


# A Framework for Functional Safety in Process Applications using EtherNet/IP

**Marc Baret, Vivek Hajarnavis, Ethan Puerto, Joseph Dufresne**
Endress+Hauser, Rockwell Automation, Emerson/Micromotion, Samson

**October 21, 2026**

# Abstract

Since NAMUR identified EtherNet/IP as a viable Industrial Ethernet application protocol for process control, ODVA has developed specification enhancements to align with the needs of these applications, covering Device Management, Profiles, aspects related to the Physical Layer, Security and Functional Safety.

- **Device Management**
- **Profiles**
- **Physical Layer**
- **Security**
- **Functional Safety**

**This presentation aims to address this last item: Functional Safety.**
Typical functional-safety scenarios in process applications will be described and mapped to how they can be achieved using EtherNet/IP.


© 2026 ODVA, Inc.
All rights reserved.

# NAMUR Requirements

NAMUR specified a multi-standard approach for Ethernet in process applications, currently identifying PROFINET and EtherNet/IP, together with the technical requirements needed for successful deployment:

| NAMUR requirement | Status in ODVA and the EtherNet/IP Specification |
|---|---|
| Advanced Physical Layer (APL), for hazardous environments | Specifications published; Conformance Test procedures well established and mature |
| Profiles, for consistent data structures and device exchange | Profiles published for Mass Flow, Magnetic Flow, Pressure, Temperature and Level |
| FDI packages for configuration & device management | FDI packages for EtherNet/IP instrumentation widely available |
| Cybersecurity characteristics for devices | CIP Security applies to both discrete and process; the need is implementation by device vendors |
| **Functional Safety** | **Additional guidance needed for applying functional safety to EtherNet/IP in process applications.** |

**This presentation identifies where work is needed to realize functional safety with ODVA Technologies.**


© 2026 ODVA, Inc.
All rights reserved.

# Industries

If ODVA Technology is to be used in applications beyond where it has seen use to date, it needs to evolve to meet these additional needs.

TODAY

## Food & life-science

**Strong regulatory requirements**

- Materials
- Contamination
- Traceability

Functional-safety applications are often addressed using established factory automation techniques, although some have process-control requirements that require process control functional safety.



NEXT

## Oil, gas & chemical

**Additional safety needs**

- Intrinsic Safety
- Detecting conditions that could impact the performance of critical components
- Other aspects that could affect the safety of the operation


© 2026 ODVA, Inc.
All rights reserved.

# The Application Context

For this discussion, process instruments are grouped by how they receive power.

## Four wire

**Power and communications are on two separate pairs of wires**

**Examples: Flow, analytics**

Few functional safety implications

## Two wire

**Power and communications are on same single pair of wires**

**Examples: Level, pressure, temperature**

Functional safety will be a focal item


© 2026 ODVA, Inc.
All rights reserved.

# Why Two Wire Devices Are the Focus

Three design considerations motivate this presentation's focus on two-wire devices.

| Power | Hazardous environments | Market Requirements |
|---|---|---|
| **Limited** | **Ex** | **Device Suitability** |
| Ethernet-APL increases available power, but two-wire devices remain power constrained. | Where energy limitation is required, it further constrains the design. | Required functionality, diagnostics, and certifications must be accommodated within cost and space constraints. |

**Power, space, and cost constraints can make multi-processor functional-safety architectures difficult to implement.**


© 2026 ODVA, Inc.
All rights reserved.

# Standards

**There are several international standards which provide the guiding principles for achieving functional safety in process applications.**

| Standard | Definition | Scope |
|---|---|---|
| **IEC 61508** | The generic parent standard for functional safety of electrical / electronic / programmable electronic safety-related systems | The base framework from which sector standards are derived |
| **IEC 62061** | Machinery-sector functional safety standard based on the IEC 61508 framework | Safety-related control systems for machines, not process-industry SIS |
| **IEC 61511** | Process-industry sector standard based on IEC 61508 | The main standard for Safety Instrumented Systems (SIS) in process plants |


© 2026 ODVA, Inc.
All rights reserved.

