

CIP SAFETY MECHANISMS & ITS INTEGRATION IN DYNAMIC ENVIRONMENTS

Technical Paper Presentation

ODVA 2026 Industry Conference & 24th Annual Meeting

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

October 21, 2026

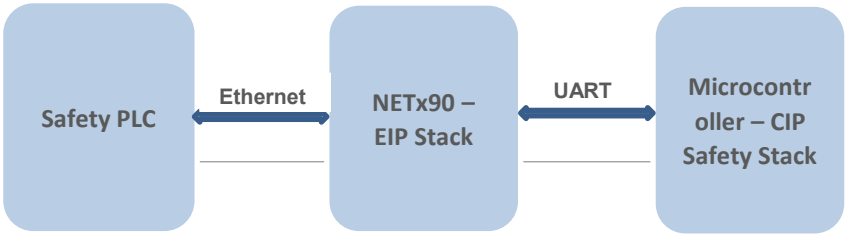
Presentation Outline

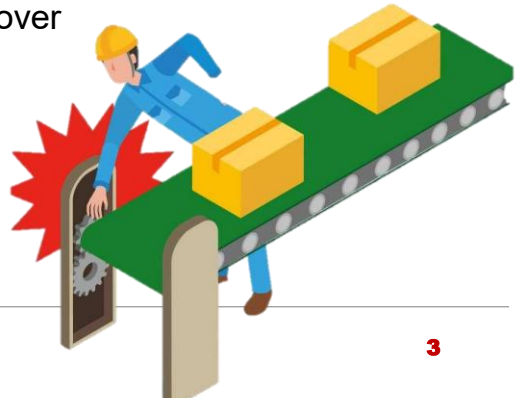
- CIP Safety- overview
- Volume 5 coverage
- problem statement + proposed solution
- Application example
- Four Mechanisms
- Communication & FMEA
- Conclusion

CIP Safety Overview

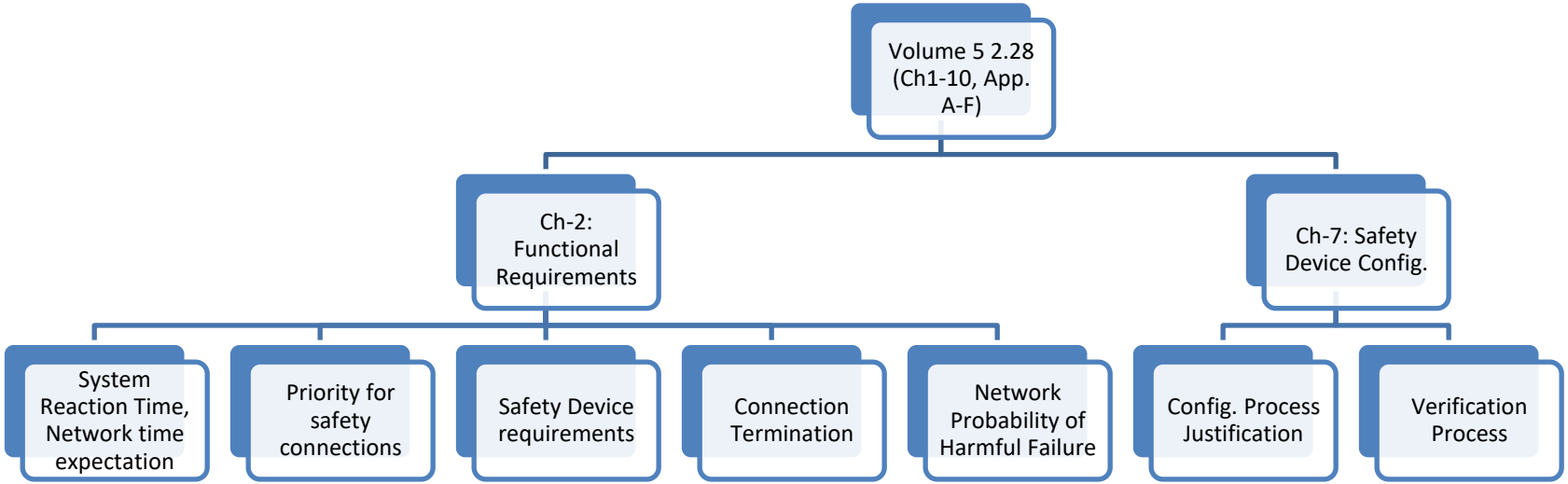
- Did you know that fatal accidents reported in manufacturing places across EU was 3367 in 2024?
- These hazards could have been avoided if functional safety was design inbuilt in these systems
- Functional safety is the freedom from unacceptable risk of physical injury or damage to health of people
- CIP Safety plays a role in ensuring communication path is suitable for functional safety architecture
- ODVA describes CIP safety as a functional safety communication protocol supporting applications upto SIL 3.

