# Managing SIS Process Measurement Risk and Cost

Advances in measurement technologies help safety system designers reduce risk and cost in their SIS designs and lifecycle management.

By Howard Siew and Nathan Hedrick, Endress+Hauser

Successful implementation and management of a safety instrumented system (SIS) requires designers and operators to address a range of risks. The safety lifecycle, according to IEC 61511 or ISA 84, provides detailed requirements and a framework for the safety management system. There are three things to consider.

First, is the specification of a proven measurement instrument such as a flowmeter (Figure 1). You need to follow specifications of sizing, material selection, installation, commissioning, validation, operation, maintenance and modifications for a given application. These are fundamental to achieving initial targeted risk reduction.

Second, is to define the support required to keep the flowmeter or other measurement subsystem available at that targeted level of risk reduction throughout the life of the SIS, this must be defined in the design and implementation phase.

**Figure 1:** Flowmeters like those shown here can play key roles in reducing risk with safety instrumented systems (SIS).

Third, is with the implementation of IEC 61511 edition 2 that introduced some changes in these guidelines and strengthened emphasis on the requirements for end users to collect reliable data from the process. This enables end users to document and make assessments of the device to ensure it is suitable for use in a SIS and meets the required functional and safety integrity requirements, based on previous operating experience in similar operating environments.

This article describes some tools, capabilities and procedures that can be considered for designing and managing a SIS installation in flow measurement applications.

## Risk Analysis and Safety Integrity Level (SIL) Identification

Under IEC 61511- ISA 84 safety lifecycle, risk analysis is carried out for the specific risk and hazard utilizing the following criteria: extent of damage, exposure time, hazard avoidance and occurrence probability. Following these criteria will lead to the conclusion of the SIL rating of the application specific safety instrumented function (SIF) (Figure 2).

With that, operators and SIS designers are required to qualify the appropriateness of an SIS measurement subsystem to do its part. This not only includes the initial design of the SIS itself, but the qualification of the measurement subsystem used in that service.

## Risk of failure sources

**Random failures** – risk of failure to perform an expected function can come from unavoidable failure sources; for example, the collective unavoidable failures of electronic components in a transmitter due to degradation overtime. Required maintenance and proof test procedures must be

