst traffic or processing load may introduce packet loss and jitter. A delayed packet does not necessarily cause termination merely because it arrives later than one EPI; termination occurs when the consumer activity monitor or Network Time Expectation is exceeded. Nevertheless, poorly selected timing parameters can cause nuisance trips, repeated connection terminations and unnecessary production downtime.

4.1.4. Root cause identification and Diagnostic ID mapping for each communication failure:

CIP Safety provides connection-status indications and several general and extended error codes. However, it does not provide a unique standardized diagnostic identifier for every runtime communication failure and physical root cause. This limitation can lead to incorrect maintenance conclusions and reduced availability. Because not every isolated communication disturbance requires immediate connection termination. Extended Format permits limited tolerance by discarding and counting an invalid packet. However, once the specified fault threshold or timing limit is reached, the required safety reaction must not be suppressed based on an uncertain root-cause diagnosis.

4.2. Impact of the Problem

When that integration guidance is incomplete or inconsistently applied, the effects appear in operation rather than in basic protocol safety. Under high network load, packet loss, delay, and jitter can expire the consumer activity monitor or Network Time Expectation even when data integrity is not permanently lost. The result is connection termination, transition to the safe state, and avoidable production downtime—affecting availability without necessarily indicating a safety failure. Integrators must also operate within protocol bounds such as the fixed Max_Fault_Number in Volume 5 [1], Edition 2.28, which cannot be extended without affecting the SIL 3 PFH budget [3] [9]. Timing tolerance therefore depends on Expected Packet Interval, Timeout Multiplier, and Network Time Expectation, together with network and application design. Volume 5 [1] defines the relationships to network reaction time and requires its inclusion in the overall system reaction-time calculation, but it cannot confirm that a chosen configuration meets process safety time, network-load profile, and availability targets for a particular machine. If Bottom-Up Requirements (BURs), Assumptions on Design (AoDs), and Assumptions of Use are poorly documented, parameters may be set too restrictively—causing nuisance trips—or too permissively—risking exceedance of the required process safety time. Further impact arises where fault diagnosis is undefined. Without clear classification of root cause and system-level effect, teams cannot reliably distinguish transient disturbances from persistent failures. Responses such as immediate connection termination, extended debounce, or continued operation may then be either overly conservative or unsafe, especially where continued communication is needed for a controlled safety response.

4.3. Impact on the network device if not correctly addressed

- Unavailability of the system impacting performance
- Longer downtime/ maintenance time because of unknown error mode classification or root cause(s) identification

5. Overview — What Problem proposed solution solves!

This paper responds to those integration and assessment gaps while preserving mandatory CIP Safety behavior. The proposed enhancements do not modify, bypass, or delay the required safety reaction when communication integrity or timeliness can no longer be demonstrated.
Instead, the paper provides system-level configuration, diagnostic, and integration guidance to help product developers, safety assessors, and standards working groups: validate timing and tolerance choices against process safety time and network performance; document and trace BURs, AoDs, and Assumptions of Use alongside communication and product FMEA [4]; classify communication faults so responses support both safety integrity to SC 3 and defined availability objectives; and
map Functional Requirement Specification identifiers and applicable test evidence, including fault-injection evaluations, in a single assessment methodology. Taken together, these elements support wider adoption of CIP Safety by making integration more predictable and demonstrable, balancing robustness and availability without compromising the black-channel safety function.

Mechanism	**Purpose**
1. Application-specific configuration and validation of EPI, NTE and Timeout Multiplier (from BURs and AoDs)	Establish traceability between the configured communication parameters, worst-case network behavior, process safety time and overall system reaction time. Parameter selection should occur during engineering or connection configuration
2. Mapping of detected communication events to communication-error classes and T–A–DI–M categories	Map each observable event, such as a CRC mismatch, sequence error or NTE timeout, to Timeliness, Authenticity, Data Integrity or Masquerade categories, together with the resulting safety action and possible causes. Standardized diagnostic-event identifiers would support faster troubleshooting
3. Network-infrastructure optimization through traffic engineering, scheduling and tuning (CIP communication part checked in product CCFA)	Use bandwidth analysis, Quality of Service, appropriate connection priorities, multicast control, topology assessment and worst-case jitter testing to reduce packet loss and excessive delay while preserving CIP Safety compliance.
4. Documentation of Bottom-Up Requirements, Assumptions on Design and Assumptions of Use	Clearly allocate integration responsibilities at the safety-application, CIP Safety and network boundaries. This supports detection of faults outside protocol coverage, improves configuration consistency and reduces avoidable nuisance trips without weakening the required safety response.

