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

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

Abstract

Since the decision by NAMUR to specify two network protocols for Ethernet-based applications in the process industries, 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. This paper aims to address this last item: Functional Safety. Typical scenarios for achieving functional safety will be described and mapped to how they can be achieved using EtherNet/IP.

NAMUR Requirements

NAMUR – the international user association for the process industries specified a dual standard approach for the use of ethernet in process applications: Profinet and EtherNet/IP[1] . Beyond this, they have specified that there are a number of technical definitions that are needed in order to ensure the successful deployment of the networking technology:

- Support for the Advanced Physical Layer, to allow deployment in hazardous environments
- Profiles, to facilitate consistency in data structures and to enable device exchange
- FDI packages for configuration & device management purposes
- A feature set that provides Cybersecurity characteristics to devices
- Functional Safety

Many of these areas have been addressed by ODVA and the EtherNet/IP Specification. The Advanced Physical Layer specifications were published in 2021 and the Conformance Test procedures are well established and mature. ODVA has now published profiles covering Mass Flow, Magnetic Flow, Pressure, Temperature and Level applications [2]. FDI packages for configuring EtherNet/IP instrumentation are widely available. The CIP Security Specification is seen as being generic enough to apply for both discrete and process applications. The primary need here is seen as implementation by device vendors.

Functional Safety in Process Applications

The one area where there is a lack of clarity relates to how functional safety is achieved in process applications. This paper will therefore aim to relate the application context to both the international standards and the CIP Specification, and identify areas where work is needed to ensure that functional safety applications can be realized using ODVA Technologies.

 ©2026 ODVA, Inc.

Industries

To date, the primary applications that have been served by EtherNet/IP are food & beverage, and life-science. Whilst these industries have strong regulatory requirements in terms of materials, contamination and traceability, these industries do not generally have specific functional safety needs beyond what is already addressed today using factory automation techniques. Whilst also having a goal of avoiding risk to people, oil, gas and chemical applications have additional needs based on the idea of preventing explosions, the detection of conditions that could impact the performance of critical components and other aspects that could affect the safety of the operation. 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.

The Application Context

Process instrumentation largely encompasses scenarios for measuring physical characteristics ranging from level, pressure, temperature, flow and analytics (such as an acidity level). The devices for achieving this can be categorized into devices that are powered independently (flow and analytics) and those which are powered by the current loop itself. Colloquially, these are referred to as “four wire” and “two wire” devices respectively – the reference to the additional pair of wires corresponding to separate power supply.

Two Wire Devices

There are two main engineering characteristics which have placed constraints on the capabilities of two wire devices. Firstly, the fact that the devices have historically been powered by the current loop itself, has limited the level of power available within the device to approximately 50mW. Secondly, the application need for many of these devices to be deployed in Hazardous environments (Ex) essentially limits the scope for developing technology for overcoming this limitation: the desire to limit the amount of energy supplied into hazardous environments makes this a hard constraint. Whilst the development of the Advanced Physical Layer has facilitated the use of powering devices using the network connection (as well as the ability to facilitate the benefits of a native network connection in a device, the power constraints remain.

Aside from the technical characteristics there are industrial factors impacting this class of device. Temperature, pressure, and level measurement devices serve a market that is highly price sensitive. This in turn means that the development and engineering cost for this class of devices must be aligned with the desire to keep the cost of the devices as low as possible.

In practical terms, these two constraints together limit the engineering flexibility that manufacturers can deploy on these devices. For example, there is limited scope to create a device based on more than a single, low power processor.

Four-Wire Devices

In contrast to two wire devices, four wire devices have the advantage of having additional power available. Furthermore, their typical usage outside of hazardous environments provides greater engineering flexibility. This class of device is typically seen as offering value-adding features, giving less price sensitivity compared to two wire devices. However, the nature of the measurements made by this class of device means that there are fewer implications from a functional safety perspective.

In summary, the focus of effort needs to be on the two-wire class of device.

 ©2026 ODVA, Inc.

Standards

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

- IEC 61508 is the generic parent standard for functional safety of electrical / electronic / programmable electronic safety-related systems. It is the base framework from which sector standards are derived
- IEC 62061 is the machinery-sector implementation of that framework. It covers safety-related control systems for machines, not process-industry Safety Instrumented Systems (SIS) as such.
- IEC 61511 is the process-industry-sector implementation of IEC 61508 and is the main standard for Safety Instrumented Systems (SIS) in process plants

SIL Levels in Process Automation Applications

SIL, or Safety Integrity Level, is the level of risk reduction provided by a safety function. It quantifies how reliably a Safety Instrumented Function (SIF) performs its job; it is not a measure of how "safe" a device is in isolation.