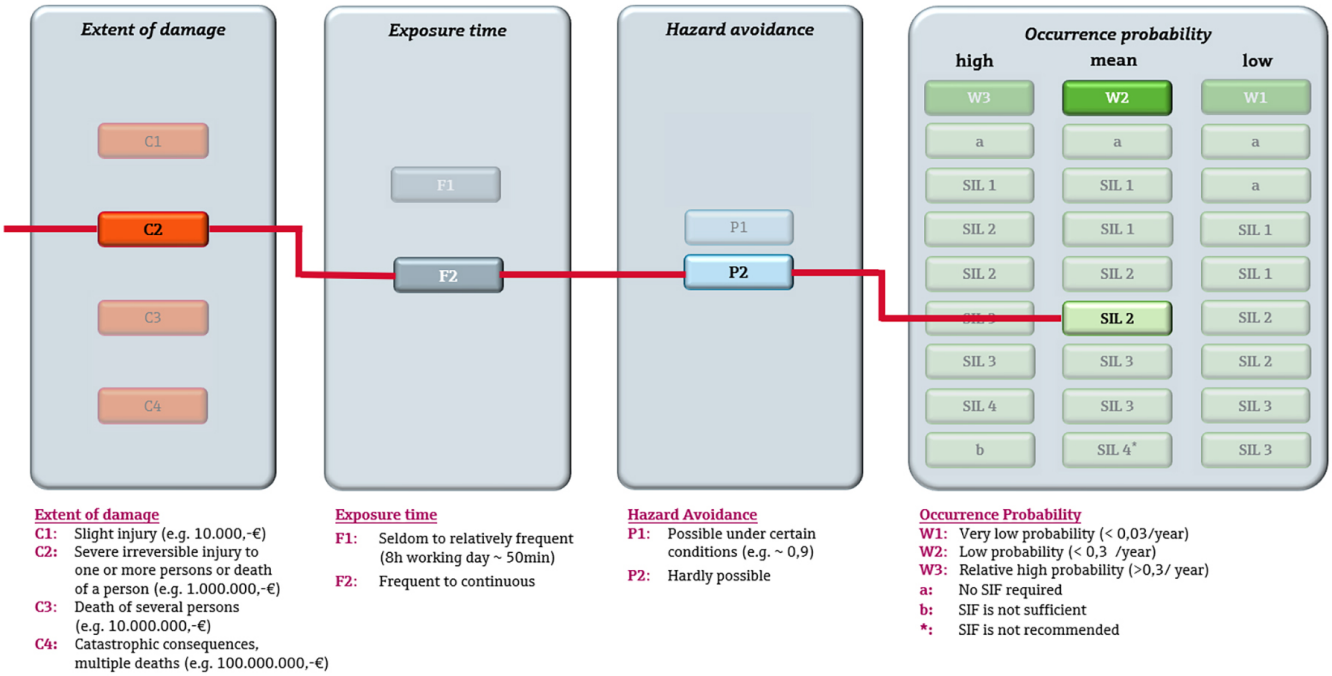



**Figure 2:** Example of a risk graph in accordance with IEC-61511-3 Annex E.

determined and executed to keep the probability of failure on demand (PFD) average and lambda dangerous undetected (λdu) fault risk, that is outside the reach of diagnostics, below a required average risk reduction target.

**Systematic failures** — risk of failure to perform an expected function can also come from systematic failure sources which can be prevented; for example, unsuitable material is selected during the design, incorrect installation or damage to a sensor while being tested. Systematic fault risk may be created by process medium properties, operating conditions, build-up or corrosion (Figure 3). Periodic visual field inspections, calibrations and maintenance that may need to be conducted can introduce failure risk. To reduce risk, personnel will need to follow written procedures to conduct activities and work with instruments that may need removed, transported, repaired, tested and reinstalled.

**Figure 3:** Buildup on free space radar antenna, which does influence the safety function.

It has been stated by a leading chemical company that "2% of every time we have human intervention, we create a problem." Another leading specialty chemical company conducted a study that concluded "4% of all devices (instruments) which are proof tested get damaged during re-installation." Reducing the need for personnel to physically touch a measurement subsystem enables the designer to reduce some systematic failure risk to a SIS.

The methods and procedures required for testing SIS diagnostics is a necessary step in the safety requirement specification (SRS) per IEC 61511 edition 2. SRS clause 10 indicates some of the requirements for proof-test procedures which includes scope, duration, state of the tested device, procedures used to test the diagnostics, state of the process, detection of common cause failures, methods and prevention of errors.

Measurement subsystems from several instrument suppliers are now available with integral redundant self-testing diagnostics that can conduct continuous availability monitoring. This means a measurement subsystem with high diagnostic coverage could also have redundancy—meaning the testing functions are redundant and continuously checking each other. This provides several benefits for the lifecycle management of instruments used in a SIS.

## Extending Proof Test Intervals

Periodic proof testing of the SIS and its measurement subsystems is required to confirm the continued operation of the required SIF, and to reduce the probability of dangerous


1. ***Option 1:*** *Functional test* of the *entire SIS*
2. ***Option 2:*** *Partial testing* of the SIS

**Figure 4:** Proof testing options

undetected failures that are not covered by diagnostics. Traditionally, a functional test of the entire SIS is being carried out (Figure 4: Option 1) and often requires removal of the sensor, final element, its wiring, transportation to a testing facility and reinstallation afterward. Modern instrumentation may provide the capability to conduct proof testing in-situ as partial testing (Figure 4: Option 2), thus eliminating the removal of equipment and risk of wire, instrument or equipment damage (Figure 4).

