Increase Uptime by Reducing Systematic Failure Risk

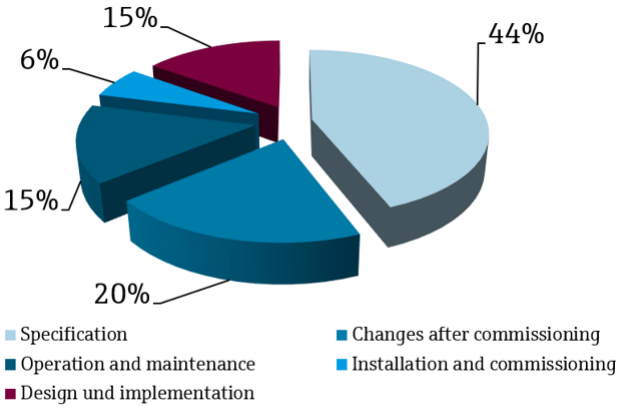
Reducing random failure is difficult, but process manufacturers can take clear steps to reduce systematic instrumentation failures.

By Howard Siew, Endress+Hauser

Pondering the history of industrial incidents, it would be incorrect to assume most failures occur at random. Muddying the already-murky waters of random versus systematic failure, safety instrumented system (SIS) design primarily considers probability of failure in demand (PFD) calculations, and PFD is tied to random failure rate and risk.

In reality, systematic failure in both safety and other automation systems occurs more frequently than random failure, as justified by United Kingdom Health Safety and Environmental Committee findings. Of failures recorded in the study, 65% were systematic in nature (Figure 1), caused by improper specification, design and implementation errors, and mistakes made during installation and commissioning.

Systematic failures of process instrumentation can be reduced by thoroughly understanding the application, sensing elements, logic solver, final element, material selection, and prior use experience. Failure conditions often originate at the design stage of a safety system before equipment is placed in service. By adjusting a device's design, manufacturing process, operating procedure, and/or documentation—process manufacturers can reduce inherent device shortcomings—which translates to decreased overall industrial process risk.



Source: United Kingdom Health Safety and Environmental Committee

Figure 1: A public study shows 65% of failures were systematic in nature and inherent in device specification, design and implementation, or installation and commissioning.

In this article, we look first at IEC 61508 (Functional Safety of Electrical/Electronic/Programmable Electronic Systems) and IEC 61511 (Functional Safety of SISs). We then describe how modern instrumentation addresses multiple risks of systematic failure, while simplifying commissioning and maintenance, for safety systems and other automation systems.

Random versus Systematic Failure

Random failure refers to primarily unavoidable hardware issues like electronic components that degrade over time and eventually fail. To reduce the impact of random failure, maintenance procedures employ proof testing throughout equipment lifecycles, with the hope of discovering fault risks and addressing them prior to failure. But even with rigorous testing, hardware is inevitably susceptible to occasional random failures (Figure 2).

Systematic failure—which refers to pre-existing problems caused by faulty equipment design, manufacturing processes, material specification, and/or device installation—is almost entirely avoidable through careful engineering. Functional safety standards protect against systematic failure by providing rules, methods and guidelines to prevent errors. When a system adheres to the appropriate standards, it functions with minimal systematic failures. Systematic failures are commonly caused by human error, be it operational or planning. For example, a lack of application understanding or insufficient maintenance planning may lead to failure caused by corrosion, abrasion, sedimentation or deterioration.

