InTech FOCUS

An *InTech* e-edition covering the fundamentals of automation

SEPTEMBER 2020

Process Safety

How Safety Best Practices Improve OT Cyber Security

Managing SIS Process Measurement Risk and Cost

The Impact of ISA-84.1

ISA/IEC 61511 Certification

Introduction

Process safety is continually evolving, both strategically and tactically. Safety best practices evolve and improve, and even influence industrial cybersecurity. Successful implementation and management of a safety instrumented system (SIS) requires designers and operators to address a range of risks and expand their areas of knowledge. The safety life cycle, according to IEC 61511 or ISA-84, provides detailed requirements and a framework for the safety management system. Understanding more about these standards and the measurement technologies behind them can help safety system designers reduce risk and cost.

InTech magazine is the official publication of ISA—The International Society of Automation. It is published six times per year. *InTech Focus* is its counterpart, brought to you in conjunction with Automation.com. This series of electronic magazines focuses on the fundamentals of essential automation components, such as instrumentation, final control elements, networks, drives, and more. Six times a year, look for *InTech Focus* to learn how to choose instrumentation and control solutions, as well as apply them, calibrate them, and optimize their contribution to efficient operations.

Find other ebooks in the series at https://www.automation.com/en-us/resources-list-pages/intech-focus-ebooks.

View and subscribe to *InTech* magazine at https://isa.org/intech

Renee Bassett, Chief Editor
rbassett@isa.org

Our Sponsors:

In This Issue

Upcoming Issues:

November: Final Control Elements

January 2021: Flow & Level

March 2021: Temperature & Pressure

Account Managers:

Chris Nelson
+1 919-990-9265
cnelson@isa.org

Richard Simpson
+1 919-414-7395
rsimpson@isa.org

KEEP IT SAFE

MOORE INDUSTRIES WORLDWIDE
Demand Moore Reliability

Keep your process and plant safe with FS Functional Safety Series instrumentation from Moore Industries. You can be confident that they will help ensure the safety of your process and facility when you need it the most. Our Logic Solver, Signal Isolators and Transmitters are built to strict IEC 61508 standards, ensuring safe and reliable operation – particularly in environments where hazardous or emergency situations are likely to occur.

The rugged and reliable FS Safety Series Instruments from Moore Industries.

To learn more about our **FS Functional Safety Series**, Call **(800) 999-2900**
or go to: **www.miinet.com/KeepItSafe**

How OT Cyber Security is Improved with Process Safety Best Practices

By Chris Lyden, PAS advisor, and Eddie Habibi, PAS Global

Information technology (IT) cyber security traditionally focuses on the "CIA triad" of confidentiality, integrity, and availability. The practices associated with this model are intended to ensure data is:

- kept private
- not compromised in any way
- available when needed.

Automation and process-safety best practices can also improve control and alarm performance, human interface effectiveness, and automation system resiliency

OT (Operational Technology) is concerned with the automation systems that facilitate safe production in process and manufacturing industries. OT cyber security differs from the IT cyber security model because it is not only concerned with data protection, but also with the prevention of cyber espionage and the risk of impact to process safety, reliability, and the environment. OT cyber risk is growing in both frequency and sophistication as malicious actors have recognized the level of dependence modern societies have on OT to manage critical infrastructure. They are increasingly using automation, machine learning and artificial intelligence to create highly tar-

geted exploits directed at critical infrastructure. These exploits must leverage detailed knowledge of specific automation systems and industrial processes

The most effective way to counter these exploits is to apply automation and process-safety best practices in addition to IT-focused cyber security measures. Beyond protecting OT systems against cyber attacks, these practices also improve control performance, alarm performance, human interface effectiveness, and automation system resiliency. This in turn improves profitability, safety, and reliability.

This article reviews the five operations safety independent protection layers (IPLs) and how applying best practices for each greatly improves OT cyber security:

- IPL 1 – Inventory and Configuration Management
- IPL 2 – Automatic Process Controls
- IPL 3 – Human Intervention
- IPL 4 – Safety Instrumented Systems
- IPL 5 – Physical Protection

Safety independent protection layers

Industrial processes and process automation systems are designed with a series of safety independent protection layers (figure 1) that serve as preventive safeguards in the event of an abnormal process event. These layers address the risk of equipment failures but are also highly valuable in the event of a cyber attack. Each layer represents an escalation in the effort to safely mitigate the effects of an abnormal event. When these layers are functioning properly, any operational changes caused by cyber exploits become apparent to plant personnel sooner, so a coordinated OT/IT response can be initiated, and remediation is easier and faster.