Safety Integrity Level (SIL) capable measurement subsystems typically have hardware and software assessments conducted during development to determine Failure Mode Effects and Diagnostic Analysis (FMEDA) and to manage change processes according to IEC 61508-2, 3. The λdu and proof test coverage (PTC) values, among other safety parameters, are provided in a safety function manual and described in a certificate. Lower λdu values give system designers greater freedom when setting measurement subsystem proof test intervals as these contribute a lower increase in Probability Failure on Demand (PFD) over time (Figure 5).

For example, some Coriolis flowmeters have λdu values in the 150 to 178 failure in time (FIT, where 1 FIT= 1 failure in a billion hours) range. Others, like two-wire Coriolis flowmeters, have λdu values in the 73 to 89 FIT range. Vortex flowmeters with λdu in the 70 to 87 range are also available. All other things being equal, a measurement subsystem with half the FIT could allow doubling the proof test interval time (Figure 6).

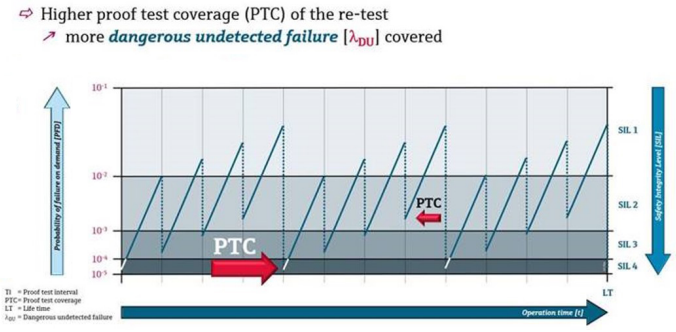
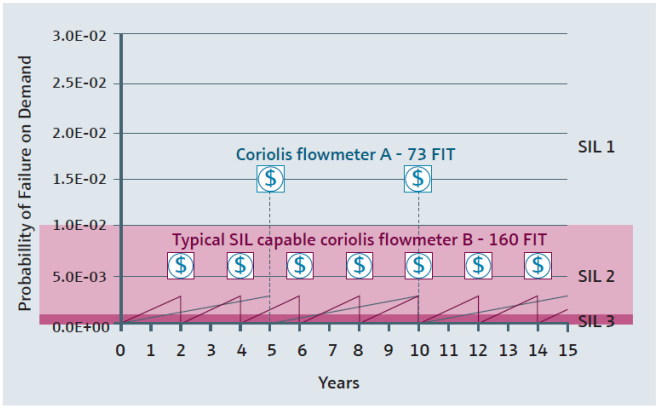



**Figure 5:** Higher proof test coverage (PTC) of the re-test reveal more dangerous undetected failures [λdu] are uncovered.



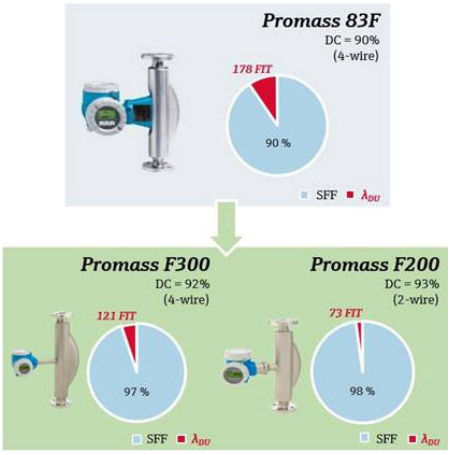




**Figure 6:** Flowmeters with a lower "dangerous undetected" (λdu FIT and in-situ testing capabilities may allow one to extend the interval time needed for proof tests requiring the flowmeter to be removed from the process. In this example, all other things being equal, flowmeters with a 160 λdu FIT have to be removed every two years for testing, while a flowmeter with a 73 λdu FIT has to be removed only every five years.