6. Application Example

Let us consider a system of high-speed packaging machines to demonstrate effectiveness of above mechanisms. This system contains:

- Safety light curtain
- CIP Safety input module
- EtherNet/IP network
- Safety PLC
- EtherNet/IP network
- CIP Safety output module
- Drive Safe Torque Off

The light curtain [5][6] and drive are connected through two CIP Safety connections:

1. Input connection: safety input module to safety PLC.
2. Output connection: safety PLC to safety output module.

Below is the system interface diagram which is to be used for all future references.

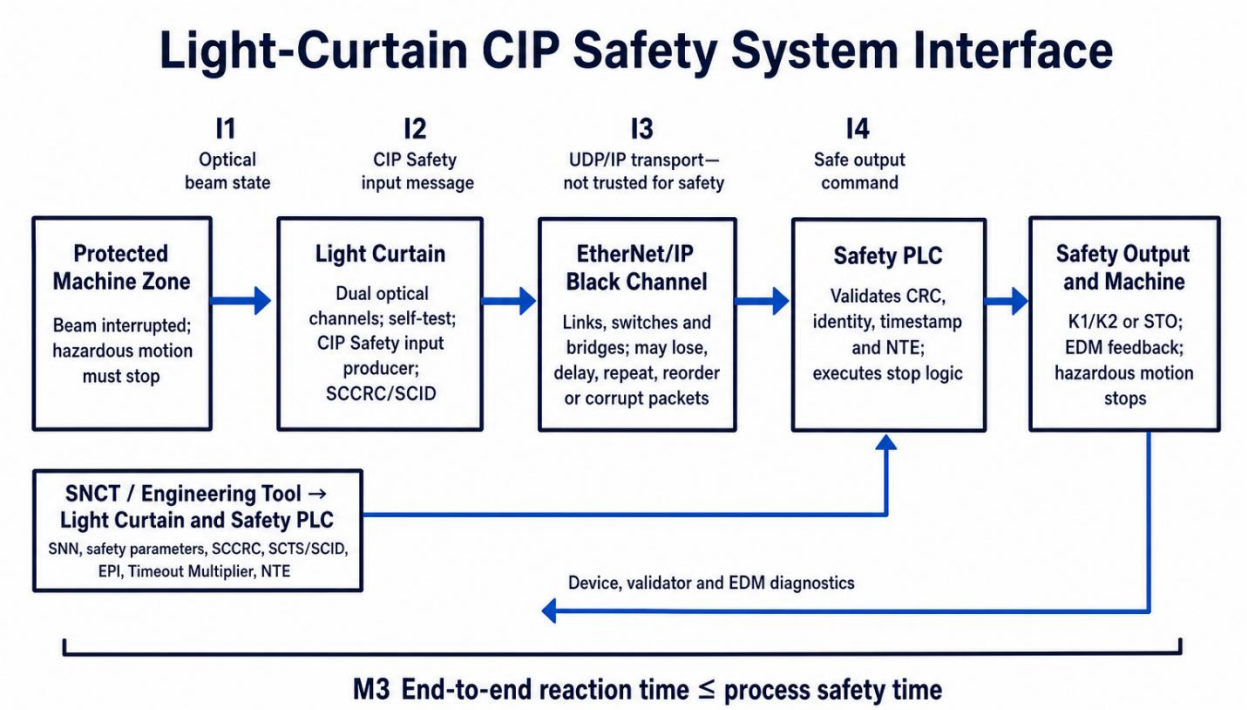


Figure1: Block diagram for Light Curtain System

Using the Keyence calculation approach[10] as a reference example and drawing on ISO 13849-1 / ISO 13855 concepts for safeguarding distance and reaction time, the following subsection illustrates typical timing values for the requirements below. The figures are illustrative; each integration must use values verified for the actual machine, drive, and safety architecture.
Safety function requirement
If a person enters the hazardous zone while hazardous motion is present, the machine shall cease hazardous motion before the person can reach the danger point. For this example, the required process safety time (PST) for that safety function is 110ms.
Therefore, the maximum permitted time to remove drive torque (including all detection, logic, output, and drive reaction contributions up to torque off) is 110ms. Any network-related reaction time (for example, CIP Safety consumer monitoring and connection handling) must be included within this budget; the remainder after non-network stages is available for the safety communication path.