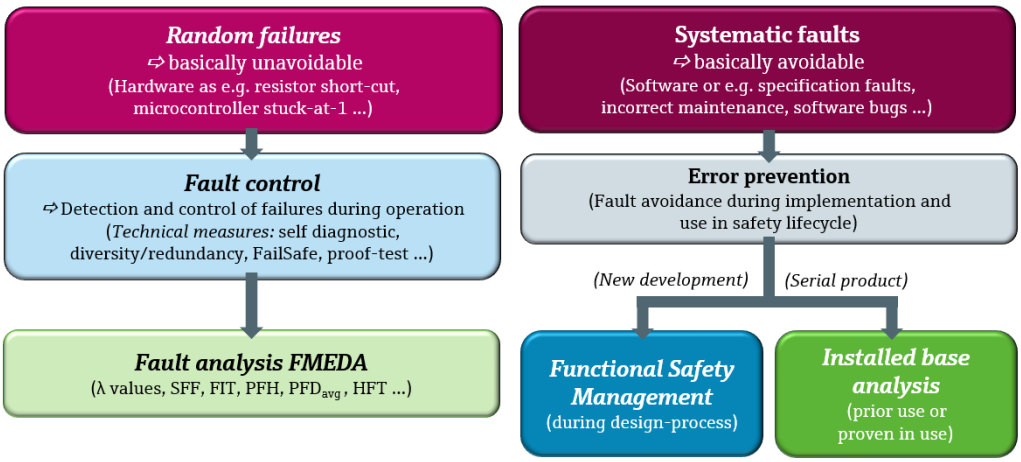


Figure 2: Random vs. Systematic Failures

IEC 61508 for Modern, Smart Instruments

Titled "functional safety of electrical/electronic/programmable electronic safety-related systems," IEC 61508 is applicable to any industry using electronic controllers within safety systems. It defines methods for application, design, deployment, and maintenance of automatic protection systems.

Per IEC 61508, manufacturers choose to certify their instruments by "design with full compliance" (Route 1H) or "proven in-use" (Route 2H) methods. Utilizing instrumentation in accordance with IEC 61508 provides several advantages:

- reduction in systematic errors throughout service life
- "prior-use" phase is shortened to 6 months versus 12 months with IEC 61508 (Figure 3) — "prior-use" status is achieved in accordance with NAMUR NE 130
- "prior-use" test following manufacturer software and firmware updates is not required for IEC 61508 compliant devices, provided they were previously in service

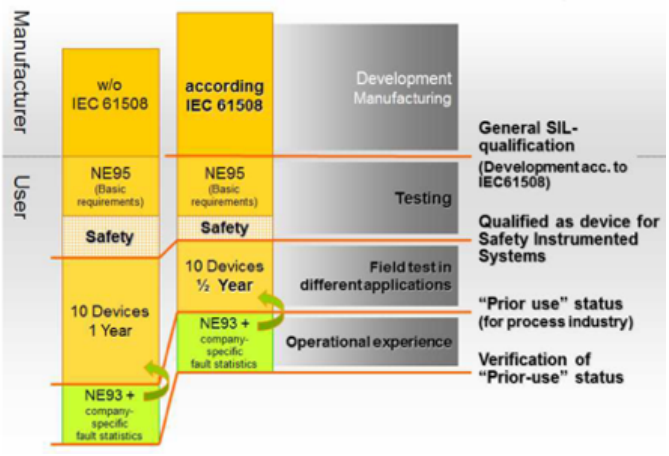


Figure 3: NAMUR NE130 provides an overview of the processes to get the "Prior-use" status. Image credit: NAMUR Recommendation version 16.09.2011

The IEC 61508 equipment functional safety manual includes critical information such as safety function, failure mode effect diagnostic analysis, and proof-test procedure. It provides all necessary information to define safety requirements of a SIS.

Process Influence on Safety Function

During SIS design, it is important to ensure instruments, materials, sizing and other factors are specified to meet the target application's requirements. If improperly specified, adverse consequences like corrosion, abrasion and cavitation can occur and degrade the safety function. Prior-use experience, when available, can aid in verifying a device's suitability to meet the required safety function. Many manufacturers offer software tools to verify specified equipment material and sizing is appropriate for the target application (Figure 4).

These types of tools can be used to simplify safety system design.

Installation and Commissioning

To meet IEC 61511 — titled "functional safety – safety instrumented systems for the process industry sector" — standards, equipment documentation must adhere to the safety requirements specification (SRS) for the SIS. An SRS for commissioning and proof testing includes scope, duration, state of the tested device, test procedures, state of the process, detection of failures and methods for error prevention.