Some measurement subsystems offer the capability to remotely invoke in-situ proof testing with a high degree of Proof Test Coverage (PTC) to reduce the Probable Failure on Demand (PFD) subsystem contribution.

Given that external visual inspections are sufficient for at least some proof test events, these measurement instruments might be proof tested in-situ without the need to remove the instrument from service. Data from these proof tests can be transmitted via 4-20mA ART from the instrument to and through some safety control systems to a digital network such as EtherNet/IP® where this can be captured. In short, the proof testing event can be invoked, and related data can be captured, managed and reported through safety control systems supporting these capabilities.

In-situ proof testing can help create documented evidence that diagnostic checks have been carried out, and thereby fulfill the documentation of proof testing requirements in accordance with IEC 61511-1, Section 16.3.3b, "Documentation of proof testing and inspections." When in-situ proof testing can be

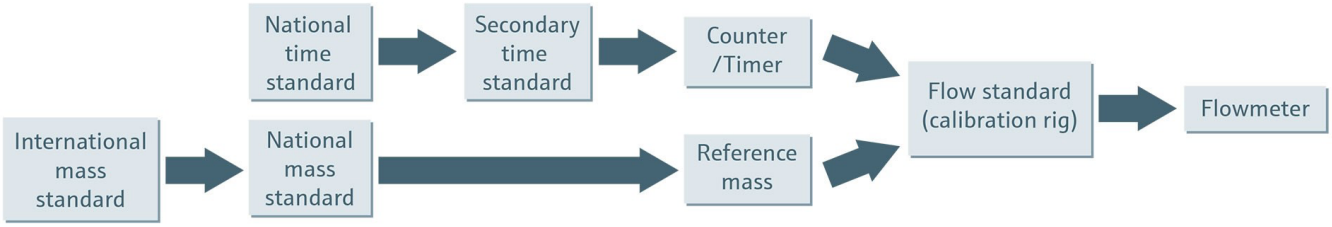



**Figure 7:** Example of a traceability chain for a mass flowmeter.

engineered into a SIS design, cost may be reduced during the maintenance cycle compared to the costs of always removing the instrument from service to perform testing.

## Traceable Calibration Verification

Measurement subsystem proof test procedures often require calibration verification of the measuring instrument. As users seek to set proof test intervals, they also need to set associated calibration verification intervals.

Verification and documentation to prove the SIS subsystem calibration is acceptable normally requires removal of the subsystem. This exposes the instrument to damage during removal, transport and reinstallation. There is also risk for unrealized damage or error introduction due to process shutdowns often required when an instrument is removed from service.

The measurement subsystem may need to be calibrated or verified with traceability to an international standard. If an organization is ISO 9001:2015 certified, it needs to address Clause 7.1.5.2a Control of Monitoring and Measuring Devices which states: "When measurement traceability is a requirement, or is considered by the organization to be an essential part of providing confidence in the validity of measurement results, measuring equipment shall be…calibrated or verified, or both, at specified intervals, or prior to use, against measurement standards traceable to international or national measurement standards; when no such standards exist…"

Some measurement instruments provide certified integral and redundant references which have been calibrated via accredited and traceable means and can thus have its measurement calibration verified in-situ. This removes sources of risk and cost associated with removing instruments from service, while still meeting ISO 9001:2015 Clause 7.1.5.2a requirements.

## Traceable and Redundant References

Appointed with the task to coordinate the realization, improvement and comparability of the world-wide measurement systems, the International Bureau of Weights and Measures defines traceability as "the property of a "measurement result to be related to a reference through a documented unbroken chain of calibrations, each contributing to the measurement uncertainty" (Figure 7).

The term "measurement result" can be used in two different ways to describe the metrological features of a measuring instrument:

1. **Measurand (Process Value):** Output signal representing the value of the primary process variable being measured (i.e., mass flow).
2. **Auxiliary Variable**: Signal(s) coming either from the instrument's sensor (transducer) or a certain element of the transmitter, such as A/D converter (ADC), amplifier, signal processing unit, etc. This variable is often used to transmit current, voltage, time, frequency, pulse and other information.