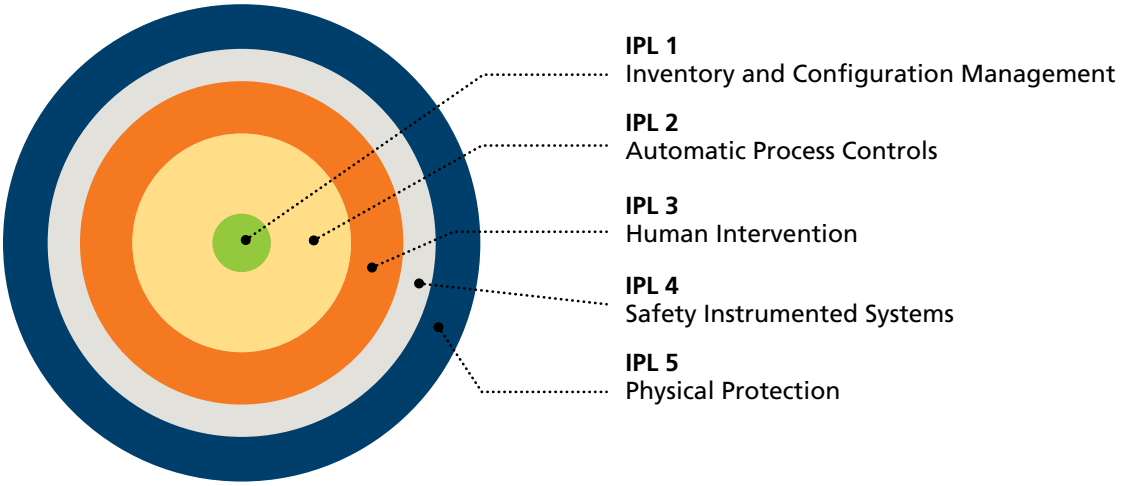


Figure 1. Independent protection layers

Safety IPL 1 – Inventory and Configuration Management

The foundational operational best practice for improving OT cyber security is inventory and configuration management of industrial process automation systems. In addition to controlling the process, automation systems are tools for continuous productivity improvement. As a part of daily operation, their configuration is routinely modified by plant personnel in pursuit of this productivity. These modifications may entail controller tuning or alarm limit changes. They may also involve the addition of a new control scheme, or a redesign of an existing one. Ensuring every configuration change is both safe and sanctioned is critical for process operations.

Most companies have implemented some degree of automation Management of Change (MOC) procedures to prevent configuration changes from causing unintended consequences. These procedures usually entail reviews for both operability and safety, and the reviews generally occur before a change is implemented.

There is often no follow-on evaluation after the change has been implemented and accepted by operations, however. In a world where cyber saboteurs seek to do damage by altering automation system configuration, the concept of management of change must expand to include continually monitoring the actual configuration database, and comparing it to a known good and protected record copy.

> "The Stuxnet attack would have been caught much earlier with effective management of change."

In the 2010 Stuxnet attack in Iran, the saboteurs used their detailed knowledge of the automation system to deploy a man-in-the-middle attack that portrayed normal operating conditions to the operators, while taking charge of the controls to destroy the process centrifuges. To accomplish this, the attack modified both the control program and the database of the process controller. Inspectors with the International Atomic Energy Agency visiting the Natanz uranium enrichment facility noticed that its centrifuges were failing at a very high rate. While no one knows for certain, there is evidence that the centrifuge failures may have begun as early as late 2009. However, Stuxnet's role in the centrifuge failures was not recognized until June 2010, months after it first began its sabotage. It is estimated that during this period, Stuxnet damaged or destroyed 984 uranium centrifuges. It is clear from the way Stuxnet functioned, that a robust configuration MOC regimen would have caught the worm long before this level of damage occurred.

Safety IPL 2 – Automatic Process Controls

Although process automation systems perform a variety of tasks, including monitoring, reporting, and historization of production data, they are foremost process control systems. They read critical process measurements and adjust control devices to keep the process at the desired operating state. Process controls are analogous to the autonomic nervous system in the human body; they operate continually and automatically to keep the plant in a stable operating state. Just as with the body's autonomic system, malfunctions can be very disruptive and sometimes dangerous.

Disruptions to process control stability can occur for a variety of reasons. Commonly, they are caused by poor controller tuning, instrument failures, or control valve problems. A sophisticated cyber attack may modify the tuning parameters of the process controllers to destabilize the process. Tuning parameters control the magnitude and speed of the process controller's response to a change in the process. A control change that is too great or that occurs too quickly can rapidly introduce disruptions to the process. A change that is too small or occurs too slowly will allow the process to drift further from the desired operating point. In either case, the process will become destabilized, which can result in product quality issues, lost production, equipment damage, or worse. The greatest risk in such an attack is that operating personnel may never think of them as cyber attacks, and simply write them off as routine process disturbances. It used to be that hackers did not understand how process controller tuning worked. Now many of them do, thereby, increasing the risk to process stability.

An important best practice in support of OT cyber security is deploying a control loop health monitoring application that identifies abnormalities in controllers, sensors, and actuators. Implement an application that can report control performance issues and prioritize them according to their impact on safety and efficiency of operations. When combined with risk management visualization and alerting tools, plant personnel can quickly identify abnormal parameters and restore controllers to normal state. In sum, what many have thought of traditionally as an operations tool is equally valuable for cyber defense.

Safety IPL 3 – Human Intervention

Human beings intervene in the handling of an abnormal event using the human interface displays and alarm handling capabilities of the process automation system. The initial design of these critical automation system components is often quite poor, creating an environment where critical operational information may

be obscured or lost—exactly when it is needed most. Using tools, services, and methodologies that greatly increase situation awareness for plant operators effectively leverages the operators as another tool in the detection of cyber incursions.

Let's examine how to defeat cyber attacks on the automation system by properly managing process alarms and operations risk management visualization tools.

Process alarms

Process alarms are preconfigured notifications of a measured process variable deviating from its desired value by a significant amount. They are the primary means of alerting operations personnel to process problems. However, cyber attackers may disable alarms to hide their mischief from plant operators.

> "In the Stuxnet attack, critical process alarms were disabled, so process operators were unaware of the sabotage."

Consider again the 2010 Stuxnet attack in Iran. It included a rootkit that hid its malicious files and disabled the critical process alarms that would have normally tipped off the process operators to the sabotage.

To prevent attacks such as this, we must ensure the alarm system cannot be disabled or alarms masked. An important part of an alarm management regimen is a process called alarm Documentation and Rationalization (D&R). D&R creates a master alarm database to maintain the alarm trip point settings and other critical alarm information separately from the automation system itself. A comprehensive alarm management solution includes functionality to audit the state of the alarms in the automation system, and if they have been modified, to automatically restore their proper values from the master alarm database. This functionality ensures that alarms disabled as part of a cyber attack strategy will not remain so.