It's a black channel principle protocol which allows for safety data to transmit over non-safety qualified communication infrastructure





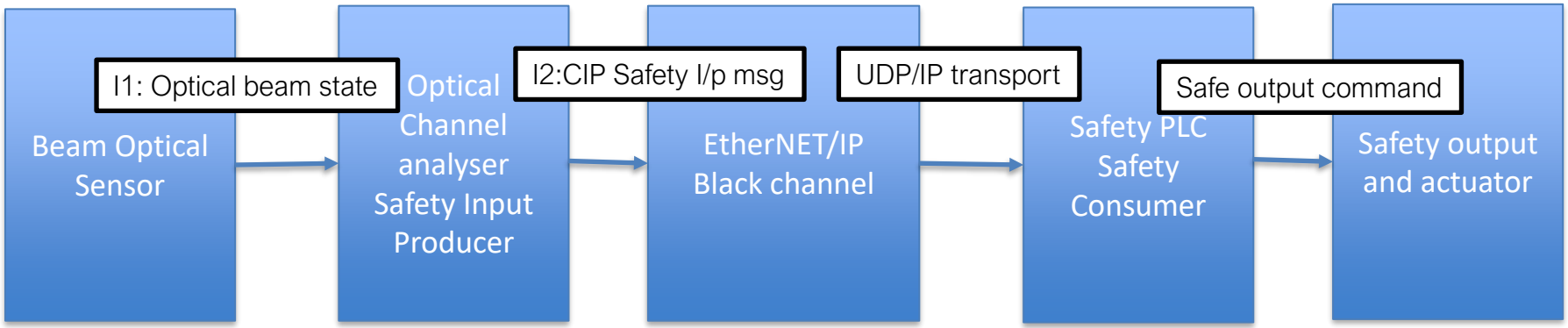
Volume 5 coverage



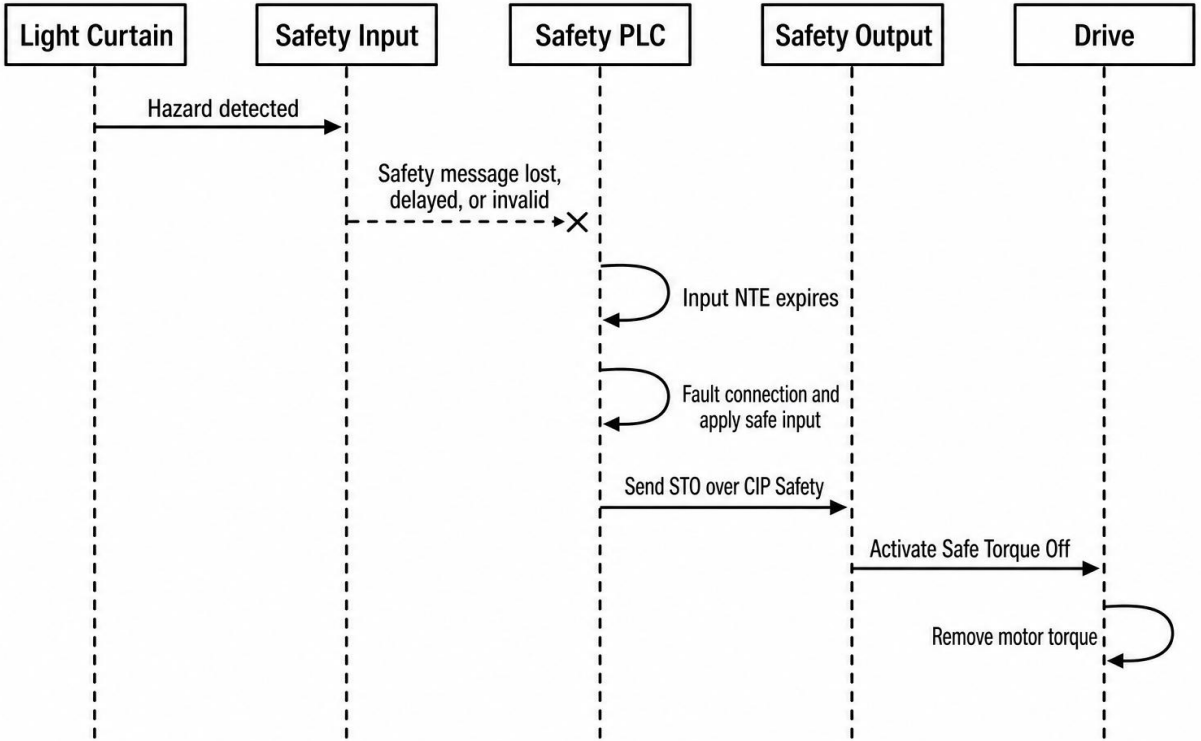
Problem Statement and Solution Overview

- Intent of this paper is to look at CIP safety integration into overall safety architecture
- When system is looked as whole, it becomes critical for integrator to know about CIP constraints, assumptions, and dependencies