Figure 8 illustrates the basic concept and the relation between subsystem elements.

During the lifecycle of any instrument, it is important to monitor measurement performance on a regular basis (ISO 9001:2015 chapter 7.1.5.2a), especially if the measurements from the instrument can significantly impact process quality.

For example, in Figure 9 the process value is defined as mass flow, and a traceable flow calibration system can be used to perform a proof test. Typically, the outcome of this test is seen in calibration certificates as a graph depicting the relative measuring error of the instrument and the maximum permissible error band. All the measurement results are

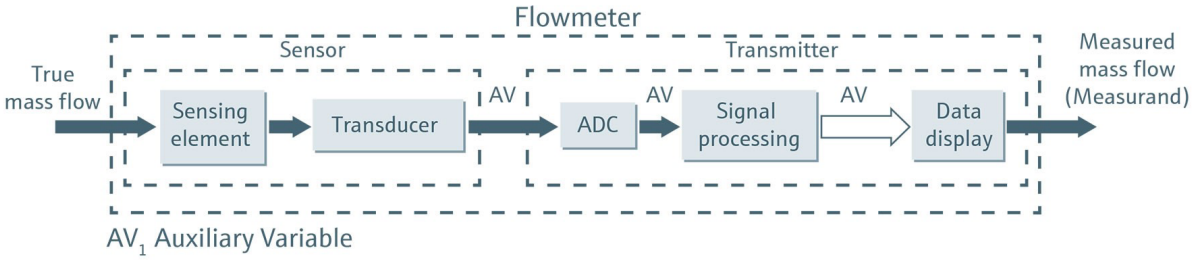



**Figure 8:** Basic components of a mass flowmeter. Source: BIPM.

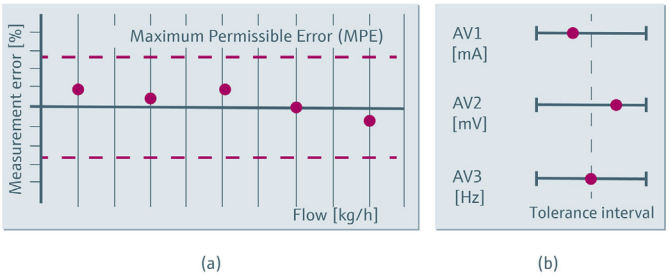



**Figure 9:** Verification concept: (a) the flowmeter is removed and the measurand (process value) is tested on a flow calibration rig. (b) auxiliary variables, such as mA and mV, are compared to reference values.

expected to be enclosed within this band for the verification to be considered positive (Figure 9a).

A second approach (Figure 9b) consists of assessing the functionality of an instrument by looking at one or several elements which can significantly impact the process value. In this case, verification can assist in assessing the instrument's functionality by observing the response of the process variable and the auxiliary variables. The auxiliary variables are compared to specific reference values to make sure they are within a tolerance interval established by the manufacturer.

Typically, proof testing requires the flowmeter to be removed from the process line and examined with specific equipment such as a mobile calibration rig or a verification unit. This rig or unit needs to be maintained and calibrated by qualified personnel, thus introducing a costly and time-consuming procedure. The process has to be shut down to perform testing, often causing a loss of production. If removal and reinstallation of the flowmeter are done in a hazardous area, safety issues can arise. In addition, the potential of personnel exposure to the process during the removal process can be another safety issue.

Modern instruments, such as mass flowmeters, typically have in-situ proof testing built into the devices. Endress+Hauser's mass flowmeters come with built-in Heartbeat Technology®. (While this article uses Endress+Hauser technology as an example of SIS management systems, other instrument suppliers may have similar technologies.)