IEC61508 defines the four discrete SIL Levels in terms of the Probability of Failure on demand (PFDavg) and its corresponding Risk Reduction Factor (RRF). This is summarized in this table:

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×

In the process industry, SIL ensures that the potential for hazardous scenarios is reduced to a tolerable level of risk, defining how much a given safety function must lower the likelihood of a dangerous event. Each level represents roughly an order-of-magnitude greater risk reduction than the one below it, from a factor of ten at SIL 1 up to a hundred thousand at SIL 4.

Random Hardware Failures vs. Systematic Failures

IEC 61508 distinguishes between two fundamentally different categories of failures: **Random Hardware Failures** and **Systematic Failures**. Understanding this distinction is important because the two categories are addressed using different methods and both must be considered when determining whether equipment is suitable for use within a Safety Instrumented Function.

Random Hardware Failures occur unpredictably over the operating life of equipment as a result of physical or electronic component failures. Examples include capacitor failures, sensor drift, broken solder joints, relay contact failures, processor memory upsets, and power-supply component failures.

Random Hardware Failures are evaluated using reliability and diagnostic analysis techniques such as **Failure Modes, Effects and Diagnostic Analysis (FMEDA), Probability of Failure on Demand (PFDavg), Probability of dangerous Failure per Hour (PFH), Diagnostic Coverage (DC), Safe Failure Fraction (SFF), and proof testing**. These analyses and measures help determine whether the random hardware integrity of the equipment is sufficient for its intended use within a Safety Instrumented Function.

Systematic Failures, in contrast, result from errors introduced during specification, design, implementation, manufacturing, operation, or maintenance. Examples include software defects, incorrect

algorithms, compiler-related errors, requirements errors, design mistakes, incorrect calibration equations, and manufacturing-process deficiencies.

Because Systematic Failures arise from underlying design or process errors rather than random component failures, they cannot be adequately addressed through probability calculations alone. Instead, IEC 61508 addresses systematic failures through measures such as **disciplined development processes, verification, validation, configuration management, documentation, independent review, and testing**. The level of rigor applied to control and avoid systematic failures is reflected in the equipment's **Systematic Capability (SC)**.

Consequently, achieving a given SIL requires consideration of **both random hardware integrity and systematic integrity**. Random hardware integrity addresses the likelihood and consequences of physical hardware failures, while systematic integrity addresses the prevention and control of errors introduced through design and development processes. Neither consideration alone is sufficient to establish the integrity of the complete Safety Instrumented Function.

SIL Levels

SIL 1 — Moderate consequences. SIL 1 failures often have moderate consequences. These could include the loss or damage of a single piece of equipment, a localized process upset, a minor environmental release within the site, or the potential for a single injury. A high-level shutdown on an atmospheric storage tank might fall into this category, where operator monitoring and bunding also help guard against an overfill.

SIL 2 — Serious consequences. SIL 2 failures carry more serious consequences: the potential for multiple injuries, fatality, fires, or toxic releases extending beyond the immediate area. These are cases where fewer independent protection layers exist, so the SIF carries a larger share of the risk reduction burden. A low-flow trip protecting a fired heater is one such case, where a loss of flow through the tubes could otherwise lead to rupture and fire.

SIL 3 — Severe consequences. SIL 3 failures have severe consequences, with a high potential for multiple fatalities, a major toxic or flammable release, and significant off-site impact. These functions are typically the last independent safeguard standing between the process and a catastrophic event, with few protection layers behind them. Overpressure protection on a high-pressure separator, or the emergency isolation of a unit handling large inventories of toxic gas, would tend to sit here.

SIL 4 —SIL 4 failures would carry consequences of the highest order: widespread multiple fatalities, catastrophic off-site impact, and damage extending well beyond the boundaries of the site. Functions at this level fall outside the scope of this paper, as SIL 4 is rarely applied in the process industry, where the accepted response to such a hazard is to revisit the design and remove the risk at source rather than rely on an ever more reliable safety function. This is considered to be out of scope for this paper.