- If overlooked it can lead to system which has issues with overall safety integrity, operational availability, or both.
- The solution to this is holistic approach towards system-level configuration, diagnostic, and integration while preserving CIP safety SIL level

Application Example



Sequence diagram



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

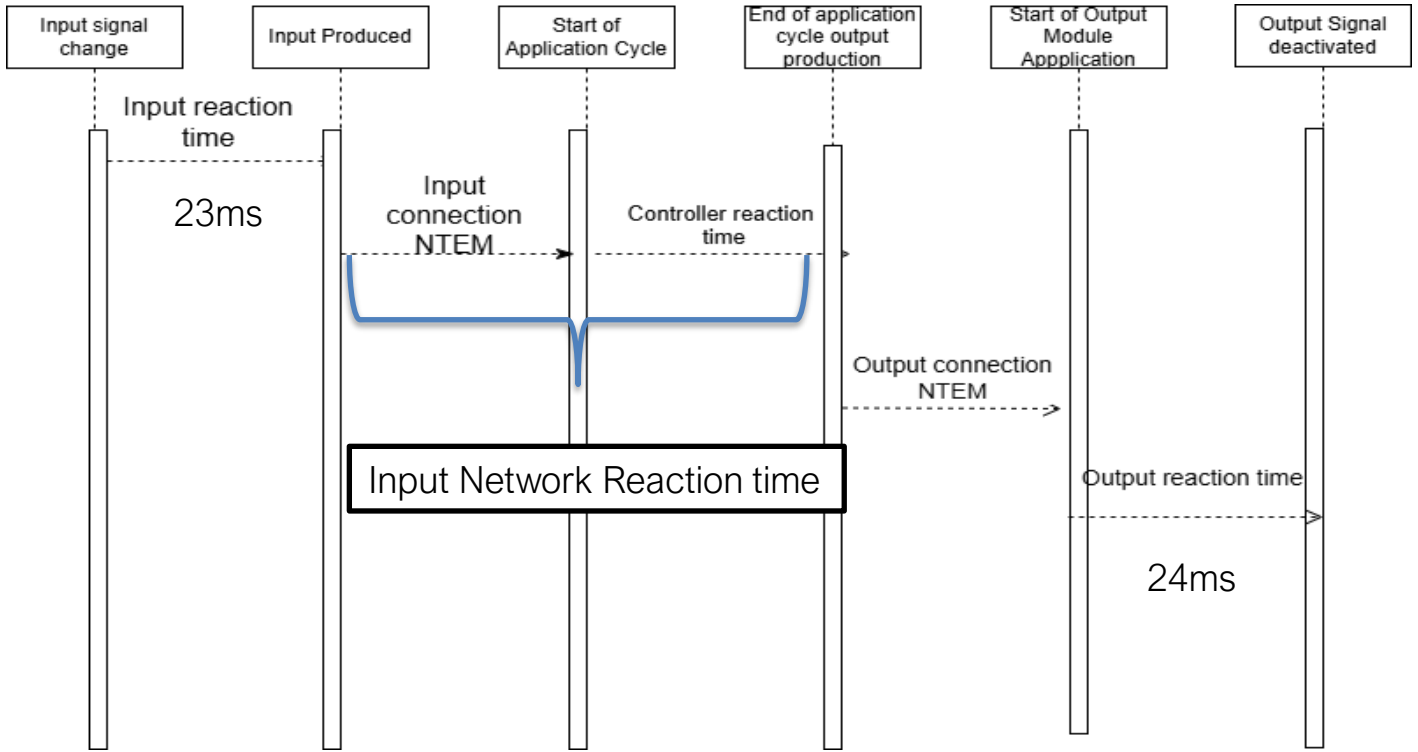
© 2026 ODVA, Inc.
All rights reserved.