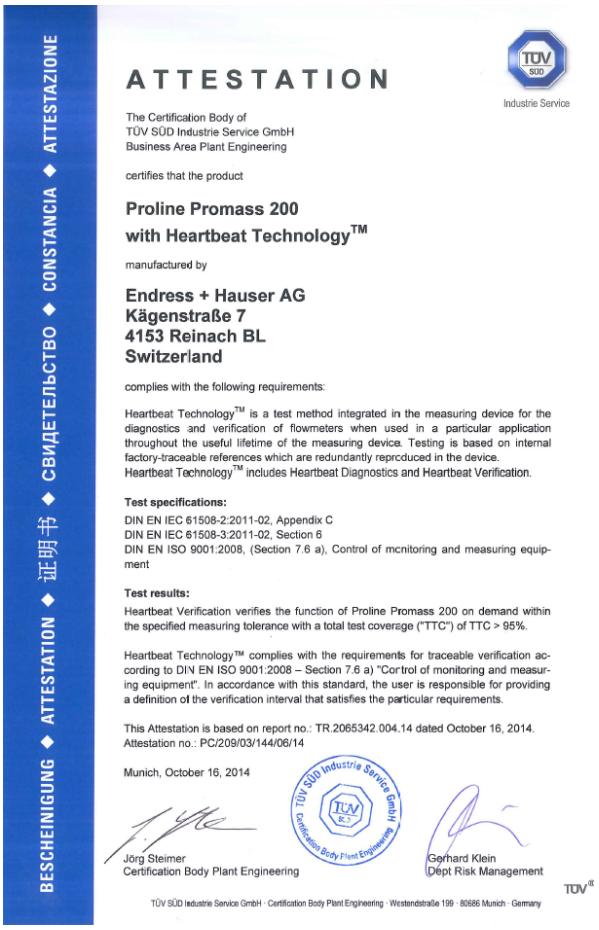
For example, with Heartbeat Verification, Endress+Hauser flowmeters offer a test method that does not require removal of the instrumentation or interruption of the process because the verification functionality is embedded in the device electronics.

A requirement of this verification method is high reliability. It must be ensured that the internal references used to verify the auxiliary variables remain stable and do not drift during the service life of the instrument. And if such drift does occur, it has to be detected immediately.

The stability of the references is ensured by using durable and high-accuracy components from suppliers meeting highest quality standards. However, it is through the use of an additional redundant reference that the detection of any potential drift is achieved. These redundant references are continuously cross-checking each other. If one or both references drift out of tolerance, these cross-checks will lead to a main electronic failure alarm to the safety controller. Redundancy of references is achieved differently depending upon measurement technology:

- Electromagnetic flowmeters use voltage references because the primary signal generated by the sensor is a voltage which is induced by the conductive fluid passing through a magnetic field.
- Coriolis, vortex, and ultrasonic flowmeters use frequency generators (i.e., digital clocks) as references because the primary signals are measured either by a time period (the phase-shift in a mass flowmeter or the time-of-flight differential in an ultrasonic flowmeter), or by the frequency of an oscillation (such as the rate of capacitance swings by the differential switched capacitor sensor in vortex flowmeters).

Seeing both references drift simultaneously in the same manner is very unlikely. On an installed base of 100,000 flowmeters, such an event is anticipated to occur just once every 148 years. Put another way, a device with a typical


BESCHEINIGUNG ◆ ATTESTATION ◆ 证明书 ◆ СВИДЕТЕЛЬСТВО ◆ CONSTANCIA ◆ ATTESTAZIONE

ATTESTATION

TÜV SÜD Industrie Service

The Certification Body of
TÜV SÜD Industrie Service GmbH
Business Area Plant Engineering

certifies that the product

**Proline Promass 200**
**with Heartbeat Technology™**

manufactured by

**Endress + Hauser AG**
**Kägenstraße 7**
**4153 Reinach BL**
**Switzerland**

complies with the following requirements:

Heartbeat Technology™ is a test method integrated in the measuring device for the diagnostics and verification of flowmeters when used in a particular application throughout the useful lifetime of the measuring device. Testing is based on internal factory-traceable references which are redundantly reproduced in the device.
Heartbeat Technology™ includes Heartbeat Diagnostics and Heartbeat Verification.

