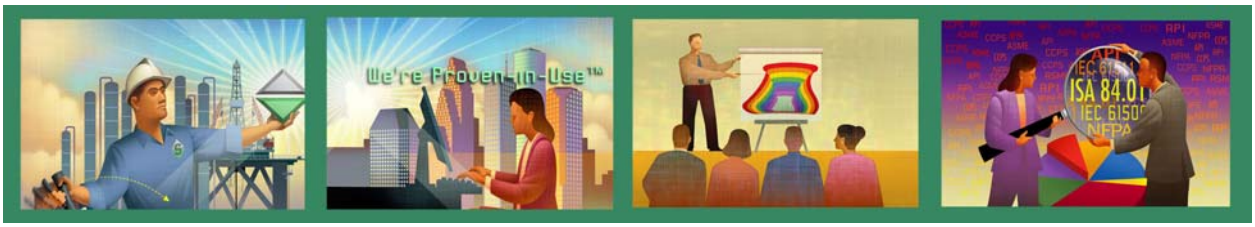


USER APPROVAL OF SAFETY INSTRUMENTED SYSTEM DEVICES

Angela E. Summers, Ph.D., P.E, President
Susan Wiley, Senior Consultant
SIS-TECH Solutions, LP

Process Plant Safety Symposium, 2006 Spring National Meeting, Orlando, Florida, April 26-27, 2006.
"Meet SIS 'User Approval' Mandates," Chemical Processing, May 2006.

Abstract

User approval is a simple process that supports design, engineering, configuration management, and management of change. User approval assesses manufacturer information and installed performance data to justify that a device is suitable for use in a safety instrumented system (SIS) application. The process supports configuration management and management of change activities by providing a means to determine whether a new or revised device is acceptable. This paper explains the concept of user approval as documented in ANSI/ISA 84.00.01-2004, ANSI/ISA TR84.00.04, and the Center for Chemical Process Safety book, Guidelines for Safe and Reliable Instrumented Protective Systems.

Introduction

This paper is distributed "as is." All warranties, either expressed or implied, are disclaimed as to quality, performance, or merchantability, whether expressed, implied or statutory, hidden defects, or fitness for any particular purpose. The author makes no representations about the suitability of the information in this paper for any purpose. Reader bears the entire risk relating to the use of this paper.

A paragraph similar to the above is contained in many end-user license agreements accepted during the installation of user software and in the hardware manufacturer's terms and conditions. The underlying concept is that the "user" of the product bears the risk associated with determining whether a product is fit for a particular purpose.

The manufacturer limits its liability associated with effects beyond its control, such as the operating environment. Other limitations are generally addressed in the installation and maintenance manual (or in the safety manual for safety instrumented system devices). Product manuals provide warnings concerning the installation, commissioning, maintenance, and testing requirements. These agreements, terms, and warnings establish the boundary for the manufacturer's claims. Deviation from the manufacturer's recommended practices generally invalidates all warranties, either expressed or implied.

No manufacturer's claim, third-party analysis, or certification report reduces the user's responsibility for determining the product is fit for purpose. This user responsibility was acknowledged in

ISA 84.01-1996, which used the term “user approved” as “hardware, software, procedures, etc., that the user has evaluated and determined to be acceptable for the application.”

The User Approval Process

A user approval process should be established to examine evidence of the suitability of devices for the application and operating environment. A device can be user approved and considered suitable for use when it can be demonstrated that the device meets the core attributes associated with its protection layer. The device boundary includes the hardware and software elements necessary for the device to perform its design intent.

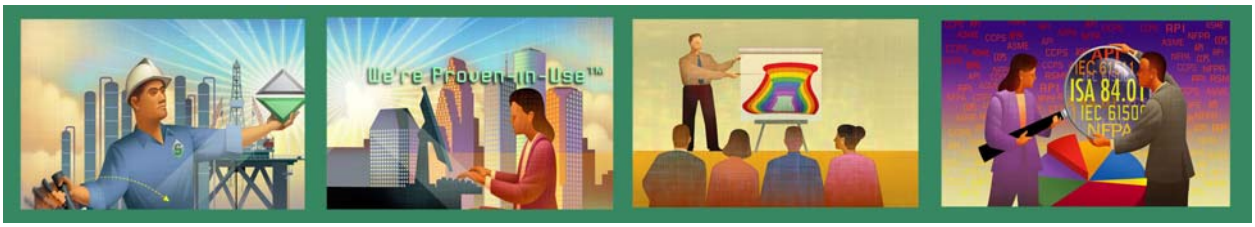
The user approval process examines the device using analysis and testing and demonstrated performance in the operating environment. The outputs of the process should be an approved manufacturer’s list and an installation, commissioning, and maintenance plan (e.g., the safety manual for the SIS) that outlines how the approved devices should be implemented.