Device Capability, Safety Instrumented Function, and Safety Instrumented System

Device Capability

Device capability describes whether an individual device is suitable for use within a Safety Instrumented Function of a specified integrity level. This capability is based on characteristics such as systematic capability, random hardware integrity, failure-rate data, diagnostic coverage, architectural constraints, and proof-test requirements. A device may therefore be assessed or certified as suitable for use in a SIL 2 or SIL 3 Safety Instrumented Function, but this does not mean that the device itself establishes the SIL of the complete safety function. The device provides one part of the evidence needed to demonstrate the integrity of the SIF.

Safety Instrumented Function (SIF)

A Safety Instrumented Function (SIF) is a specific safety function designed to detect a hazardous condition and place or maintain the process in a safe state. A SIF typically includes the required sensor(s), logic solver, and final element(s), together with any safety-related communication needed between them. The SIL is assigned to the SIF, and the achieved SIL is determined by evaluating the complete function, including device capabilities, random hardware failures, systematic integrity, architecture, diagnostics, common-cause failures, and proof testing. Therefore, the use of a SIL-capable device does not by itself establish the SIL achieved by the SIF.

Safety Instrumented System (SIS)

A Safety Instrumented System (SIS) is the overall system used to implement one or more Safety Instrumented Functions. An SIS may therefore contain multiple SIFs, each addressing a different process hazard and potentially having a different SIL requirement. The SIS provides the overall safety-system infrastructure within which the individual SIFs operate, including the associated sensors, logic solvers, final elements, communications, engineering practices, and lifecycle management. The SIS itself should therefore not be confused with an individual SIF: the SIF performs a specific safety function and has an assigned SIL, while the SIS is the broader system that implements one or more SIFs.
In summary, device capability describes the suitability of an individual component for safety-related use; the SIF is the complete safety function for which a SIL target is specified and verified; and the SIS is the overall system that implements one or more SIFs. Maintaining these distinctions is particularly important when discussing SIL 2 and SIL 3 architectures, because increasing the integrity of a SIF may be achieved through the architecture of multiple devices rather than through increased redundancy within each individual device.

Solutions

SIL1

The general approach to meeting SIL1 is achieved primarily through the assessment of the complete safety loop and ensuring that it meets the target requirement. The process for achieving SIL1 typically consists of the following steps:

1. Risk assessment to confirm that SIL1 is sufficient
2. Definition of the safety function (for example, stopping a pump if a tank reaches a high level)
3. Verification of the Safety integrity – which implies an analysis of the failure rates of the components (PFD/PFH) to verify that the safety function meets SIL1
4. Appropriate life-cycle activities, including validation, verification, testing, change management and proof testing

The main conclusion here is that SIL 1 focuses on demonstrating that the complete Safety Instrumented Function meets the required integrity target. The devices used within the SIF must be suitable for the intended safety application. Device suitability should consider systematic integrity as well as random hardware integrity, including credible failure-rate data, identified failure modes, diagnostic behavior, proof-test coverage, application suitability, and applicable proven-in-use and prior-use evidence. These factors are evaluated as part of the complete SIF to verify that the SIL 1 target is achieved.

SIL 2

Examples of applications that may require SIL2 are safety logic in a controller, or the operation of a shutdown valve.

In the case of SIL2 applications, the focus is on the Safety Instrumented Function (SIF). The steps that need to be conducted are similar:

1. Risk assessment to confirm that SIL2 is sufficient
2. Definition of the safety function to meet the SIL2 PFD target

3. Confirmation that the solution meets the IEC61508 architectural constraints
4. Following best practice through the life cycle through development, verification, validation and change management processes

The main distinction of SIL2 compared to SIL1 relates to the architectural constraints defined in IEC61508. There are two routes for achieving this:

1. Prescriptive: through the use of Safe Failure Fractions (SFF) and Hardware Fault Tolerance (HFT) based on Device Type (route $1_{H.}$) This approach is seldom used in practice.
2. Proven in use: use of field operation history and reduced HFT (route 2_H)

A SIL 2 architecture may permit the use of single-channel (1oo1) devices, subject to the applicable architectural constraints and verification that the complete SIF satisfies the required random hardware and systematic integrity requirements.