6.1. Initial system configuration

6.1.1.Non-network reaction timings

Table below summarizes example non-network contributions to the overall reaction time. These values represent local sensor, controller, output, and drive stages before safety-network propagation and consumer-side monitoring are considered.

Attributes	**timings**
Light-curtain reaction time	8ms
Input-module processing time	5ms
Safety PLC processing time	10ms
Output-module processing time	4ms
Drive STO reaction time	20ms
Total non-network time	47ms

In this example, 47ms of the 110ms PST is allocated to non-network stages, leaving 63ms for network-related reaction time and any additional consumer-side processing to be accounted for in subsequent subsections.

6.1.2. Communication configuration timings

6.1.2.1. Input connection:
EPI = 10ms
Timeout Multiplier = 2
ASYNC = 1

Note, If the producing application is asynchronous to the data production, ASYNC = 1. This ASYNC parameter shall be provided to the Safety Configuration software via an EDS file entry.[1]

Using simplified volume 5 [1] equation:

$$Network\ Time\ Expectation\ Multipler\ (NTEM) = \left(EPI\ x \frac{Timeout\ multiplier + 2}{128}\right) us$$

$$NTEM = (10ms\ x\ 4)/128us$$

= 312.5, $round\ up\ to\ next\ integer$ ~313

The application is asynchronous. Therefore,

$$Input\ Network\ Reaction\ time = NTE = 313x128us = 40.06ms$$

6.1.2.2. Output Connection
EPI = 5ms
Timeout Multiplier = 2
ASYNC = 1

Using simplified volume 5 [1] equation:

$$NTEM = \left(EPI\ x \frac{Timeout\ multiplier + 2}{128}\right) us$$

$$NTEM = (5ms\ x\ 4)/128us$$

= 156.25, $round\ up\ to\ next\ integer$ ~157

$$NTE = 157x128us = 20.09ms$$

The application is asynchronous. Therefore,

$$Output\ Network\ Reaction\ Time = 20.09ms + 5ms = 25.09ms$$

6.1.3. Initial total reaction time:

System reaction time = total non-network reaction time + Input network reaction time + output network reaction time

$$T = 47ms + 40ms + 25ms = 112.16ms$$

The initial configuration exceeds the required process safety time of 110ms. It therefore cannot be accepted even though every individual parameter is within the legal CIP Safety range.
This demonstrates the system-level gap: **protocol-valid configuration does not automatically mean application-valid configuration.**

6.2. Application of four proposed mechanisms on Safety Light Curtain

6.2.1. M1- Application specific timing configuration

Purpose: Demonstrate application-specific timing configuration for the safety input connection, Parameter values below are illustrative; they must be justified for the actual producer/consumer pair, network load assumptions, and documented AoDs.
Starting assumptions (from §6.1). Required process safety time = 110ms; non-network reaction time = 47ms; network and related safety-communication budget ≈ 63ms (to be allocated among input path, output path, and any additional consumer processing).

Revised connection parameters (engineering configuration).

- If timing parameters are revised as follows:
  - Input EPI=8ms
  - Output EPI=4ms
  - Timeout multiplier=2
  - ASYNC=1

$$Revised\ NTEM\ for\ input\ connection = \frac{8ms\ x\ 4}{128us} = 250\ , round\ up\ to\ next\ integer \sim 251$$

$$Revised\ NTE = 251\ x\ 128us = 32.12ms$$

$$Revised\ Input\ Network\ Reaction\ time = 32.12ms$$

$$Revised\ NTEM\ for\ output\ connection = \frac{4msx4}{125us} = 125, round\ up\ to\ next\ integer\ \sim 126$$

$$Revised\ NTE = 126x128us = 16.12ms$$

$$Revised\ Output\ Network\ Reaction\ time = 20.12ms$$

$$Revised\ System\ Reaction\ time = 47ms + 32.12ms + 20.12ms = 99.24ms$$

The revised configuration of EPI satisfies the process safety time. However, it needs to check for increased production rate under worst case load conditions.

This completes one traceability step from BUR/AoD assumptions → configured EPI / Timeout Multiplier / NTEM → demonstrated compliance with PST. CCFA-driven network optimization (traffic engineering, scheduling) is treated separately and must remain consistent with the worst-case network behavior assumed here.