User approval requires a close relationship between the manufacturer and the owner/operator as a product moves from early development through obsolescence. Technology evolution results in some devices moving rapidly toward obsolescence. For example, the lifespan of some programmable devices is less than 10 years due to the rapid development of computer technology, the increasing demand for interconnectivity, and a desire for uniform configuration tools. Such rapid evolution results in the manufacturer selling products that have some of the desired hardware and software features with a migration path for future upgrades. In some cases, significant changes in the product may be required to correct problems or to provide requested functionality.

The owner/operator should have a process to control the replacement of components in any way other than “like” for “like.” When the manufacturer offers a new version of an approved component or recommends a replacement, these new components should go through the user approval process. For new versions of approved products, this process can be simplified when the manufacturer provides documentation explaining changes to the products and highlights any configuration changes.

Configuration management can be challenging, but is essential to achieve the core attributes. Success requires that SIS product specialists serve as an information resource for the owner/operator. These SIS specialists should be highly familiar with SIS requirements, receive and review advisory notices and product information from the manufacturer, and make decisions regarding the addition or removal of devices from the approved manufacturer’s list. It is recommended that the SIS product specialist be independent of the project team seeking approval of the device.

Field performance and lessons learned in applying a device should be shared with the manufacturer to assist in future product development and in the dissemination of information regarding critical failures. Monitoring field performance and sharing failure reports with project and plant personnel is important for performance improvement.



Operating Environment

The operating environment can be identified by drawing an imaginary bubble around the device as installed in the process. The bubble establishes the boundary of the device. The operating environment may include a variety of items that affect device operation:

- External environmental conditions,
- Process operational conditions,
- Communications and interconnectivity,
- Human interfaces,
- Access security,
- Support systems, e.g. instrument air and electricity.

For Programmable Electronic (PE) logic solvers, the operating environment also covers the embedded software, the hardware architecture, application software, I/O configuration, communication to other systems, operator and engineering interfaces, and access security.

Analysis and Testing

Devices should be subjected to analysis and testing to evaluate the device's design, manufacture, and validation procedures, as well as the manufacturer's quality and change management systems. The rigor of the analysis and testing is related to the complexity of the device and the maturity of its technology. When completed, there should be a better understanding of how the device functions and fails. This analysis should consider the device boundary and should result in the following:

- Description of the analysis boundary.
- Identification of potential dangerous failures.
- Identification of means to detect dangerous failures by diagnostics or testing.
- Description of assumed diagnostic coverage factor and any user requirements necessary to achieve the diagnostic coverage, e.g., configuration requirements and the need for external diagnostics.
- Statement of the probability of safe and dangerous failures with any assumptions regarding maintenance activities and testing intervals.

Analysis and testing should also include evaluation of the device's conformance to applicable codes, standards, and practices. Meeting the area classification (e.g., hazardous environments) and following applicable electrical codes is important for all instrumented system applications. Devices that do not meet the area classification can become ignition sources should a loss of containment occur. For SIS, the requirements of IEC 61511 Clause 11.5 should be met. Guidance on complying with this clause is also provided in ANSI/ISA TR84.00.04 Annex L.

Manufacturers, who wish to advertise their products as safety products, analyze and test their devices for compliance with the intent of IEC 61508. An IEC 61508 evaluation may yield a "certification" if

the product is evaluated by a recognized certification body. A certified device can be labeled with an "SIL (Safety Integrity Level) Claim Limit." In the United States, certification to IEC 61508 is issued by Nationally Recognized Testing Laboratories (NRTL), such as those listed on the US-OSHA website (www.osha.gov). The OSHA website has a complete listing of NRTLs. Other countries establish certification requirements by policy or regulation acceptable certification bodies.

When a device is certified according to IEC 61508, the manufacturer supplies a safety manual providing the criteria for its implementation. Successful implementation of SIS devices often requires a specific configuration, the addition of external diagnostics, the provision for inspection and maintenance, mandated proof test intervals, and specific installation details. Deviation from the safety manual may invalidate the SIL Claim Limit.