- Internal diagnostic capabilities such as watchdogs, RAM/ROM tests, pulse tests and cross monitoring within the device
- Safety rating to IEC61508 with SC2 systemic capability

A key characteristic of SIL 2 systems is the manner in which errors are detected, handled, and reported. There is however a disconnect between these goals and the prevailing technologies in use: for example, in HART-based systems, process data is transmitted to the DCS via the 4–20 mA current signal, so fault conditions must be signaled within that same analog range but there is no inherent mechanism for error detection handling and reporting.

.

This is the case with all the networking protocols, but it is addressed using the Safety extensions. All of the ethernet-based safety communication protocols have the same based characteristics of providing protection against errors (repetition, loss/deletion, insertion, incorrect sequence, data corruption, delay, masquerading and revolving memory failure). In EtherNet/IP-based architectures, the equivalent function is provided by CIP Safety.

Therefore, a process application over EtherNet/IP that meets SIL2 can be achieved using:

- Commercial devices intended for use in SIL 2 Safety Instrumented Functions. These are typically certified or assessed as suitable for use in SIL 2 applications, with the appropriate Systematic Capability and hardware integrity characteristics. However, device capability alone does not establish the SIL of the complete SIF. The device's dangerous random failure contribution must also be included in the PFDavg or PFH calculation, together with the contributions of the other elements of the Safety Instrumented Function.A controller architecture that is based on 1oo1
- Communication using CIP Safety

There is no requirement for redundancy of devices nor controllers, provided that the equipment meets the appropriate certification requirements, and the PFH and PFD values are in line with what is needed to achieve the SIL2 requirements.

Current commercially available CIP Safety implementations have generally been developed using dual-processor architectures to satisfy their functional safety objectives. While this approach has proven successful in factory automation, it presents practical challenges for two-wire process instruments where power consumption, physical size, and cost are tightly constrained. Consequently, broader adoption of CIP Safety in process instrumentation would benefit from enabling technology and implementation guidance that support IEC 61508-compliant single-processor architectures while maintaining the communication integrity defined by the CIP Safety specification and the functional safety objectives established by IEC 61508 and IEC 61511.

SIL 3

Examples of applications that may require SIL3 are overpressure protection on a high-pressure separator, or the emergency isolation of a unit handling a large inventory of toxic gas.

For SIL3 applications, the focus shifts from the sufficiency of the Safety Instrumented Function to the tolerance of the architecture to a single fault. The steps remain the same in principle:

1. Risk assessment to confirm that SIL3 is required, and that the hazard cannot reasonably be removed at source
2. Definition of the safety function to meet the SIL3 PFD target
3. Confirmation that the solution meets the IEC61508 architectural constraints, which at SIL3 will generally require a hardware fault tolerance of one fault. This also implies following best practice through the life cycle, with the systematic capability of both hardware and software elements demonstrated at SC3

The distinguishing characteristic of many SIL 3 Safety Instrumented Functions is the need to tolerate a single dangerous fault while continuing to perform the required safety function. In practice, this is commonly achieved through redundant architectures, such as dual sensors, redundant logic solvers, or voting arrangements, together with appropriate diagnostics and systematic capability.
In practical terms this means:

- For SIL 3 Safety Instrumented Functions, the required hardware fault tolerance is frequently achieved through redundant system architectures. As a result, process applications commonly employ multiple SIL-capable field devices in voting arrangements rather than relying on a single device to provide the required level of fault tolerance. Field instrumentation: in process applications the required integrity is frequently obtained not from a single SIL3 instrument but from multiple SIL2-rated instruments arranged in a voting configuration such as 1oo2, 2oo2 or 2oo3. A representative example uses two SIL2-capable level transmitters in a 2oo2 arrangement, falling back to 1oo1 if one channel becomes unhealthy
- Certification: systematic capability of SC3, rather than the SC2 required at SIL2

Today, many process devices are developed and certified in accordance with IEC 61508 to be suitable for use in Safety Instrumented Functions up to SIL 3 (see the certificate from a Micro Motion Coriolis Mass Flowmeter) in the Appendix for an example. Many process field devices are certified as suitable for use in SIL 2 Safety Instrumented Functions when used as a single device. Higher-integrity Safety Instrumented Functions, including SIL 3 applications, are commonly a achieved by combining multiple SIL-capable devices within a redundant architecture that satisfies the IEC 61508 and IEC 61511 requirements for the complete Safety Instrumented Function. One way in which this is achieved is through voting mechanisms within the DCS.