6.2.2.M2- Communication Error and T-A-DI-M Diagnostic Mapping

The following example shows why detected communication events should be classified and linked to T-A-DI-M framework. Tagging an observed behaviour—such as a CRC failure followed by recovery on the next valid packet—to a Data Integrity class helps maintenance teams identify root cause and restore production more quickly. During development, the same mapping gives engineers a repeatable way to relate protocol behavior to design assumptions, reproduce faults, and target fixes.

Assume there is EMI interference on the safety input pack of light curtain, and the sequence is as below:

1. Operator enters protected area.
2. Light curtain changes to unsafe state.
3. Input module captures the unsafe state.
4. First safety packet is corrupted during transmission.
5. Safety CRC check fails at the PLC.
6. Invalid packets are discarded.
7. Consumer_Fault_Counter becomes 1.
8. Connection remains active because Max_Fault_Number is 2.

 ©2026 ODVA, Inc.

9. The next valid packet carries the unsafe state.
10. PLC processes the unsafe state.
11. PLC sends the STO command.
12. Output module removes torque.

Proposed diagnostic record which is based on T-A-DI-M framework of IEC 61784-3 edition 4 [2] is as follows:

- Diagnostic event: Safety Data CRC Mismatch
- T–A–DI–M class: Data Integrity
- Affected connection: Light Curtain Input Connection
- Detection point: Safety Validator Consumer
- Protocol action: Packet discarded
- Consumer fault count: 1 of 2
- Connection state: Active
- Safety-data age: Within NTE
- Probable lower-layer correlation: FCS error increase
- Final system action: Next valid production processed

Depending on the use case the framework will identify the closest matches.

- NTE exceeded
  → Timeliness
- SafetyOpen connection-identity mismatch
  → Authenticity
- Standard message received by safety consumer
  → Masquerade
- Safety CRC or cross-check mismatch
  → Data Integrity

Note, the diagnostic event ID identifies the detected safety-layer symptom, not necessarily the physical root cause.

6.2.3.M3- Network Infrastructure Optimization

The trade-off between shorter Expected Packet Intervals and increased network loading affects shared infrastructure used by multiple safety connections. This is appropriately treated as a common-cause concern: a single overloaded switch, multicast domain, or inconsistent Quality-of-Service policy can disturb several CIP Safety paths together. Product-level common-cause failure analysis (CCFA), for example using IEC 61508-2 Annex F, is used to verify that proposed network controls are adequate under worst-case conditions. Although CIP Safety and related material address these topics in several places, consolidated integrator-facing guidance—such as the illustrative example below—helps ensure that shared-infrastructure dependencies and corresponding network measures are not overlooked during system analysis.

The proposed network controls are:

- Use point-to-point safety connections unless multicast is explicitly required.
- Assign safety I/O traffic an appropriate EtherNet/IP priority.
- Configure Quality of Service consistently in devices and switches.

- Control multicast propagation using managed network infrastructure.
- Limit unnecessary broadcast and multicast traffic.
- Verify switch queueing and forwarding delays.
- Reserve sufficient bandwidth for safety, standard and diagnostic traffic.
- Measure packet delay, loss and jitter under maximum vision-system and production load.
- Monitor Ethernet Link Object counters for Frame Check Sequence (FCS) errors, discards and link failures.
- Revalidate timing after topology, switch or traffic changes.

The network test must demonstrate that
Worst case successful message time ≤ NTE calculation &
Worst case total system reaction time ≤ expected system reaction time.

6.2.4.M4- List of bottom-up requirements and assumptions on design

Off-the-shelf stacks and safety controllers need documented integration assumptions to be used safely. Volume 5 [1] defines related obligations in several sections, but not in one traceable place. The BURs and AoDs below are derived from Volume 5 [1]; this list is illustrative only. The paper proposes a dedicated BUR–AoD annex with consolidated, largely vendor-independent guidance for integrators—as integration/specification guidance only, not as changes to mandatory CIP Safety runtime behaviour. Additional BUR-AoDs can be ones that support traceability to connection configuration (EPI, Timeout Multiplier, NTE), communication FMEA, and system-level common-cause analysis, safe state definition, and reduce the risk that integrator obligations are overlooked.