Documented SRS procedures do not guarantee errorless installations, as plant personnel must pay careful attention not to miss critical parameter settings. However, they provide a roadmap to guide the way.

Modern, smart instruments also provide tools to aid in commissioning. A manufacturer can preset many of the required configuration parameters prior to device shipment, though it is still necessary to check these settings as part of installation and commissioning. To provide reliable safety functionality, the proper configuration must be initialized for the specific safety instrumented function.

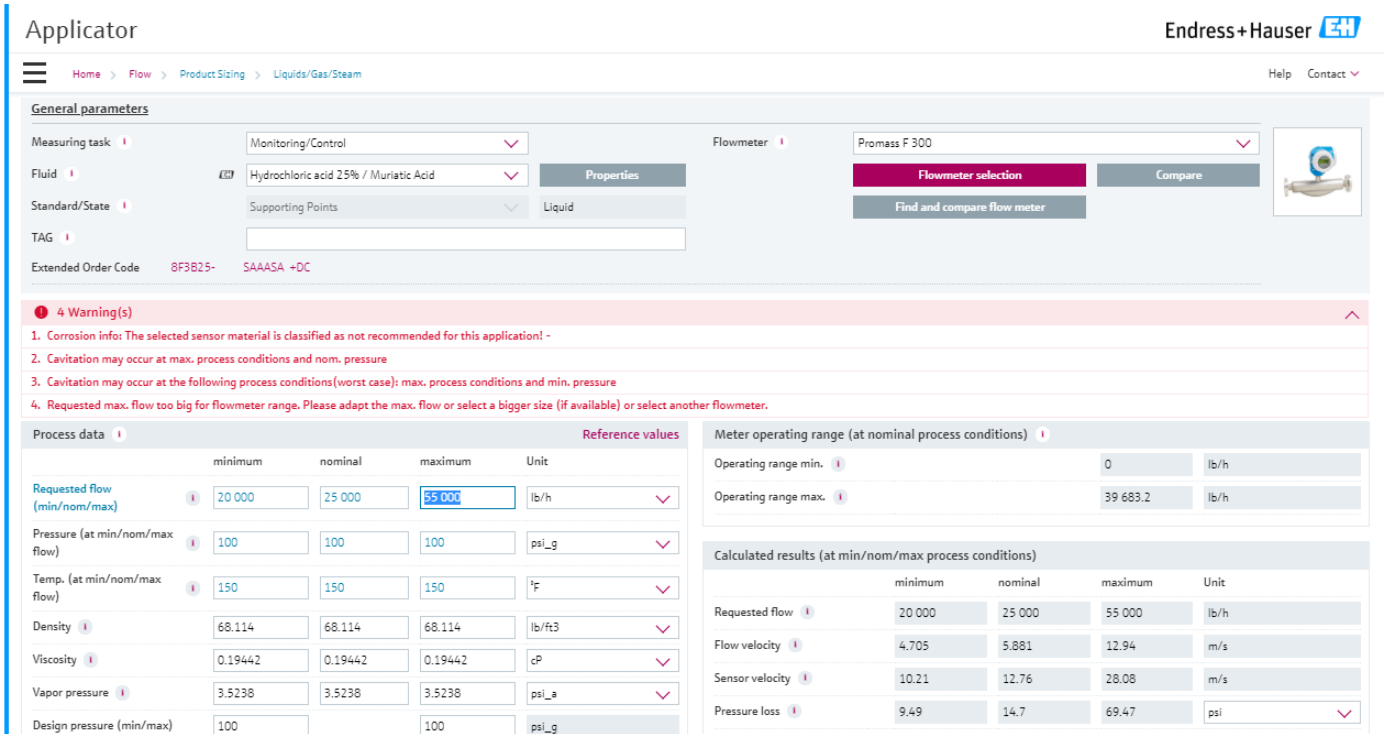


Figure 4: Endress+Hauser's online Applicator® tool helps ensure a device's function, material and size is suitable for the target process application.