# SIL Levels in Process Automation Applications

**Safety Integrity Level (SIL) is a discrete level specifying the safety integrity requirements of a safety function.**

**In process applications, the required risk reduction is determined for a Safety Instrumented Function (SIF) and expressed as a target SIL. The SIF is then designed and verified to demonstrate that it meets the required SIL.**

| SIL | Low-demand PFDavg | Typical Risk Reduction |
|---|---|---|
| **SIL 1** | $10^{-2}$ to $<10^{-1}$ | 10–100× |
| **SIL 2** | $10^{-3}$ to $<10^{-2}$ | 100–1,000× |
| **SIL 3** | $10^{-4}$ to $<10^{-3}$ | 1,000–10,000× |
| **SIL 4** | $10^{-5}$ to $<10^{-4}$ | 10,000–100,000× |

Hazard & Risk Assessment → Required Risk Reduction → Target SIL → SIF Design → SIL Verification


© 2026 ODVA, Inc.
All rights reserved.

# SIL Levels: Potential Impact and Examples

| Level | Potential impact | Example |
|---|---|---|
| **SIL 1** | Loss or damage of a single piece of equipment, a localized process upset, a minor environmental release, or a single injury | High-level shutdown on an atmospheric storage tank |
| **SIL 2** | Multiple injuries, fatality, fires, or toxic releases extending beyond the immediate area | Low-flow trip protecting a fired heater |
| **SIL 3** | Multiple fatalities, a major toxic or flammable release, and significant off-site impact | Overpressure protection on a high-pressure separator |
| **SIL 4** | Widespread multiple fatalities and catastrophic off-site impact | Out of scope: rarely applied in the process industry |

Examples are illustrative only. Target SIL is determined by the required risk reduction identified through the applicable hazard and risk assessment.


© 2026 ODVA, Inc.
All rights reserved.

# SIL 1 and SIL 2: Steps to Compliance

| | Risk assessment | Definition | Verification | Life cycle |
|---|---|---|---|---|
| **SIL 1**<br>Focus: Safety Instrumented Function (SIF) | Confirm that SIL 1 is sufficient | Define the required safety function<br><br>Determine required risk reduction<br><br>Design the SIF to meet the required SIL | Verify PFDavg / PFH and applicable architectural constraints are met | Apply functional-safety lifecycle requirements |
| **SIL 2**<br>Focus: SIF with higher required safety integrity | Confirm that SIL 2 is sufficient | | | |

**The steps to compliance do not fundamentally change from SIL 1 to SIL 2; the required integrity and associated constraints increase.**

Individual devices do not establish the SIL of the SIF. Devices must be suitable for their intended safety application, and their contribution is considered when verifying the complete SIF.


© 2026 ODVA, Inc.
All rights reserved.

# SIL 2: IEC61508 Integrity Considerations

**Achieving SIL 2 requires consideration of random hardware integrity, architectural constraints, and systematic integrity.**

**Two routes for achieving this**

## Route 1H – SFF / HFT Approach

- Based on Safe Failure Fraction (SFF) and Hardware Fault Tolerance (HFT)
- SIL depends on device type, SFF, and HFT
- 1oo1 (HFT = 0) architecture may be permitted when the applicable requirements are satisfied

## Route 2H – Reliability Data Approach

- Based on **reliability data supported by sufficient field experience**
- Requires adequate confidence in the failure-rate data
- Provides an alternative to the Route 1H SFF-based architectural constraints

**IEC 61508 does not inherently require redundant processors or devices for SIL 2; a 1oo1 architecture may be suitable when the applicable hardware and systematic integrity requirements are satisfied.**


© 2026 ODVA, Inc.
All rights reserved.

# SIL 2: How Faults Reach the SIS Logic Solver

**HART-BASED SYSTEMS**

## 4–20 mA current signal

Device detects internal fault

4-20 mA provides safety-related process signal / fault response

HART provides additional diagnostics and status

SIS Logic Solver receives the information



**NETWORKED SYSTEMS**

## Safety protocol

Device detects internal fault

Safety-related process data and device status are communicated digitally

Functional-safety protocol protects the communication of safety-related information

SIS Logic Solver receives the information

The device is responsible for detecting its internal faults; **the safety communication protocol provides integrity for communicating safety-related information between safety endpoints.**


© 2026 ODVA, Inc.
All rights reserved.