Proposed Safety Mechanisms

Safety Mechanism# & title	Purpose
1. Application-specific configuration and validation of Network reaction times	Establish traceability between the configured communication parameters, worst-case network behavior, process safety time & overall system reaction time
2. Mapping of detected communication events to communication error classes	Map each observable event to Timeliness, Authenticity, Data Integrity or Masquerade categories with T-A-DI-M
3. Network-infrastructure optimization through traffic engineering, scheduling and tuning	Use bandwidth analysis, Quality of Service, connection priorities, topology assessment, and worst-case jitter testing to balance safety and availability
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.

© 2026 ODVA, Inc.
All rights reserved.

Sequence Diagram for Network Reaction Times



Attribute	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

© 2026 ODVA, Inc.

All rights reserved.

Example of initial configuration (Before)

110 ms	47 ms	112.16 ms	-2.16 ms
Process safety time (PST)	Non-network total	System reaction time	Margin vs PST

Communication configuration timings

Input connection

EPI = 10 ms · Timeout Multiplier = 2 · ASYNC = 1

If the producing application is asynchronous to the data production, ASYNC = 1 (via EDS).

Network Time Expectation Multiplier (NTEM)

```
NTEM = (EPI x (Timeout Multiplier + 2)) / 128 µs
NTEM = (10 ms x 4) / 128 µs = 312.50
```

Round up to the next integer: NTEM = 313

Network Time Expectation (NTE)

```
NTE = 313 x 128 µs = 40.06 ms
```

The application is asynchronous. Therefore:

Input network reaction time = NTE = 40.06 ms

Output connection

EPI = 5 ms · Timeout Multiplier = 2 · ASYNC = 1

Network Time Expectation Multiplier (NTEM)

```
NTEM = (EPI x (Timeout Multiplier + 2)) / 128 µs
NTEM = (5 ms x 4) / 128 µs = 156.25
```

Round up to the next integer: NTEM = 157

Network Time Expectation (NTE)

```
NTE = 157 x 128 µs = 20.10 ms
```

The application is asynchronous. Therefore:

Output network reaction time = 20.10 ms + 5 ms (Output EPI) = 25.10 ms

Initial total reaction time

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

T = 47 ms + 40.06 ms + 25.10 ms = 112.16 ms

Reaction time budget

112.2 ms of 110 ms scale



© 2026 ODVA, Inc.

All rights reserved.

Example of initial configuration (After)

Example 2 — Revised configuration (M1)

110 ms	47 ms	99.00 ms	+11.00 ms
Process safety time (PST)	Non-network total	System reaction time	Margin vs PST

Communication configuration timings

Input connection

EPI = 8 ms · Timeout Multiplier = 2 · ASYNC = 1
If the producing application is asynchronous to the data production, ASYNC = 1 (via EDS).

Network Time Expectation Multiplier (NTEM)

```
NTEM = (EPI × (Timeout Multiplier + 2)) / 128 µs
NTEM = (8 ms × 4) / 128 µs = 250.00
```

Round up to the next integer: NTEM = 250

Network Time Expectation (NTE)

```
NTE = 250 × 128 µs = 32.00 ms
```

The application is asynchronous. Therefore:
Input network reaction time = NTE = 32.00 ms

Output connection

EPI = 4 ms · Timeout Multiplier = 2 · ASYNC = 1

Network Time Expectation Multiplier (NTEM)

```
NTEM = (EPI × (Timeout Multiplier + 2)) / 128 µs
NTEM = (4 ms × 4) / 128 µs = 125.00
```

Round up to the next integer: NTEM = 125

Network Time Expectation (NTE)

```
NTE = 125 × 128 µs = 16.00 ms
```

The application is asynchronous. Therefore:
Output network reaction time = 16.00 ms + 4 ms (Output EPI) = 20.00 ms

Revised total reaction time

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

T = 47 ms + 32.00 ms + 20.00 ms = 99.00 ms

Reaction time budget — 99.0 ms of 110 ms PST



© 2026 ODVA, Inc.