High-performance HMI and risk management visualization tools

Processes are generally operated from a set of computer screens (referred to as Human-Machine Interfaces [HMIs]) that depict the operation of the process by displaying key measurements and process alarms. Because automation systems are so easily customized, project engineers often pack information too densely onto the HMI screen, and use display attributes (such as colors, blinking and reverse video) too generously and inconsistently. This approach produces cluttered HMIs that reduce the ability of process operators to rapidly distinguish abnormal situations as they develop. Figure 2 is an example of a poorly designed HMI display that makes rapid identification of abnormal situations extremely difficult.

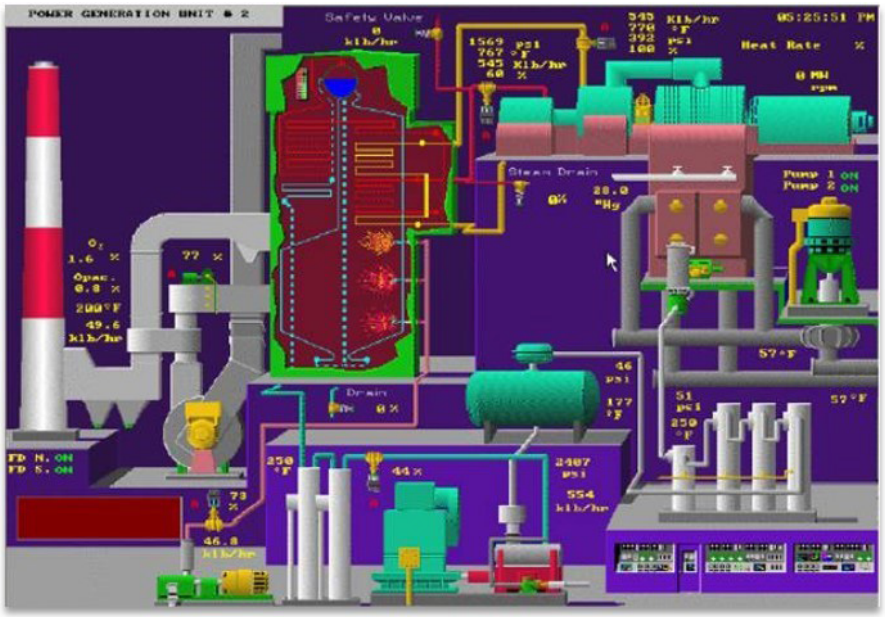


Figure 2. Example of poor HMI design

Source: Maximize Operator Effectiveness: High Performance HMI Principles and Best Practices, Bill Hollifield, PAS Global, LLC, 2015.

For IPL 3 to be maximally effective, plant operators must rapidly identify an abnormal situation and effectively react to it. HMI screens should use a standard set of display objects and be developed using a consistent style guide. Best practices for HMI development call for minimal use of color, and then only to draw attention to a deviation from normal operation. Figure 3 shows a properly designed display. It is easy to see how the display in figure 3 facilitates a faster and more accurate response by operations personnel to both process and cyber events.

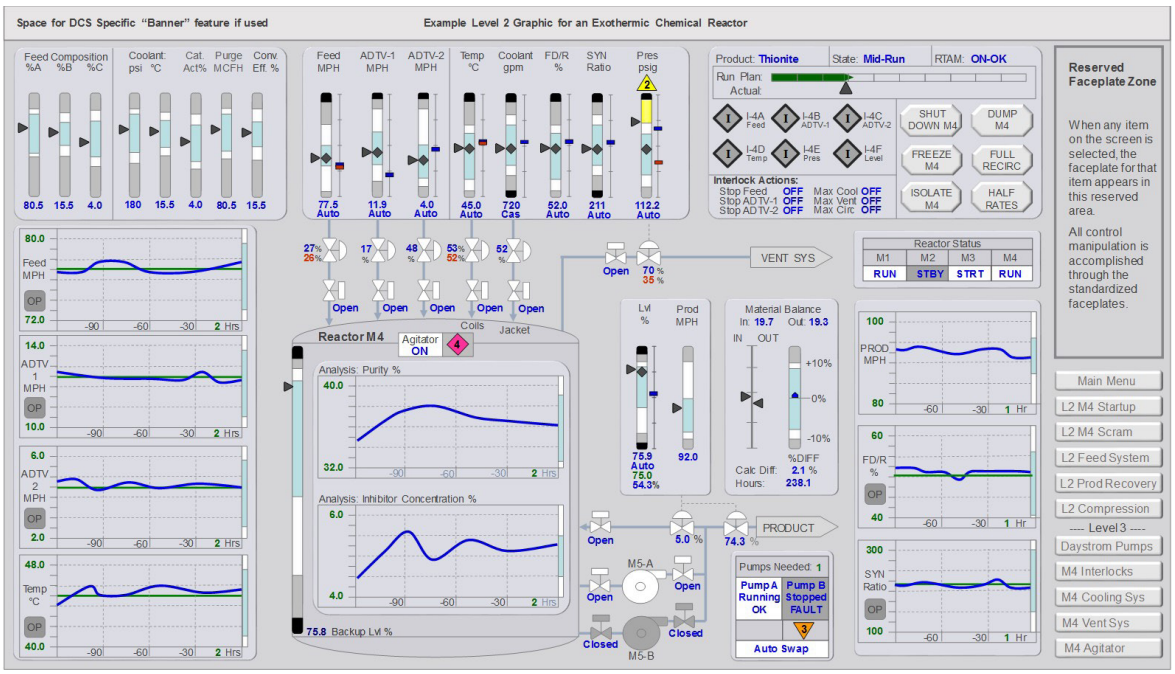


Figure 3. High-performance HMI design

Source: Screenshot of PAS High Performance HMI™ design

Safety IPL 4 – Safety Instrumented Systems

A Safety Instrumented System (SIS) monitors critical safety-related process measurements in a plant. If the predefined thresholds of these critical measurements are violated, the SIS runs automated procedures to bring the plant back to a safe operating state. Often, the safe operating state entails a complete—but safe—shutdown of the process.