The following integration requirements and assumptions are derived for the same application example.
Bottom-up requirements:

- The light-curtain state shall be validated before it is supplied to the CIP Safety producer.
- The input safety buffer shall be protected from unauthorized DMA and standard-software access.
- The input module shall detect stale acquisition data even if communication packets continue to be produced.
- The safety PLC shall place the affected safety function in its safe state when the input connection becomes faulted.
- The output module shall locally remove drive torque if valid output data is not received within its configured NTE.
- Invalid Safety CRC packets shall never be passed to the safety application.
- Diagnostic processing shall not delay the required safety reaction.
- The system shall meet the derived process safety time (for this example: 110ms) under maximum specified traffic load.

Assumptions on design and use:

- The network contains no more than the assessed number of switches.
- The specified QoS configuration remains enabled. QoS, bandwidth, multicast and wireless roaming assumptions must be documented.
- Safety and standard traffic remain within the verified bandwidth envelope.
- The input and output applications are treated as asynchronous unless synchronization is demonstrated.
- Device reaction times are taken from certified Safety Manuals and/or EDS.
- Any change to topology, EPI, timeout, switch configuration or production traffic triggers reaction-time revalidation. That is replacing switches, wireless access points, or routes shall trigger performance revalidation.
- The drive reaches its defined safe state when STO is activated.
- A communication failure does not prevent the output module from performing its local safe-state reaction.
- The residual error target remains satisfied at all safety devices

- SC3 compliance of CIP safety communication features does not guarantee up to SIL3 [3] compliance, system integrator must additionally validate hardware integrity, application behaviour, communication configuration, reaction time, and safe-state behaviour.