# SIL 2 over EtherNet/IP with CIP Safety

CIP Safety adds functional-safety communication mechanisms to EtherNet/IP for the high-integrity transfer of safety-related information.

| | | | |
|---|---|---|---|
| **Repetition** | **Loss / deletion** | **Insertion** | **Incorrect sequence** |
| **Data corruption** | **Delay** | **Masquerading** | **Addressing errors** |

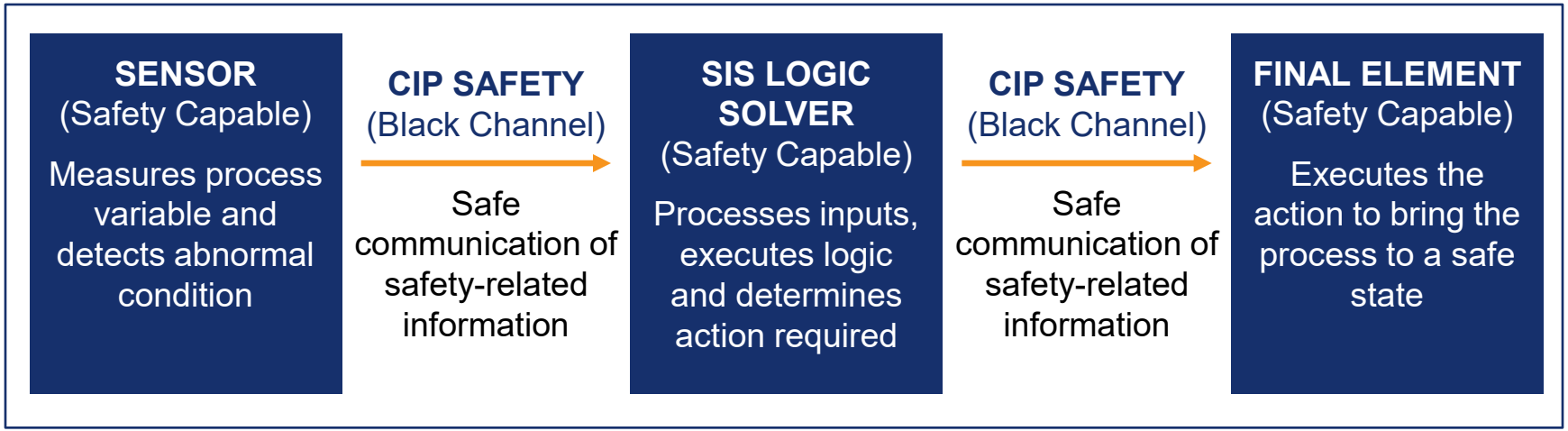
**CIP Safety mechanisms:**

| | |
|---|---|
| **Connection identification/authentication** | **Redundancy and cross-checking** |
| **Safety CRC** | **Time expectation** |

**CIP Safety provides the safety communication layer; it does not determine the SIL of the complete SIF.** A SIL 2 SIF may use 1oo1 architectures where the applicable hardware, systematic, architectural, and SIF-level requirements are satisfied.


© 2026 ODVA, Inc.
All rights reserved.

# Safety Instrumented Function (SIF)




**CIP Safety provides the functional-safety communication layer**
**IEC 61508 and IEC 61511 govern the complete Safety Instrumented Function.**

CIP Safety provides certified, standard-based protection for the transmission of safety-related information without changing the fundamental responsibilities of the equipment in the Safety Instrumented Function.


© 2026 ODVA, Inc.
All rights reserved.

# SIL 3: Open Questions and Next Steps

## Current Approach

**SIL 3 devices commonly combine two SIL 2 channels running the functional safety stack on one processor.**

## Questions for the CIP Safety SIG

| | |
|---|---|
| 1 | Can EtherNet/IP with CIP Safety replace the traditional 4–20 mA safety-related communication path while maintaining the required functional-safety integrity? |
| 2 | Can EtherNet/IP with CIP Safety support a SIL 3 SIF built from two SIL 2 channels on one processor? |

## Aim

**Enable the dual-SIL 2, single-processor architecture on EtherNet/IP.**

### Potential Next steps

1. Draft a CIP Safety SIG proposal
2. Reuse the exida / TÜV validation


© 2026 ODVA, Inc.
All rights reserved.


2026
ODVA
Industry Conference and Annual Meeting