Recently, a tailored exploit called Triton attempted to penetrate the SIS at a large petrochemical plant in the Middle East. The intent of the exploit was apparently to modify the safety instrumented functions in the SIS to prevent it from executing its shutdown function. It is speculated that the exploit may have also intended to penetrate the plant's process control system to manipulate key operating parameters, causing the plant to go out of control. Had this exploit been successful, the result could have been lost production, physical damage to the plant, and possibly harm to plant personnel. Exploits like Triton underscore the importance of SISs to saboteurs and should cause us to place increased cyber security emphasis on the SIS.

"In the Triton attack, safety instrumented functions were modified to prevent a safe shutdown."

SIS monitoring

To ensure that the SIS is available to perform its job if an abnormal event demands it, use an application that monitors and analyzes the performance of Safety Instrumented Functions (SIFs), which are the automated procedures that return a plant to a safe operating state when an abnormal situation occurs.

Tracking the rate of demand on the SIS offers an indication of how often it is called upon to intervene in an abnormal situation. A significant increase in SIS demand may be an early indicator of malevolent cyber activity affecting the process controls, so it is important to monitor this on an operational risk dashboard.

In some normal operational scenarios, such as process transitions, it is necessary to temporarily bypass the safety instrumented functions of the SIS. When this occurs, the safety functions are performed and closely monitored by operations personnel. If, however, the SIFs were bypassed as part of a cyber attack, operations personnel may not be aware of it. This scenario is very similar to the Triton attack mentioned above and would leave a plant dangerously exposed.

Operational boundary management

The nature of some processes requires operations to push production to the limits of equipment physical design constraints. This often requires personnel to monitor a variety of new parameters, which taken together define safe operational boundaries. These parameters include process alarm limits, SIS trip points, environmental excursion limits, and relief valve settings. As long as process operations remain within the boundaries defined collectively by these parameters, they will function safely to onsite and remote personnel.

These safe operational boundary parameters exist in every plant, but they are scattered among a variety of different databases and systems. This distribution of key safety parameters prevents process operators from having a full understanding of their operational boundaries. Therefore, a best practice is to validate and aggregate all of those parameters and visualize them contextually in relation to each other. Leverage an application that performs this validation, aggregation, and visualization in real time, and provides automatic notification of boundary excursions.

Cyber attacks that reconfigure operating boundaries have the potential to do great harm. For example, an attacker may set the value of a reactor high-pressure alarm above the SIS trip point. In this scenario, the reactor pressure could rise to dangerous levels, and the SIS could shut down the process without the operator ever knowing why. Leverage a tool that validates not only the absolute value of the parameters, but also their dynamic relationship to one another, which would therefore prevent such an attack from being successful. Only by aggregating, monitoring, and validating these diverse parameters, can we prevent such an attack.

Safety IPL 5 – Physical Protection

Industrial plants equipment has built-in physical protections designed into the process itself. These devices include rupture disks and pressure relief valves. Generally, these remedies prevent catastrophic outcomes, but also result in a loss of containment. When an abnormal situation progresses to this point, the focus shifts from proactive protection to reactive mitigation. The intent of a rigorous OT cyber security program should be to identify and prevent activities before the physical protections of IPL 5 are engaged.

Safety IPLs essential

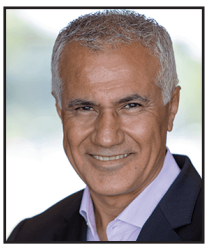
Traditional IT cyber security practices are a necessary part of a comprehensive OT security program. But OT cyber security requires additional tools and best practices based on a detailed

"Cyber attacks that reconfigure operating boundaries have the potential to do great harm."

understanding of the internal workings of each of the process automation systems implemented in a plant. All five of the safety IPLs described in this article are essential to an effective OT cyber security strategy. They quickly identify database changes that may lead to catastrophe and enable plant personnel to serve as additional detectors of potentially malicious cyber intrusions. They facilitate mitigation and remediation in the event of a cyber attack and greatly improve the operational safety and efficiency of the plant, as well as its productivity to the business bottom line. No OT cyber security program is complete without them.