All rights reserved.

Mechanism 2: Diagnosis of communication error classes

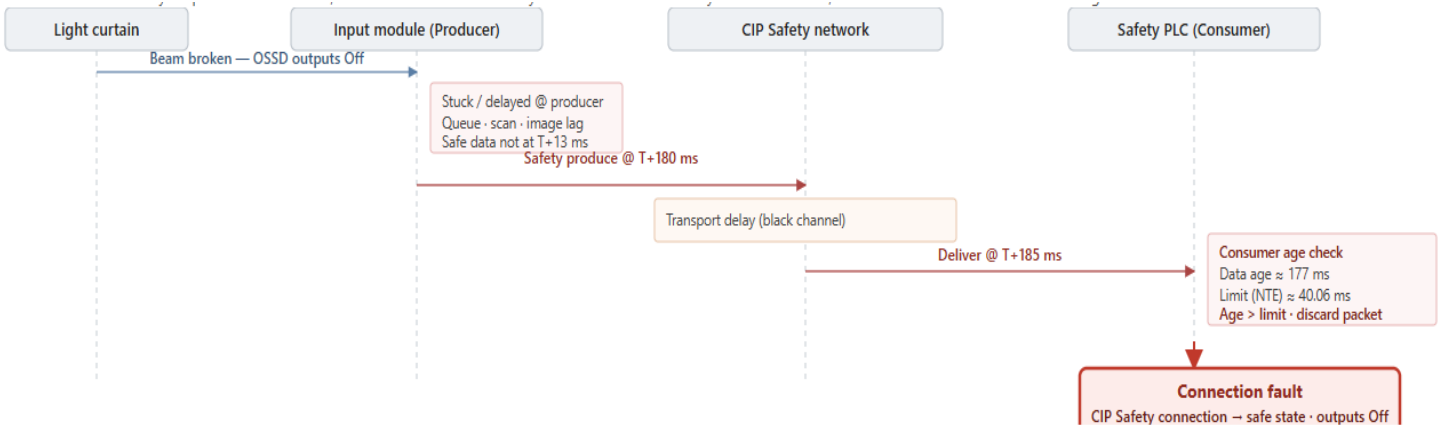
- Example Simple Rules that can be applied for diagnosis

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

- Standardization of the sub-rules for each of T-A-D-I is needed to avoid mis-diagnosis

Stale Time Stamps, and clock drifts/ lags diagnosis

- **When the network looks fine, but the data is already old**
- *Issue: Stale process image vs healthy communication*
- Sensor → Safety Producer → Black Channel → Safety Consumer
  CRC, sequence, and ACK can all pass while safety-relevant data is outdated.



© 2026 ODVA, Inc.

All rights reserved.