6.3. Sequence Diagram

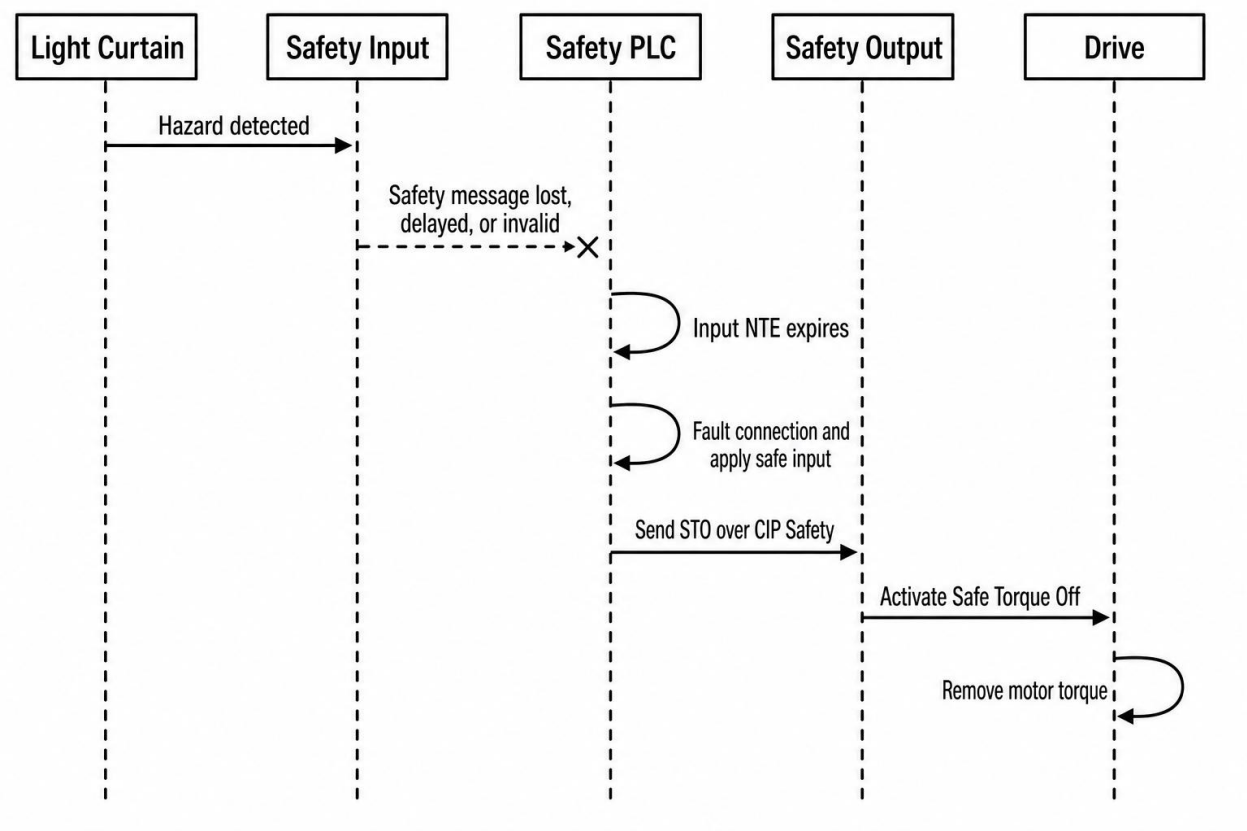


Figure 2: Sequence diagram of Light Curtain

Safety path following communication failure. If no valid input message is accepted before NTE expires, the PLC faults the input connection and commands Safe Torque Off. The drive must reach its safe state within the permitted process safety time.

6.4. Alignment with ODVA CIP Safety (Volume 5 [1])

The proposed solution aligns with and extends ODVA CIP Safety principles as defined in Volume 5_2.28.

Proposed Mechanism	ODVA CIP Safety Equivalent	Volume 5 [1] / Training Reference
Application of specific timing configuration	System Reaction time	2-7: System Reaction Time, 2-7.4: Equations for calculating Network reaction times (2-126-2-129)
Communication Error and T-A-DI-M Diagnostic Mapping	Four types of error: Integrity, Authenticity, Timeliness, and Masquerade as per IEC 61784-3 Edition 4 [2]	2-8: Network PHF of extended format (2-130)
Network Infrastructure Optimization	Prioritizing safety traffic on EtherNet/IP	2-10.4: Priority for Safety Connections (2-141)
Network Infrastructure Optimization	Point-to-Point connections	2-10.2: Default Safety I/O Service (2-141)

 ©2026 ODVA, Inc.

Network Infrastructure Optimization	Measures to protect standard devices from safety devices	2-1.2.11: Measures to Protect Standard Devices from Safety Devices (2-9)
Network Infrastructure Optimization	EPI, NTE, and network acceptance	2-6.1.1: NTE configuration (2-107-2-108) 2-7.2 Network Time Expectation
Network Infrastructure Optimization	Devicenet performance methodology	2-9.2.1: Devicenet safety performance (2-136)
Bottom-up requirements and assumptions on design	Complete devise integration and non-interference	2-2.1: High Level View of a Safety Device (2-44-2-46)
Bottom-up requirements and assumptions on design	Configuration Integrity requirements	7-1.1.4: Configuration Process Justification (7-6-7-7)
Bottom-up requirements and assumptions on design	User Verification and Safety Manual instructions	7-5.1: Verification Process (7-16)
Bottom-up requirements and assumptions on design	Connection termination and application safe state	2-1.3.2 Connection Termination (2-9)
Bottom-up requirements and assumptions on design	Safety Device fault behavior	2-1.11 Safety Device Requirements (Device behavior)

6.5. Communication and Product FMEA

6.5.1. Communication FMEA

Boundary and assumptions
The analysis considers a generic architecture: dual-channel light curtain → CIP Safety input producer → safety PLC consumer → safety output / final switching element. Once the safe state is confirmed, the safety function is assumed to request de-energization and cessation of hazardous motion. Actual device architecture, process safety time, and severity, occurrence, and diagnostic coverage ratings must be supplied by the device vendor and system integrator for the specific application.

Enhanced FMEA introduction

The communication FMEA in this paper is extended beyond a conventional fault list. Having consolidated the integration mechanisms M1–M4 (application-specific timing configuration; communication-event classification; network infrastructure / common-cause considerations; and BUR–AoD traceability), each failure mode and observable event should be mapped to:

1. T–A–DI–M category (Timeliness, Authenticity, Data Integrity, Masquerade), and
2. One or more mechanism IDs (M1–M4) where the failure is addressed, mitigated, or evidenced.

If a failure mode maps to M4, it should be read as conditional on integrator/vendor compliance with stated BURs and AoDs. If it maps to M3, the system integrator should explicitly include that fault in common-cause failure analysis. If it maps to M2, it should carry a T–A–DI–M class and, where defined, a diagnostic / DTC identifier for field and development use. Feedback loop: If an identified failure mode or field observation does not map to an existing mechanism but clearly belongs to the scope of M1–M4, that item is treated as a candidate to extend the mechanism list, the BUR–AoD catalogue, or the diagnostic table. This keeps the methodology living rather than frozen at first publication.