ABOUT THE AUTHORS

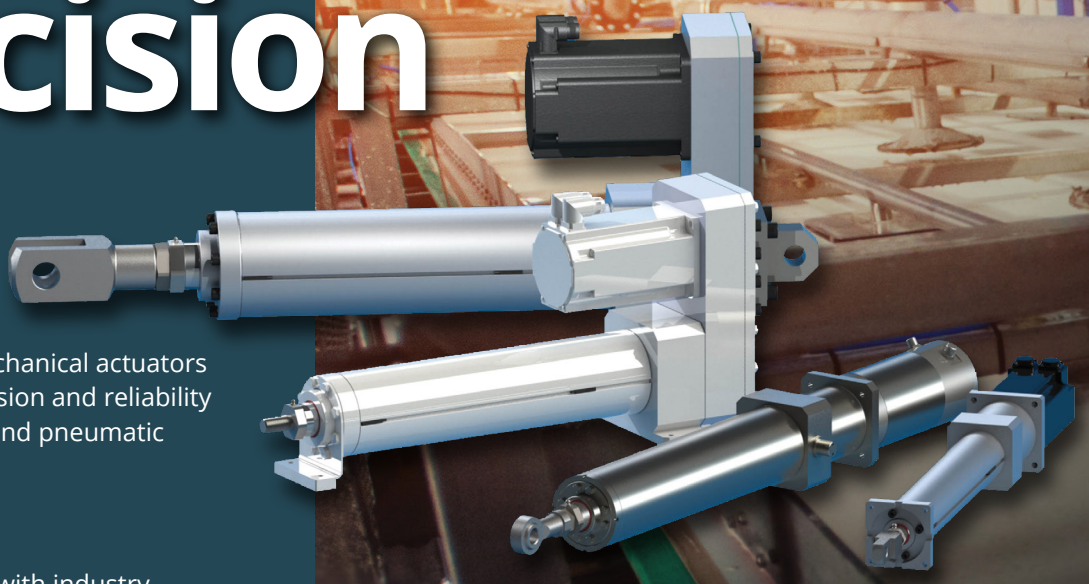
Chris Lyden, PAS advisor, is an accomplished professional engineer with 44 years of experience in the process automation industry. He has worked throughout the process industries, including in oil refining, petrochemical manufacturing, fine chemicals and pharmaceuticals, and power generation. He has held positions in R&D, project delivery, sales, marketing, strategy, and executive management at Honeywell, Invensys/Schneider Electric, and PAS. Lyden retired in January 2019 and serves in an advisory capacity to PAS.



Eddie Habibi is the founder and CEO of PAS Global, a leading provider of software solutions for the industrial sector. A visionary and thought leader in the fields of industrial control systems and operational technology, Habibi is a renowned industry speaker, author, and business executive. Habibi's expertise spans industrial cyber security, the Industrial Internet of Things, Industrie 4.0, data analytics, and operations management, and his guidance is highly valued by commercial enterprises, government organizations, and industry associations worldwide. In 2017, Habibi was listed by CRN as one of the "30 Internet of Things Executives Whose Names You Should Know." He is the coauthor of two popular best-practices books on operational risk and safety management: *The Alarm Management Handbook and The High Performance HMI Handbook*. Habibi holds an engineering degree from the University of Houston and an MBA from the University of St. Thomas.

HUNT VALVE
ACTUATOR DIVISION

Unparalleled Linear Motion Precision



Hunt Valve Actuator Division specializes in electromechanical actuators that offer superior precision and reliability compared to hydraulic and pneumatic driven units.

Our actuators offer:

- Ease of integration with industry-standard motors, drives and PLCs
- Exceptional performance, quality, and durability
- Extreme configurability of drive and mounting styles
- Decrease lifetime costs compared to hydraulic and pneumatic
- Reliable solutions for a wide range of environments

Learn more about the advantages of electromechanical actuators and the factors to consider when choosing your unique solution by downloading our guide, *How to Select the Appropriate Electromechanical Actuator*.

I Want the Guide

» Contact Us to Get Started » www.huntvalveactuators.com » 540-871-9871

ISA-84: Development and Impact of the SIS Standard

By Paul Gruhn, PE, CFSE, aeSolutions

Thirty-six years ago, ISA-84.1 changed the automation industry. This standard for the application of safety instrumented systems for the process industries has led to the development of IEC standards on functional safety—and so much more

ISA-84.1, *Application of Safety Instrumented Systems for the Process Industries*, was the world's first standard on safety instrumented systems (SISs) (a.k.a. emergency shutdown systems) developed by a standards development organization. The standard was chartered in 1984 (hence its number) and was first released in 1996. It led to the development of International Electrotechnical Commission (IEC) standards on functional safety, product and personnel qualification programs, new books, new products, new software, and recognition by regulators around the world. In short, it changed the industry.

Relays have been used in safety applications for almost 100 years. Solid-state systems (that did not use software) were developed by several vendors in the 1970s. General-purpose programmable logic controllers (PLCs) have been used in some safety applications since the 1970s. Safety PLCs have been available since the early 1980s. Yet at that time there was no industry agreement on what steps to include in a project life cycle, how to determine the performance required of a system, how to model the performance of hardware and software, and much more.

Safety PLCs have been available since the early 1980s, but there was no industry agreement on what steps to include in a project life cycle.

The development of a standard was proposed to ISA in the early 1980s. Someone from one of the safety PLC vendors served as the first chairman of the committee. Within a few years it was decided that a vendor should not lead such an effort, and the leadership transitioned to an end user.

The original charter of the standard was to cover software-based logic solvers only; field devices were not included in the original scope. The scope was expanded in the early 1990s to include other logic solver technologies, as well as field devices.

The ISA84 committee met three times a year at the ISA leader meetings (then called president's meetings) around the U.S. Although there were hundreds of committee members, attendance at face-to-face meetings was typically fewer than 50.

Since it is virtually impossible to get 50 people in a room together to agree on anything, the committee formed into four working groups: general, design/engineering, system analysis/modeling, and operations/maintenance. Although loud discussions could be heard through the hotel meeting room walls, the smaller groups were able to develop their respective portions of the final document.

Ten years of deliberation brought consensus on the following topics: system life cycle; methods to determine the required system performance (safety integrity level [SIL]); methods to analyze the performance of hardware and what to include in the calculations; factors to include in the design of a system; and factors to consider in the operation, maintenance, and changes of a system. The first edition of the standard, released in February 1996, was approximately 40 pages long and had five informative annexes totaling almost 60 pages.