Diagnosis breakdown

- There are two timestamps available both with different use case

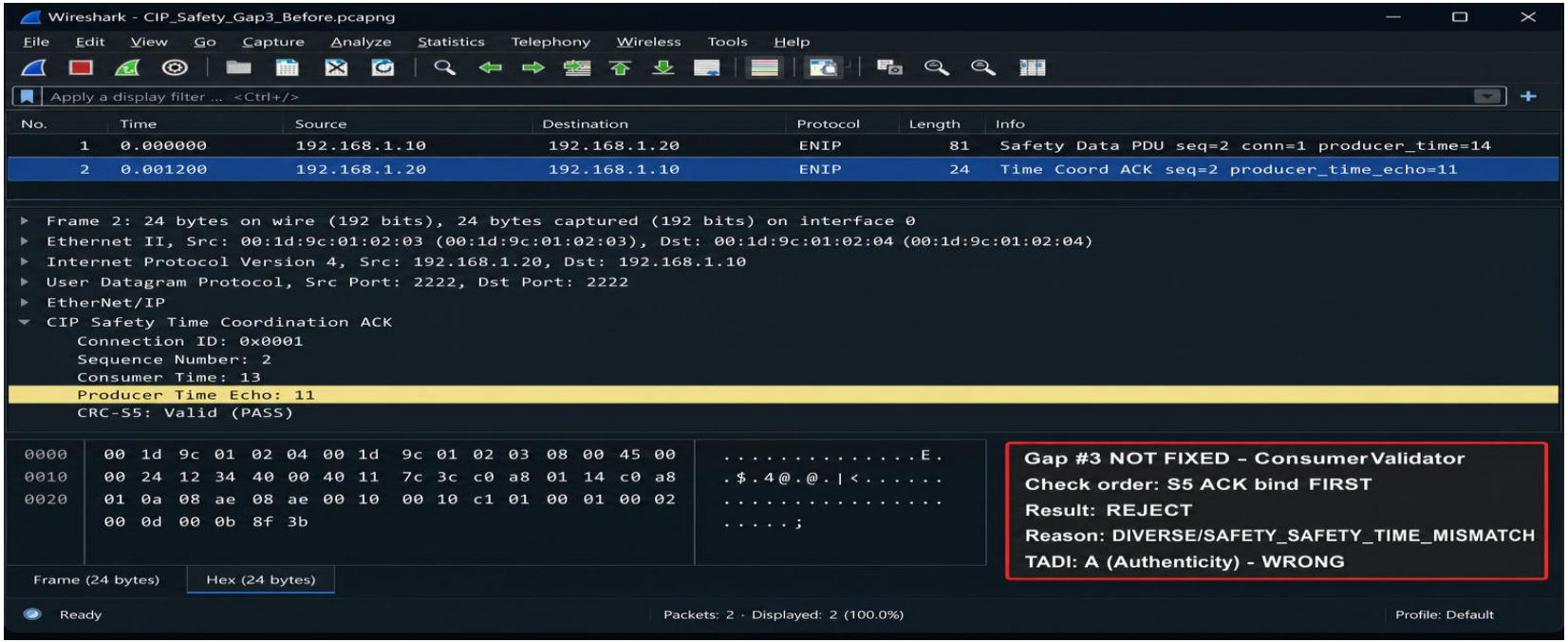
Field	Where	Compared to	Question	If it fails
`producer_time`	DATA PDU	`consumer_time`	Is this production **still fresh**?	**T** — Timeliness → S1 timestamp
`producer_time_echo`	ACK PDU	`producer_time`	Does this ACK **match this DATA**?	**A** — Authenticity → S5 diverse

Producer_time: Producer's clock when this production was built/stamped
Producer_time_echo: Consumer copying producer time from the receiving data PDU
Consumer_time: Consumer's local clock when ACK was sent

- In industrial norm S5 ACK/diverse is checked first before S1 (time stamp)

© 2026 ODVA, Inc.
All rights reserved.