FMEA ID	Failure	Example Cause (s)	Effect	Existing mechanism(s)	FRSID	TestID	Mapping to new mechanism And T-A-DI-M
CF-01	Intermittent/ periodic communication faults	Periodic EMI or microbursts cause recurring CRC errors, packet loss, or jitter near the timeout boundary	Repeated nuisance trips reduce availability,	CRC detection, Extended format fault counter/ max_fault_number where applicable, timestamp and NTE timeout.	FRS13 FRS85 FRS86 FRS87	LC-TC-COM-005: inject periodic bursts at multiple phases and verify both fault threshold and worst-case stop time.	M1, M2, M4 Timeliness and Data Integrity
CF-02	Insertion, addressing errors, or masquerade	A message from another safety device or connection is delivered to the light-curtain consumer path.	Another device's "clear" state could be associated with the protected machine zone leading to safety hazard	PID/CID-seeded Safety CRC, safety/standard format separation, TUNID/OUNID and SafetyOpen configuration checks.[8]	FRS5 FRS7 FRS8 FRS153 FRS164 FRS166 FRS168	LC-TC-COM-004: substitute a valid packet and configuration from another light curtain, SNN or connection.	M4, M2 Authenticity and Masquerade
CF-03	Repetition or incorrect sequence	An old valid "clear" packet is replayed, duplicated or delivered out of order after the curtain becomes blocked.	Stale process data could be treated as current and delay the stop request.	Timestamp age, Monotonic timestamp behavior, NTE, EF out-of-sequence handling	FRS84 FRS74 FRS372 FRS80/ 81	LC-TC-COM-003: duplicate, reorder and replay packets across timestamp rollover and restart boundaries.	M1, M2 T- Timeliness

6.5.2. Product FMEA

This extended Product FMEA assesses the complete safety chain from the sensor and CIP Safety communication path through the safety controller, output device, and final machine response (including hazardous-motion stop). It complements the Communication FMEA (§6.5.1) by covering application and machine-level effects that are not visible from the protocol layer alone. Each failure mode is analysed for its effect on functional safety, process safety time, and availability, and is cross-linked to integration mechanisms M1–M4 where applicable: M1 (timing and reaction-time validation), M2 (T–A–DI–M classification and diagnostics), M3 (common-cause / shared infrastructure), and M4 (compliance with BURs and AoDs). Communication FMEA entries feed this table; Product FMEA entries that imply new

communication or integration gaps feed the feedback loop described in §6.5.1. Although the black-channel principle preserves communication safety integrity when intermediate network components change, those changes can still affect latency, packet loss, nuisance tripping, diagnostic resolution, and overall availability. Product FMEA makes those system-level consequences explicit.

FMEA ID	Failure	Example Cause (s)	Effect	Existing mechanism(s)	TestID	Mapping to new mechanism And T-A-DI-M
PF-01	Memory, DMA or data-mapping corruption before Safety CRC generation	The input image or safety assembly is overwritten with a plausible “clear” state before it is protected.	The protocol can transport the wrong value with a valid CRC because corruption occurred before CRC calculation	Memory protection, end-to-end data ownership, range/state plausibility, diverse readback and non-interference evidence.	LC-TC-PRD-001: corrupt each pre-CRC data-transfer boundary and demonstrate detection before transmission.	M4 Data Integrity before safety input transmits on black channel
PF-02	Wrong or incomplete safety configuration	Incorrect response time, operating mode, muting behavior or safety parameters are downloaded or retained.	The light curtain may respond too slowly or permit an unsafe operating condition.	SCCRC, SCTS/SCID, SNCT workflow, ownership checks, configuration locking and user verification.	LC-TC-CFG-001: change one safety parameter, attempt partial/old downloads and verify SCID mismatch or controlled recommissioning.	M4, M2 Data Integrity (of configuration) Masquerade (in case wrong device or owner is configured)
PF-03	PLC/output/actuator does not achieve the machine safe state	The consumer detects the blocked beam or communication timeout, but the final switching element remains energized.	CIP Safety reaches its communic-ation safe state, yet hazardous motion continues.	Safety application logic, output diagnostics, external-device monitoring and de-energized safe-state validation.	LC-TC-SYS-001: block the curtain and inject welded contactor/output faults; measure complete hazard stopping.	M4 NA

7. Enhanced FMEA — traceability and stakeholder benefits

The Communication FMEA and Product FMEA together form an enhanced FMEA when failure modes are mapped to T–A–DI–M, M1–M4, and (where applicable) BUR/AoD references and diagnostic identifiers.