In the mid-1990s, the IEC started developing its functional safety standards. The ISA84 committee actively participated in the development of the IEC 61511 standard for the process industry. That standard was first released in 2003 and was adopted as ANSI/ISA-84-2004 one year later with the addition of one sentence.

ANSI/ISA-84-2004 is a three-part standard. Part 1, the normative portion, was more than 90 pages. Part 2, an informative document, was also more than 90 pages. Part 3, another informative document summarizing various SIL selection methodologies, was more than 60 pages.

The Occupational Safety and Health Administration published interpretation letters stating that it considered the first and second editions of the ISA-84 standard to be "recognized and generally accepted good engineering practice" (RAGAGEP). After the IEC released a second edition of the 61511 standard in 2016—and after a one-year period of editorial changes—the ISA84 committee accepted the new standard verbatim (although it added a new U.S. forward in Part 2). The standard is now called ANSI/ISA 61511-2018.

The work continues. Over the past 15 years, the ISA84 committee has written eight technical reports comprising more than 1,000 pages further explaining the standard and the ways of implementing its various requirements.

ABOUT THE AUTHOR

Paul Gruhn, PE, CFSE, and ISA Life Fellow, is a global functional safety consultant at aeSolutions in Houston, Texas. Gruhn is a Society past president, ISA Fellow, and cochair and 30-year member of the ISA84 standard committee. He is a developer and instructor of ISA courses on safety systems and the author of two ISA textbooks, two chapters in other books, and over two dozen published articles. He also developed the first commercial safety system software modeling program. Gruhn has a BS in mechanical engineering from Illinois Institute of Technology, is a licensed professional engineer (PE) in Texas, and both a Certified Functional Safety Expert (CFSE) and an ISA-84 Safety Instrumented Systems Expert.

Speaking of Standards

With this year marking the 75th anniversary of ISA, many are looking back at the origins of its many significant standards. Standards such as ISA-84 for safety instrumented systems, ISA-95 for enterprise and control system integration, and ISA-99 for industrial cybersecurity owe their existence to the many ISA member volunteers willing to move the industry forward through standards work. Visit ISA.org to find out more about ISA standards history, the ISA standards committees looking for volunteers, and ways to become a member.

ISA GLOBAL CYBERSECURITY ALLIANCE

THE TIME IS NOW

Industrial Cybersecurity is a Global Imperative

It's time to join forces. We are stronger together.

The ISA Global Cybersecurity Alliance is an open, collaborative body. We welcome members of all kinds:

- end-user companies
- asset owners
- automation and control systems vendors
- cybersecurity technology vendors
- IT infrastructure vendors
- services providers
- system integrators
- industry organizations
- government agencies
- insurance companies
- other stakeholders

Founding Members:

Honeywell
Johnson Controls
Rockwell Automation
Life Is On Schneider Electric
NOZOMI NETWORKS
PAS
CLAROTY Clarity for OT Networks
WALLIX CYBERSECURITY SIMPLIFIED
xage SECURITY
MOCANA
BAYSHORE
radiflow Secure your Assets
senhasegura by MT4 TECHNOLOGY GROUP
INL Idaho National Laboratory
威努特 WINICSSEC
exida
munio SECURITY
tenable
DRAGOS
TiSafe
ae Solutions
tripwire
DIGITAL IMMUNITY STAY PRODUCTIVE, STAY SECURE
WisePlant Smart, Safe & Secure
MSI Mission Secure, Inc.
1898 & CO. PART OF BURNS & MCDONNELL
ACET SOLUTIONS
CYBEROWL
Nova Systems

Understanding the ISA/IEC 61511 Safety Instrumented Systems Certificate Program

The ISA/IEC 61511 Safety Instrumented Systems Certificate Program, which comprises three certificate exams, helps increase knowledge and awareness of the standard

By Melissa Landon, Automation.com

ISA and the Automation Standards Compliance Institute (ASCI) established the ISA/IEC 61511 Safety Instrumented Systems Certificate Program as part of an initiative to increase knowledge and awareness of the ISA/IEC 61511 standard. The program comprises three certificate exams: the ISA/IEC 61511 SIS Fundamentals Specialist, the ISA/IEC 61511 SIL Selection Specialist, and the ISA/IEC 61511 SIL Verification Specialist. These exams can also be referred to as certificates 1, 2, and 3.

Obtaining an ISA/IEC 61511 Safety Instrumented Systems Certificate

To get the certificate, one must successfully complete a designated training course, meet work experience prerequisites (for certificates 2 and 3), and pass a multiple-choice exam. Though no work experience documentation is required to take exam 1, an employment summary/supervisor verification document is required for certificate exams 2 and 3. Participants will receive continuing education units (CEUs) for the courses they take. Those who have all ISA/IEC 61511 certificates are considered ISA/IEC 61511 SIS Experts.

Course fees are determined by the length of the course and can be found at the requirements link at www.isa.org/isa84certificate. Each registration includes the course and exam fee.

Testing for the ISA/IEC 61511 Safety Instrumented Systems Certificate

Once the required courses are completed, applicants become eligible to take an exam. The exam must be completed within six months from the date the course is completed, and applicants must pass exam 1 before taking exams 2 and 3.

The ISA/IEC 61511 Safety Instrumented Systems Certificate Program exams are offered electronically through the Prometric global network of testing centers. The exams are not offered the day after completing the required course. Applicants who complete the program requirements will receive an email with an eligibility code. This code is used to review locations and schedule an appointment with Prometric: www.prometric.com/isa. Arrive at least 30 minutes early to the testing site and prepare to spend two hours taking the exam. Be sure to bring a government-issued photo ID with a signature.