Many process instrumentation manufacturers develop and certify their products to the highest practical systematic capability and hardware integrity level. This provides end users and system integrators with greater application flexibility, allowing the same certified device to be applied across a wide range of Safety Instrumented Functions. The achieved SIL is then determined by the design and verification of the complete Safety Instrumented Function rather than by the device certification alone.

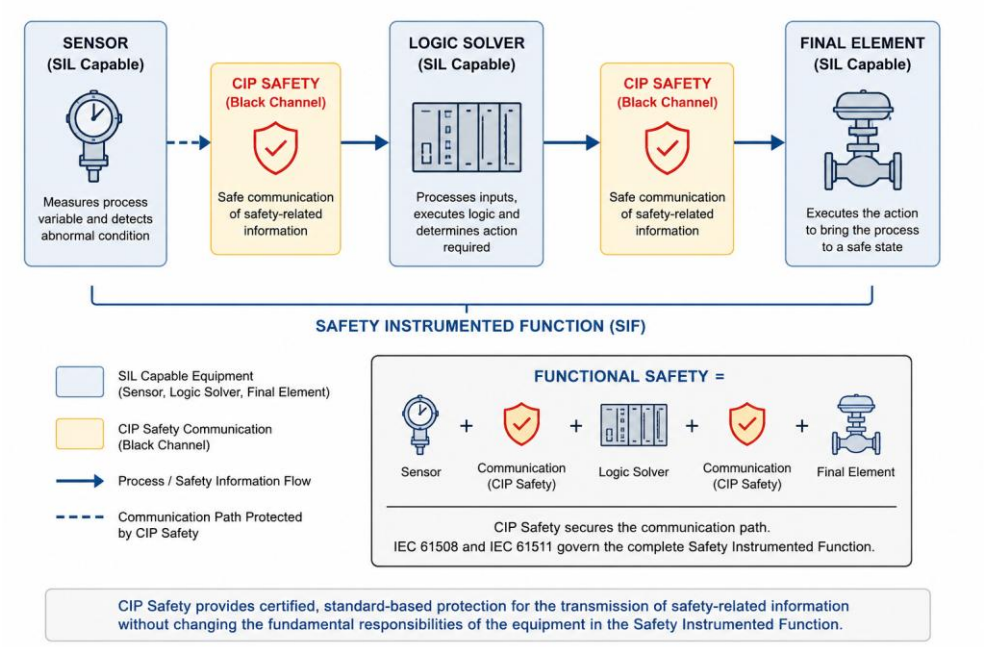
The practical implication is as follows: SIL 3 devices are rarely built for process applications; instead, the safety function is typically achieved through redundancy in the application: using multiple devices that are rated to a lower level..

The Role of CIP Safety and Ethernet Safety Protocols

Like all of the Safety protocols, CIP Safety does not replace the functional safety requirements of IEC 61508 or IEC 61511, nor does it determine the Safety Integrity Level of a Safety Instrumented Function. Instead, it provides a certified communication mechanism that preserves the integrity of safety-related

information transmitted between certified devices. By implementing the Black Channel principle, CIP Safety protects against communication failures such as corruption, repetition, omission, incorrect sequencing, delay, masquerade, and other transmission errors while remaining independent of the underlying Ethernet transport. This allows the communication path to contribute to the overall integrity of the Safety Instrumented Function without changing the fundamental responsibilities of the sensors, logic solver, or final elements.

From a graphical standpoint you can view it as:



CIP Safety secures the communication path. IEC 61508 and IEC 61511 govern the complete Safety Instrumented Function.

Within a Safety Instrumented Function, CIP Safety provides a safety communication layer that ensures the integrity of safety-related information exchanged between certified devices. Through mechanisms such as end-to-end safety checking, sequence monitoring, timeout supervision, and message authentication, CIP Safety detects communication faults including corruption, loss, repetition, insertion, delay, and incorrect routing of safety messages. This allows the communication network to become part of the certified Safety Instrumented Function while preserving the functional safety objectives established by IEC 61508 and IEC 61511.

Implementation in Practice

Multiple instrumentation providers have faced a challenge with the implementation of Safety functions in devices. The way CIP Safety is defined at present, the expectation is that it will be deployed on multi-processor hardware. Available safety enabling technology has therefore made this assumption, and there has been no path for achieving CIP Safety on single processor devices. This in contrast to other non-CIP ethernet technologies where there is a precedent for achieving a SIL2-certified Safety Instrumented Function (SIF) using a single processor.