An installer can perform the required safety integrity level (SIL) commissioning sequence through guided prompts on the instrument's device display or through asset management software tools (Figure 5). When using software, it is possible to generate a SIL-relevant parameters report following commissioning to ensure compliance with the safety function. The last step is to activate the SIL lock when present to prevent unauthorized tampering.

Operating Standards Aid Error Detection

A typical instrument, like a level transmitter, connects to a logic solver or safety controller in a SIS and sends the process variable via a 4-20mA or 4-20mA HART current signal. While a 4-20mA signal can only transmit the process variable, HART allows many other parameters to be transmitted, including diagnostic information.

Even with a basic 4-20mA signal type, per NAMUR NE 43 recommendations, a current in the 3.8-20.5mA range conveys a valid measurement value, while a signal less than 3.6 mA or greater than 21 mA indicates failure information to the safety controller or transmitter (Figure 6). NE 43 is utilized extensively across many industries, and most suppliers manufacture instrumentation operating within the 4-20mA signal range.

By adhering to the 4-20mA signal standard, manufacturers ensure their devices function with other vendors' instrumentation, and simultaneously reduce potential for incompatibility. Without this type of standardization, instrumentation cross-compatibility would be limited, and SIS errors would occur more frequently.

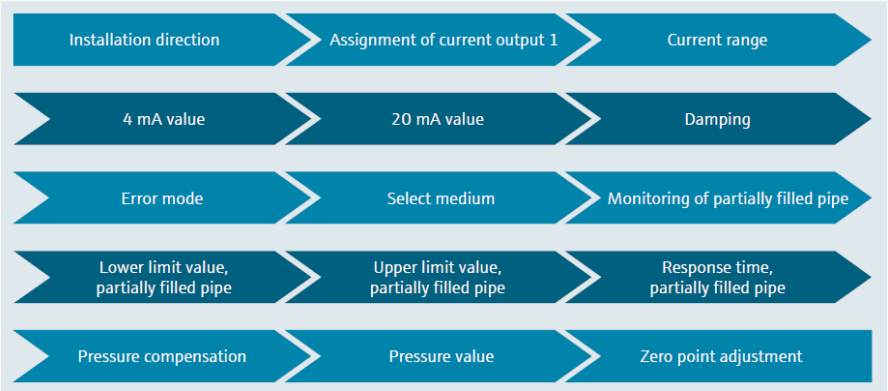


Figure 5: A SIL confirmation sequence using Endress+Hauser's FieldCare® software for checking flowmeter parameters

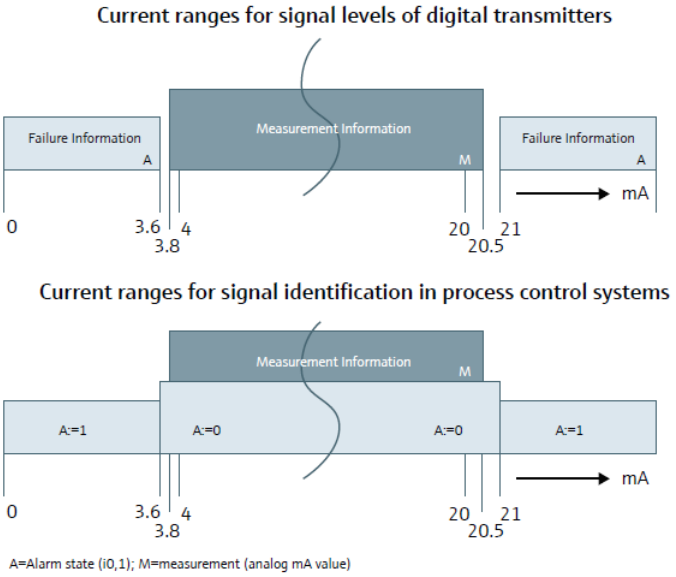


Figure 6: NAMUR NE 43 recommendations for 4-20mA transmitters (top) and process control systems (bottom) allow end users to confidently mix instruments from various vendors.