Within 24 hours after the test, applicants will receive notification of whether they passed or failed. If a candidate does not pass the exam within the six-month window after the course and would like to receive the certificate, the applicant must register for the course and exam again and retake both.

Certificate 1
ISA/IEC 61511 SIS Fundamentals Specialist

Certificate 2
ISA/IEC 61511 SIL Selection Specialist

Certificate 3
ISA/IEC 61511 SIL Verification Specialist

ISA/IEC 61511 EXPERT

Do I need to renew my certificate?

You are not required to renew your ISA/IEC 61511 certificate; however, once obtained your certificate will only be considered current for three years. Click here to learn more about extending the current status of your certificate.

Displaying your ISA/IEC 61511 Safety Instrumented Systems Certificate

On your business card or resume, display your ISA/IEC 61511 certificate designation in an area distinctly separate from your name and certificate, licensure, and degree designations (e.g., CAP, PE, MBA).

When possible, include "Certificate" or "Certificate Holder" after your ISA/IEC 61511 designation listing (e.g., ISA/IEC 61511 SIL Selection Specialist Certificate Holder).

If you need another copy of your certificate, send a written request to ISA with your mailing address and $15. Once your payment is received, you will get the certificate in the mail.

ABOUT THE AUTHOR

Melissa Landon (mlandon@automation.com) is a content editor at Automation.com, a subsidiary of the International Society of Automation.

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 a 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

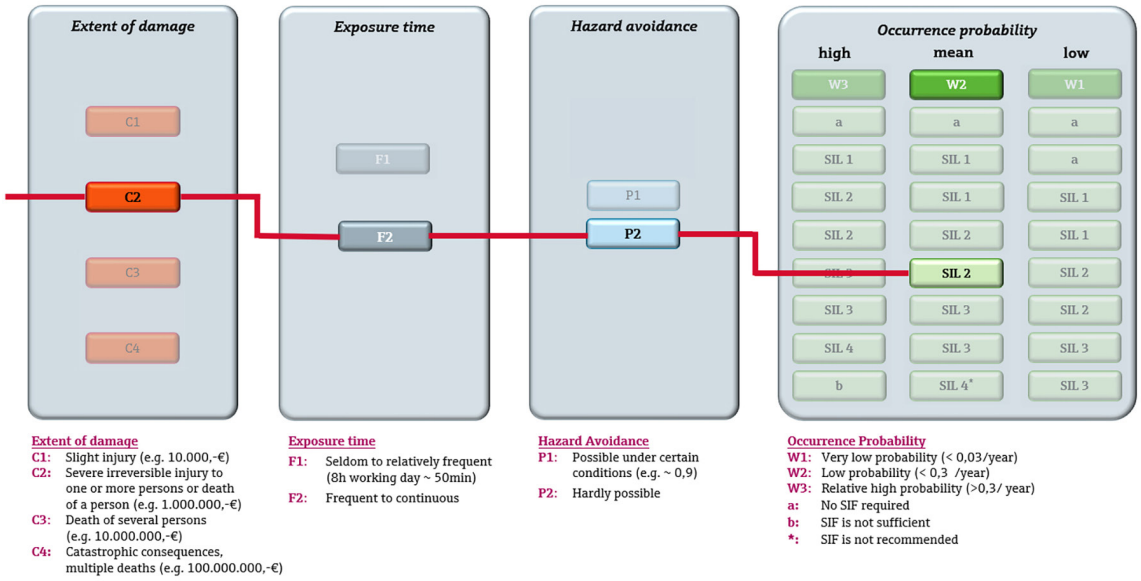


Figure 2. Example of a risk graph in accordance with IEC 61511-3 Annex E.

be 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 selection 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 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 wir-

ing, 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).

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

Figure 4. Proof testing options

Safety integrity level 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).

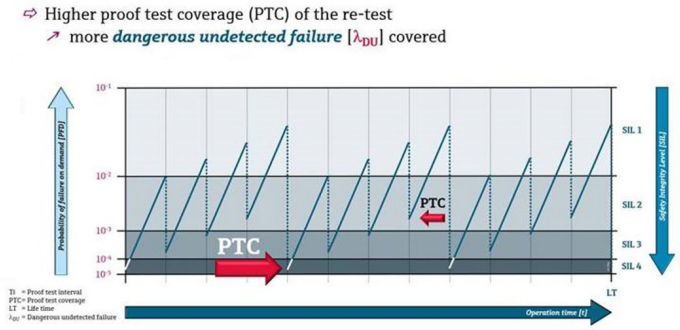
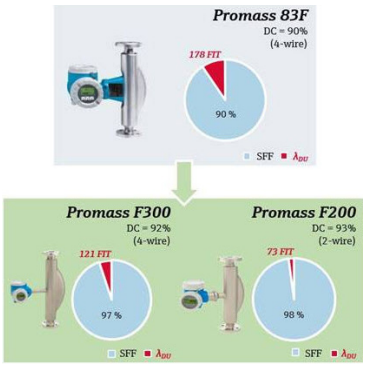


Figure 5. Higher proof test coverage (PTC) of the re-test reveal more dangerous undetected failures [λdu] are uncovered.

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).