Conclusions

This paper has identified that there are both technical and industrial constraints which have limited the adoption of the techniques used in factory automation for achieving functional safety in process applications.

Alignment is needed between the way in which functional safety is achieved in the process application scenarios described in this paper, and the way in which the CIP Safety protocol meets certification needs. Further work is needed to explore what changes could be made to the protocol, how it is used and how certification is met in order to achieve functional safety in both the technical and commercial environment in which process devices are deployed.

The ask of the ODVA Community is to explore whether there are parts of the definition in Volume 5 [3] of the CIP Specification that can be adapted to meet the needs of the process application space. An area to explore would be to establish the opportunities to deploy a CIP Safety stack on single processor device architectures, for alignment with SIL2 applications.

In addition, there is a need for technical documentation and marketing material to better describe how functional safety can be achieved in process applications using EtherNet/IP. This paper aims to serve as a starting point for the creation of that material.

References (optional – samples included that can be used or removed)

[1] NAMUR Recommendation NE 168, *Requirements for an Ethernet Communication System for the Field Level*, Edition 2024-05-27, NAMUR User Association of Automation Technology in Process Industries, 2024.
[2] ODVA, The CIP Networks Library, Volume 1: Common Industrial Protocol, Edition 3.40, April 2026, Ann Arbor: ODVA, Inc., 2001-2026.
[3] ODVA, The CIP Networks Library, Volume 5: CIP Safety, Ann Arbor: ODVA, Inc., 2005-2026.

****
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.

Appendix – Example Certificate

The manufacturer may use the mark:

Revision 1.3 April 24, 2024
Surveillance Audit Due
May 1, 2027

ANSI National Accreditation Board
ACCREDITED
ISO/IEC 17065
PRODUCT CERTIFICATION BODY
#1004

Certificate / Certificat
Zertifikat / 合格証

MMI 2212121 C001

exida hereby confirms that the:

Model 4700 Field-Mount Transmitter

Micro Motion Inc.
Boulder, CO - USA

Has been assessed per the relevant requirements of:

IEC 61508 : 2010 Parts 1-3

and meets requirements providing a level of integrity to:

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type B Element

SIL 2 @ HFT=0; SIL 3 @ HFT = 1; Route 2_H

PFH/PFD_{avg} and Architecture Constraints must be verified for each application

Safety Function:

The primary safety function 4700 Coriolis Flowmeter shall provide continuous representation of the mass flow rate or density or volume flow rate to its safety certified output.

Application Restrictions:

The unit must be properly designed into a Safety Instrumented Function per the Safety Manual requirements.

Evaluating Assessor

Certifying Assessor

Page 1 of 2

 ©2026 ODVA, Inc.

Certificate / Certificat / Zertifikat / 合格証

MMI 2212121 C001

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type B Element

SIL 2 @ HFT=0; SIL 3 @ HFT = 1; Route 2_H

PFH/PFD_{avg} and Architecture Constraints must be verified for each application

Model 4700 Field-Mount Transmitter

Systematic Capability:

The product has met manufacturer design process requirements of Safety Integrity Level (SIL) 3. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer.

A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than stated.

Random Capability:

The SIL limit imposed by the Architectural Constraints must be met for each element. This element meets *exida* criteria for Route 2_H.

Application / Device Configuration	SD	SU	DD	DU
Model 4700 Field-Mount Transmitter 9 Wire Power Board - Internal Core	12	54	3310	183
Model 4700 Field-Mount Transmitter 4 Wire Power Board - 700 Core	613	168	3901	181
Model 4700 Field-Mount Transmitter 4 Wire Power Board - 800 Core	900	229	4218	241

IEC 61508 Failure Rates in FIT*

* FIT = 1 failure / 10^9 hours

SIL Verification:

The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFH/PFD_{avg} considering redundant architectures, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each element must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

The following documents are a mandatory part of certification:

Assessment Report: MMI 22-12-121 R003 V1R2 (or later)

Safety Manual: 4700SIS_8_11 Safety Manual.pdf Rev AA Aug'23

80 N Main St
Sellersville, PA 18960

T-002, V7R2

 ©2026 ODVA, Inc.