Status signal	Color	Symbol
Normal; valid output signal		
Maintenance required; still valid output signal		
Out of specification; signal out of the specified range		
Fuction check; temporary non-valid output signal		
Failure; non-valid ouput signal		

Figure 7: Five standard status states specified by the NAMUR NE 107 recommendation

Many modern, smart devices also utilize NAMUR NE 107 recommendations to provide five basic status indications for identifying normal state or one of four error types (Figure 7). These status indications, when present, are most often communicated via HART. Error types include:

- maintenance required
- signal out of specified range (often adjustable via a transmitter)
- function check/temporary invalid signal
- instrument failure

NE 107 allows for routing of error signals to operations or maintenance staff when a problem exists. A user can drill down into further diagnostic data to identify error causes by utilizing a field device management tool, such as Endress+Hauser's FieldCare software.

Reducing Systematic Failure during Proof Testing

Every plant requires personnel to run, manage and ensure continued operation, but human error can introduce problems to automated systems, particularly during atypical maintenance procedures. For example, instruments temporarily pulled out of service for proof testing are sometimes damaged in the course of re-installation. When possible, it is advantageous to reduce touchpoints on instrumentation to lessen systematic failure risk, especially for components of a SIS.

For certain applications requiring proof tests, partial in-situ testing can reduce the frequency of full proof tests. In a full test, the instrument under examination is manually removed from service and tested on a bench. In-situ testing eliminates instrument removal and should therefore be used whenever possible because it reduces system downtime, saves money on testing, avoids exposure to hazardous process or chemicals and reduces systematic error rates.

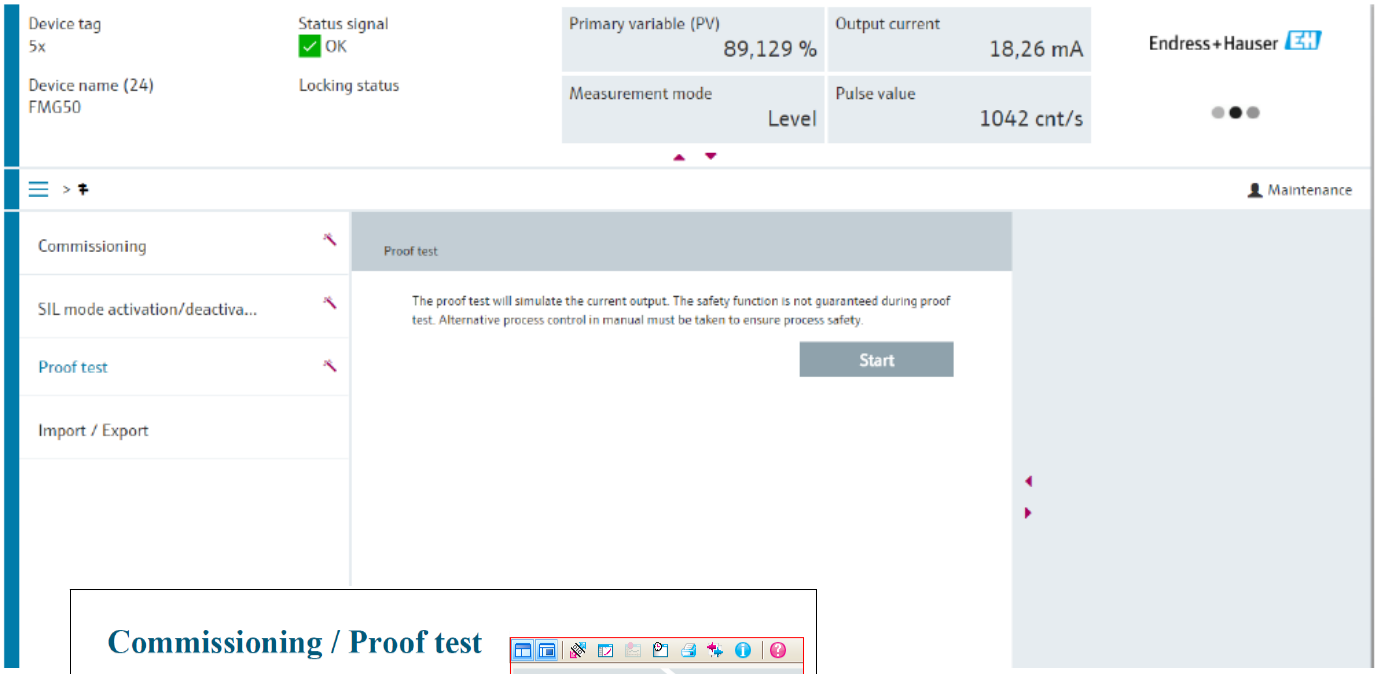
For applications where in-situ testing is not possible, IEC 61508-compliant manufacturers offer guided proof testing sequences to minimize systematic failure. These step-by-step instructions reduce the potential for human error (Figure 8).