- Standards working groups: supports a reviewable, extensible catalogue of BURs/AoDs and integration mechanisms.
- Developers: supports a consistent DTC / event-ID set tied to failure modes for reproduction and correction in development.
- System integrators: M3/M4 tags strengthen CCFA and integration checklists; M1 ties modes to validated timing.
- Maintenance: M2 mappings link field symptoms to FMEA rows and plausible causes for faster root-cause analysis.

Items that fit M1–M4 but match no current row enter a feedback loop to update the FMEA, mechanism list, BUR/AoD catalogue, or diagnostic table.

8. Conclusion

This study began by evaluating whether the safety mechanisms defined in CIP Safety provide sufficient communication-fault coverage. The assessment indicated that, when correctly implemented and configured, these mechanisms can satisfy the intended residual-error and probability of dangerous failure per hour (PFH) contribution and achieve Systematic Capability 3 (SC 3) at protocol level. At product and system level, integration gaps can nevertheless remain in timing validation, diagnostics, common-cause dependencies, and availability management; this paper and its proposals address those areas as integration and assessment guidance, not as deficiencies in the black-channel model. The study therefore extended its focus to system integration, end-to-end reaction time, common-cause failures, diagnostic accessibility, and nuisance-tripping risk. On that basis, four complementary mechanisms (M1–M4) are proposed to strengthen existing integration practice and provide consolidated, practical guidance for CIP Safety deployments without changing mandatory runtime safety behavior. The light-curtain application example demonstrates how these mechanisms can be applied in communication and product FMEAs, requirement traceability, interface definitions, and verification testing.

9. Appendix

9.1. Abbreviations and Acronyms

Abbreviation	Definition
A	Authenticity
AoD	Assumptions on Design
BF	Base Format
BUR	Bottom-up Requirement
CID	Consumer Identifier
CIP	Common Industrial Protocol
CRC	Cyclic Redundancy Check
DI	Data Integrity
DMA	Direct Memory Access
EDM	External Device Monitoring
EDS	Electronic Data Sheet
EF	Extended Format
EMI	Electromagnetic interference
EPI	Expected Packet Interval
FRS	Functional Requirements Specification
M	Masquerade

NTE	Network Time Expectation
NTEM	Network Time Expectation Multipler
ODVA	ODVA, Inc.
OUNID	Originator Unique Network Identifier
PFH	Probability of dangerous Failure per hour
PID	Product Identifier
PLC	Programmable Logic Controller
QoS	Quality of Service
RCA	Root Cause Analysis
SC/ SC3	Systematic Capability/ Systematic Capability 3
SCCRC	Safety Configuration CRC
SCID	Safety Configuration Identifier
SCTS	Safety Configuration Time Stamp
SIL	Safety Integrity Level
SNN	Safety Network Number
SNCT	Safety Network Configuration Tool
SRS	Safety Requirements Specification
STO	Safe Torque Off
T	Timeliness
T-A-DI-M	Timeliness, Authenticity, Data Integrity, and Masquerade
TCP/ IP	Transmission Control Protocol/ Internet Protocol
TST	Test Specification/ Test Identifier
TUNID	Target Unique Network Identifier

10. References

[1] ODVA, The CIP Networks Library, Volume 5: CIP Safety, Edition 2.28, November 2025, PUB00085.
[2] IEC 61784-3:2021, Functional safety fieldbuses — General rules and profile definitions.
[3] IEC 61508:2010, Parts 1–7, Functional safety of E/E/PE safety-related systems.
[4] IEC 60812:2018, Failure modes and effects analysis (FMEA and FMECA).
[5] IEC 61496-1:2020, Electro-sensitive protective equipment — General requirements and tests.
[6] IEC 61496-2:2020, Particular requirements for active opto-electronic protective devices
[7] CIP Safety™ | Common Industrial Protocol | ODVA Technologies
[8] PUB00110R4_CIP_Safety.pdf
[9] ODVA, The CIP Networks Library, Volume 7C: Integration of IO-Link Devices into the CIP Architecture, Ann Arbor: ODVA, Inc., 2019-2026.
[10] Light Curtain Installation and Safety Distance (Minimum Distance) : Safety Knowledge | KEYENCE India

****

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.