**Test specifications:**
DIN EN IEC 61508-2:2011-02, Appendix C
DIN EN IEC 61508-3:2011-02, Section 6
DIN EN ISO 9001:2008, (Section 7.6 a), Control of monitoring and measuring equipment

**Test results:**
Heartbeat Verification verifies the function of Proline Promass 200 on demand within the specified measuring tolerance with a total test coverage ("TTC") of TTC > 95%.

Heartbeat Technology™ complies with the requirements for traceable verification according to DIN EN ISO 9001:2008 – Section 7.6 a) "Control of monitoring and measuring equipment". In accordance with this standard, the user is responsible for providing a definition of the verification interval that satisfies the particular requirements.

This Attestation is based on report no.: TR.2065342.004.14 dated October 16, 2014.
Attestation no.: PC/209/03/144/06/14

Munich, October 16, 2014

TÜV SÜD Industrie Service GmbH Certification Body Plant Engineering

Jörg Steimer
Certification Body Plant Engineering

Gerhard Klein
Dept Risk Management

TÜV SÜD Industrie Service GmbH · Certification Body Plant Engineering · Westendstraße 199 · 80686 Munich · Germany

**Figure 10:** Sample TÜV Attestation for the Endress+Hauser Promass 200 mass flowmeter.

lifecycle of 20 years would have only a 0.007% probability of experiencing such a drift during its life.

Using the redundancy of internal references for a cross-check is a unique capability of this built-in technology. The validity of this approach has been attested to by independent third-party TÜV which states, “Testing is based on internal factory-traceable references which are redundantly reproduced in the device. Heartbeat Technology includes Heartbeat Diagnostics and Heartbeat Verification.” Additionally, TÜV attests that “Heartbeat Technology complies with the requirements for traceable verification according to DIN EN ISO 9001.” A sample attestation is included in Figure 10.

Heartbeat Verification thus ensures the traceable factory calibration of the internal references remains valid over the entire service lifetime of the flowmeter. The verification report satisfies the need to provide a document, either in electronic form, or printed and signed.

In practice, a verification report constitutes the front end of an unbroken, documented chain of traceability. Since the internal references remain valid over the lifetime of the instrument, their own documented factory-calibration performed in accredited facilities is the next link in this chain.

In addition, a traceable calibration of the instrument ensures that the integrity of the device has not deteriorated during assembly or handling in the plant. Calibration of the equipment used for calibration in the factory can then be traced back to national standards. In-situ verification is therefore compliant with international standards for traceable verification.

## Summary

Implementation of a SIS requires process risk protection to a targeted minimum while maintaining design and lifecycle costs at a reasonable level. Intelligent instruments and lifecycle management tools can help process plant personnel reduce risks and costs associated with a SIS system. They can also aid in capturing reliability data.


### About the Authors

Nathan Hedrick has more than ten years of experience consulting on process automation. He graduated from Rose-Hulman in 2009 with a Bachelor’s degree in Chemical Engineering. He began his career with Endress+Hauser in 2009 as a Technical Support Engineer. In 2014, Nathan became the Technical Support Team Manager for Flow where he was responsible for managing the technical support team covering the flow product line. He has been in Product Management since 2015 and is a TüV certified Functional Safety Engineer.

Howard Siew is the Chemical Industry Manager at Endress+Hauser USA. He’s responsible for the overall business development and growth of the company position related to the Chemical Industry. He is a chemical engineering graduate of Louisiana State University and TüV certified as Functional Safety Engineer in the area of SIS. In addition, he represents Endress+Hauser in the ISA84 working group where he contributes expertise and gains an understanding of the latest industry standards to advise customers and colleagues.

This document was originally authored by Craig McIntyre and Nathan Hedrick in 2016. It has been updated to/with current information by Howard Siew and Nathan Hedrick.