These documents also detail the reporting format to create comprehensive verification reports, consistent across every instrument in the plant.

Reducing Operational Systematic Failures

Conditions like corrosion, abrasion, sedimentation, and overall process deterioration can cause system upsets. Smart devices' predictive statistics can be used to predict these and other types of failures, allowing personnel to attend to potential faults prior to malfunction.

Condition monitoring systems help interpret measured data to more accurately forecast failure possibilities. The predictions provided by these systems help users schedule maintenance and improve process optimization. Possible applications of condition monitoring include the detection of deposit buildup or corrosion-induced wear (Figure 9). Systematic failures can also occur during device replacement. Even when an instrument is replaced with an identical substitute, the complexity of modern instrumented systems makes it difficult to properly set all parameters manually. However, there are tools that validate an identical copy of configuration parameters—such as watchdog, checksum, reverse conversion loops, and others—from the old instrument to the new. These elements are integrated into



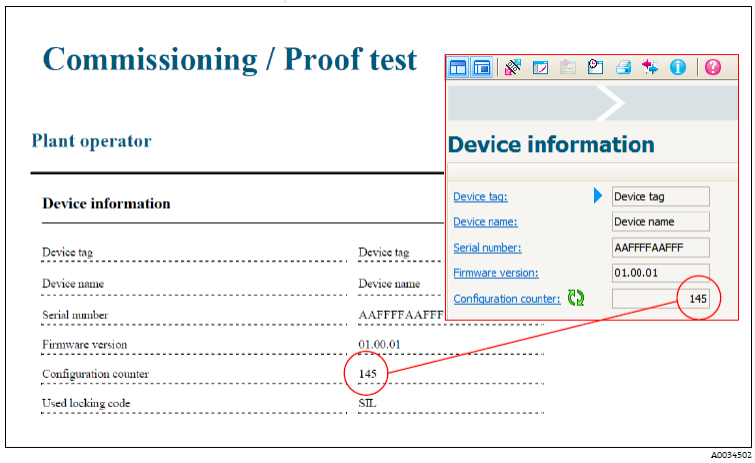


Figure 8: A guided proof test helps diminish operator errors. If the values indicated as shown above are identical, the device configuration has not changed since the last proof test.