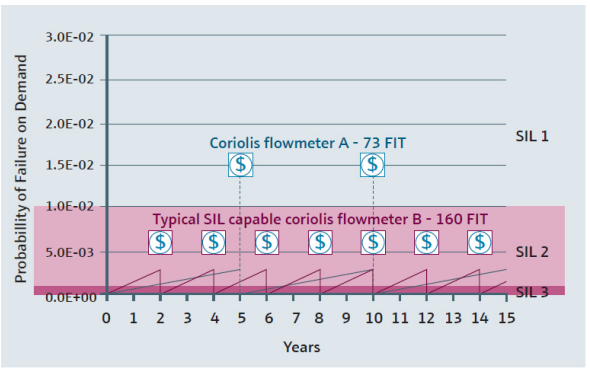


Figure 6. Flowmeters with a lower "dangerous undetected" (λdu) FIT and in-situ testing capabilities may allow one to extend the interval time needed for proof tests requiring the flowmeter to be removed from the process. In this example, all other things being equal, flowmeters with a 160 λdu FIT have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

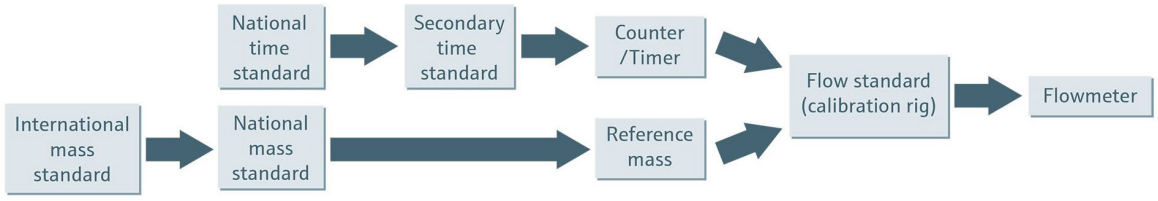


Figure 7. Example of a traceability chain for a mass flowmeter.

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.

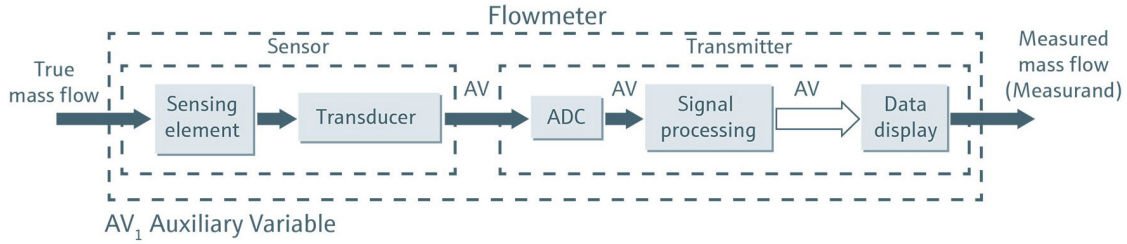


Figure 8. Basic components of a mass flowmeter. Source: BIPM.

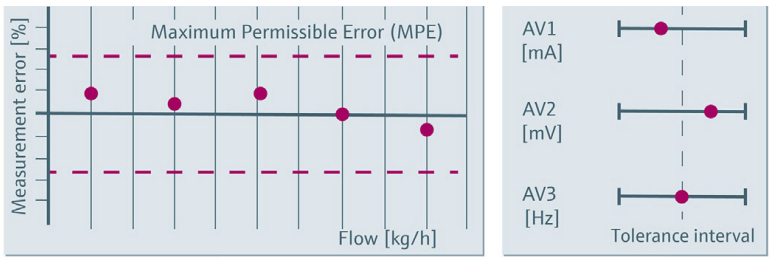


Figure 9. Verification concept: (a) the flowmeter is removed and the measurand (process value) is tested on a flow calibration rig. (b) auxiliary variables, such as mA and mV, are compared to reference values.

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 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.

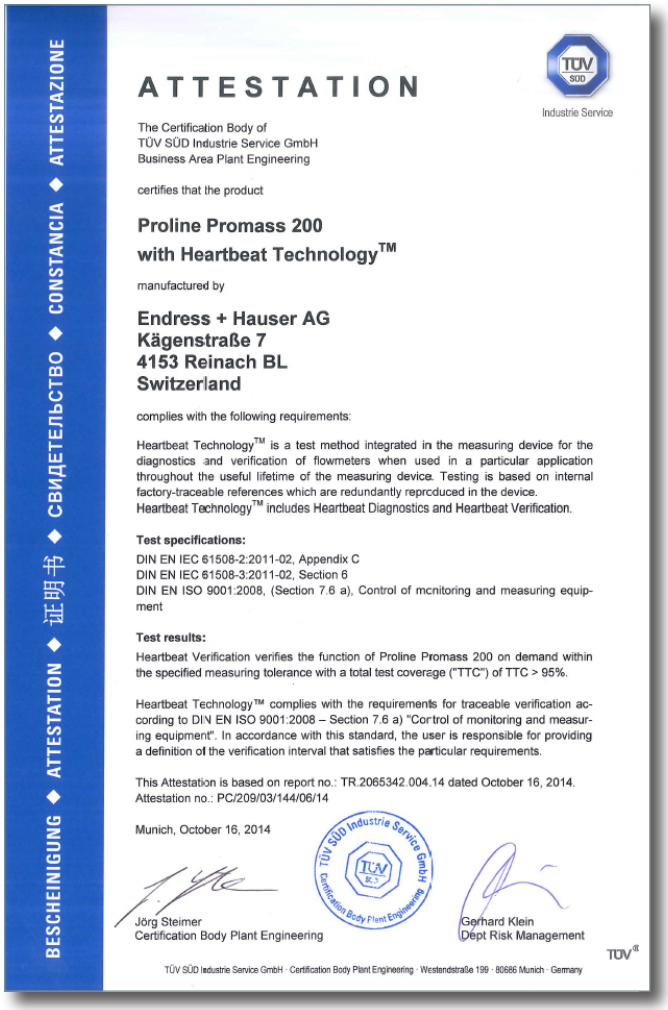
Redundancy of references is achieved differently depending upon measurement technology:

- 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 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



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.

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 10 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, Hedrick 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 participates 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.