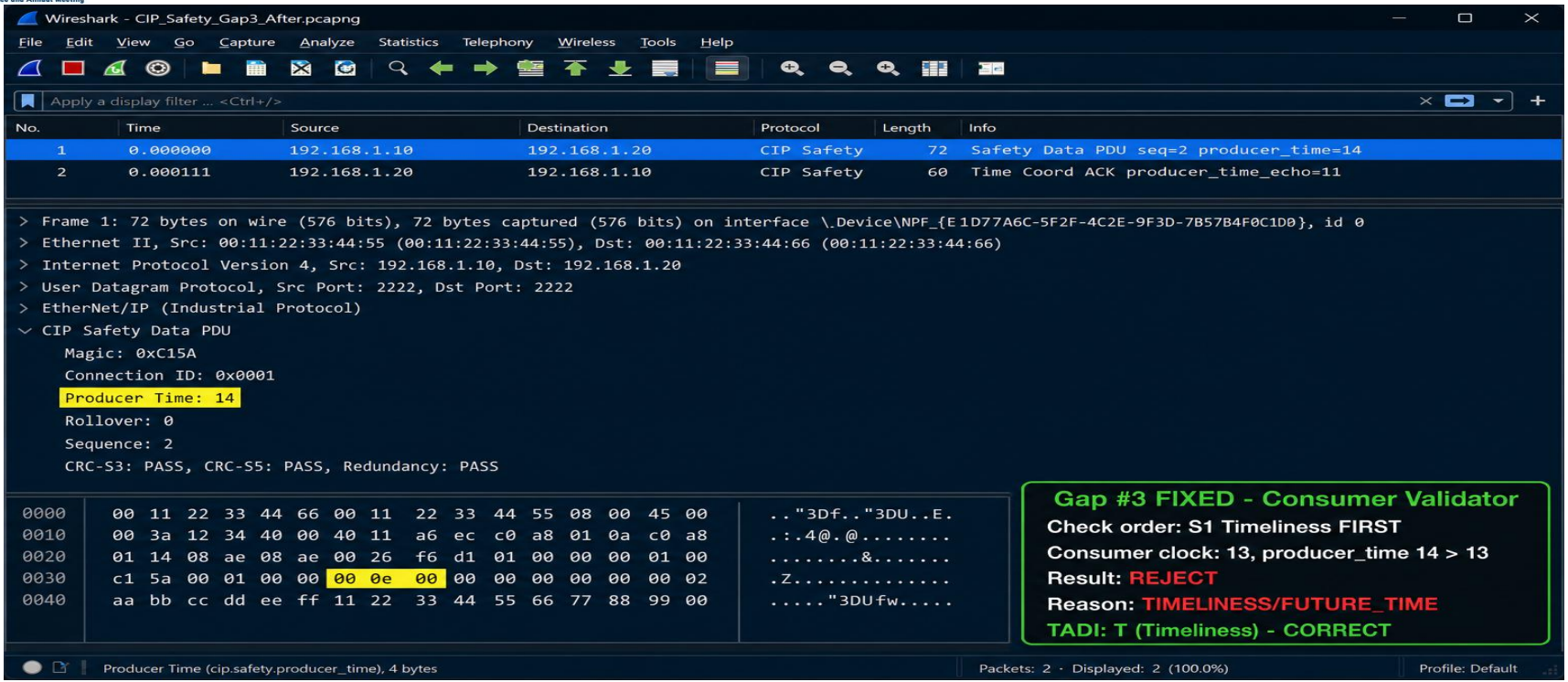
Gap 3: Wireshark Span shots (Simulated display- Old)



© 2026 ODVA, Inc.

All rights reserved.

Gap 3: Wireshark Span shots (Simulated display- new)



© 2026 ODVA, Inc.

All rights reserved.

Mechanism 3: Network Infrastructure Optimization

Network Time — NTE and System Reaction Time

- Worst case successful message time ≤ NTE calculation &
- Worst case total system reaction time ≤ expected system reaction time.

Quality of Service — QoS

- Configure Quality of Service consistently in devices and switches.

Safety Priority — For I/o and Diagnostics

- Assign safety I/O traffic an appropriate EtherNet/IP priority.
- Reserve sufficient bandwidth for safety, standard and diagnostic traffic.

Mechanism 4: Bottom-up Requirements & Assumptions on Design

BUR ID	BUR Description
BUR-1	The light-curtain state shall be validated before it is supplied to the CIP Safety producer.
BUR-2	The output module shall locally remove drive torque if valid output data is not received within its configured NTE.
BUR-3	The safety PLC shall place the affected safety function in its safe state when the i/p, o/p connection is in fault
AOD	**AOD Description**
AOD-1	Device reaction times are taken from certified Safety Manuals and/or EDS.
AOD-2	The input and output applications are treated as asynchronous unless synchronization is demonstrated.
AOD-3	The residual error target remains satisfied at all safety devices

Communication and Product FMEA

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
PF-01	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.	NA	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)

Key Takeaways

- The Communication FMEA and Product FMEA together form an enhanced FMEA where failure modes are mapped to T–A–DI–M, M1–M4, BUR/AoD references and diagnostic identifiers.
- **Standards working groups**: paper 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 Common mode Common Failure Analysis 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 mechanism list but match no current row in FMEA enter a feedback loop to update the FMEA, mechanism list, BUR/AoD catalogue, or diagnostic table.

Selected 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

Thank You

- Questions and Discussion
- Riya Rahul Shah | Shyam Sundar Pal | Utthunga Technologies, India
- Contact us after the session for technical follow-up

- *ODVA 2026 Industry Conference | www.odva.org*