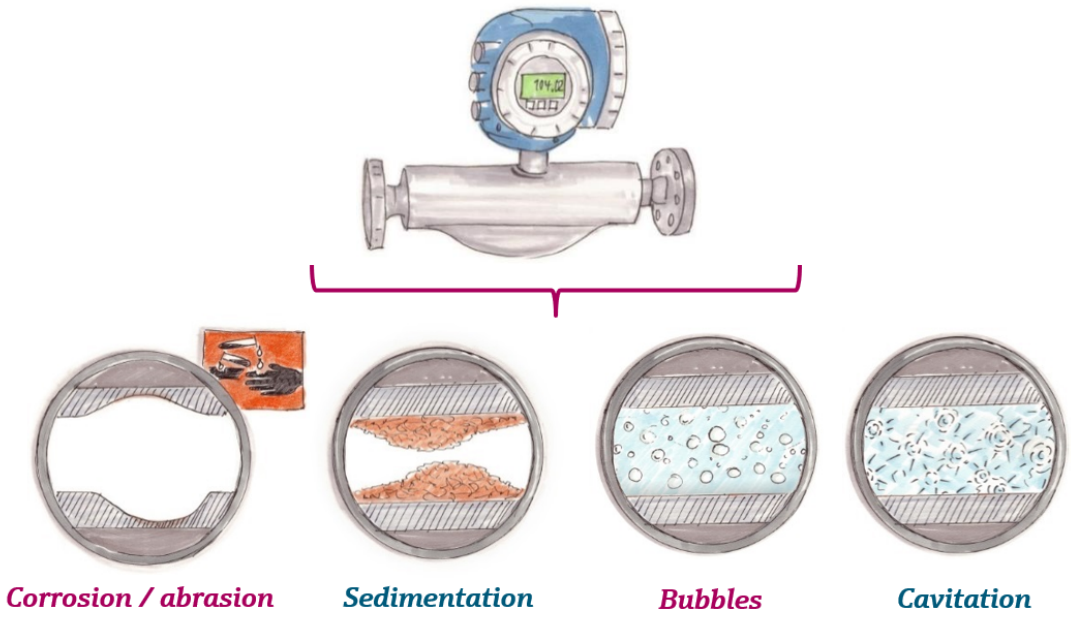


Figure 9: A condition monitoring system can detect process variances in the early stages to avoid costly systematic failures.

the instrument device diagnostics. If a user is notified of a disparity, this indicates a potentially erroneous configuration. Configuration software can automatically detect and alert the user when there is a difference in these settings.

IEC 61508 Compliant Level Switches Ease Maintenance

A hydrocarbon producer plagued with maintenance issues introduced IEC 61508-compliant tuning fork level switches to streamline operations and reduce risk of systematic failure. Previously, the producer used non-compliant level switches to prevent tank overfill of a highly toxic chemical, and the tank needed to be emptied and cleaned once annually to remove the level switches and perform full proof tests.

After replacing the instrumentation with IEC 61508 compliant level switches, the producer was able to perform in-situ testing without instrument removal, requiring a full proof test just once every three years.

Personnel are now able to monitor the tuning fork level switch diagnostic functions and oscillation frequencies to detect corrosion before it is visible to the human eye, enabling predictive maintenance for decreased systematic failure occurrence.

In-situ proof testing of the new instrumentation is carried out using Endress+Hauser's SIL verification sequence wizard, which provides step-by-step instructions to ensure adherence to the proper procedure. The sequence wizard produces a SIL verification report at its conclusion, transmittable as a portable document format file. These new capabilities cut system downtime, ease maintenance difficulties and reduce systematic failures.

Summary

Throughout the safety lifecycle, systematic failure focus is critical in SIS design. Proper risk assessment and comprehension of the safety application helps minimize systematic failures. While random failure risk will always exist in varying quantities, systematic failure risk can be reduced to exceptionally low levels by employing the following tactics:

- consider available application data and ensure device function, material, and sizing suitability
- deploy detailed operating procedures for devices in service
- adhere to standards such as IEC 61508 (Functional Safety) and IEC 61511 (SIS)
- reduce human touchpoints and minimize frequency of full proof tests, as allowed by the SIS

Reducing systematic failure risk of instrumentation leads to increased uptime and throughput, while reducing maintenance expenses and improving process safety. Risk reduction starts with careful supplier selection, and continues throughout design, installation, commissioning, operation and maintenance.

About the Author

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 participates in the ISA84 working group where he contributes expertise and gains an understanding of the latest industry standards to advise customers and colleagues.