It is important to note that IEC 61508 is a generic functional safety standard that applies to safety-related systems used in many different industry sectors, including process, rail, machinery, and medical. Since this standard applies to many sectors, there are devices that meet the requirements of IEC 61508, but are not sufficiently robust for the operating environment in many process industry facilities. A device developed for use on a manufacturing floor may not be appropriate for use in a refinery SIS.

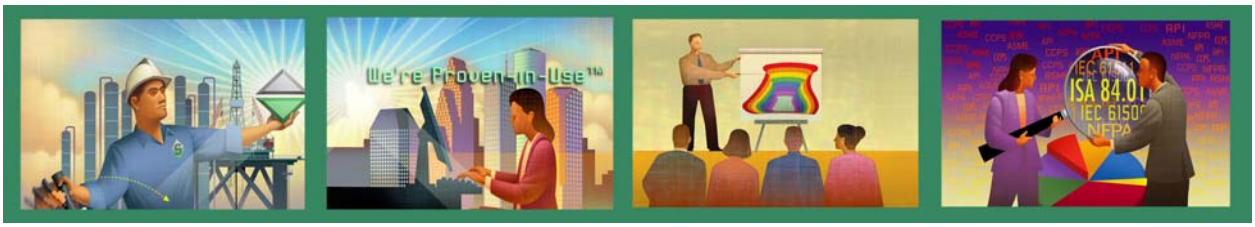
Manufacturers sometimes provide field performance reports based on an installed base at other owner/operator sites. More often, manufacturers supply analysis and testing results and documented predictive calculations of their product's probability to fail on demand and spurious trip rate based on the product's "shelf-state" design and manufacture. For any new technology, the analysis and testing is generally based on very limited field operating experience. Thus, the manufacturer evaluation represents the highest performance that can be expected from the device when it is implemented in accordance with its safety manual.

Field device and non-PE logic solver performance is generally dictated by the operating environment and the owner/operator's inspection and maintenance practices. For example, a sampling of data for pressure transmitters from various manufacturers show 600 to 800 year mean time to failure dangerous (MTTFD), however, owner/operator prior use data show a range of 75 to 200 year MTTFD.

Many important failure modes are excluded from the manufacturer's boundary. This includes the process connections, manner of installation, power supplies, and communication interfaces. Failures due to the operating environment can be significantly greater than failures due to device manufacture. Failures in the interfaces between the device, the process, and other protective systems should be considered when determining its suitability for addition to the approved manufacturer's list.

Some owner/operators develop installation details for each type of technology. These owner/operators then analyze the installation itself to ensure that the core attributes of a protective system are achieved, e.g., independence, functionality, integrity, reliability, auditability, access security, and management of change. This provides a consistent operator and maintenance interface and allows the analysis and testing for device approvals to be limited to the device and its ability to work within the existing approved installations.

For PE logic solvers, performance is generally dictated by how well the safety manual is followed, how recommended upgrades are executed, and whether the manufacturer's recommended operating environment is maintained. When implemented according to manufacturer's recommendations, PE logic



solvers tend to achieve the reported level of safety. This does not necessarily mean that the PE logic solver has the robustness to provide the trouble free service that may be desired. In general, PE logic solvers tend to fail-safe more frequently than reported by analysis. This is largely due to violation of the operating environment requirements or human error.

Prior Use History

In general, manufacturer failure rate data is 3 to 10 times better for programmable devices than the actual performance observed in the process industry. For mechanical devices, the ratio is 30 to 100 times better. Programmable electronic systems are not immune, with some certifications assuming diagnostics coverage factors that are simply not achievable using current practices. Because of the discrepancy between manufacturer and owner/operator environments, devices should be selected based on demonstrated history in a similar operating environment.

The intent of prior use is to gain an understanding of the device's failure modes so that the design and operating basis can take them into account. Previous operating experience provides valuable information for the selection of field devices, because it identifies how the operating environment degrades the theoretical performance claimed by the manufacturer. For some devices, especially field devices, evidence of successful operating experience in similar process applications is very important. In IEC 61508, this is called "proven-in-use;" while in IEC 61511, it is called "prior use."

There are specific requirements and limitations regarding the prior use evaluation in IEC 61511 Clauses 11.4 and 11.53 through 11.5.6. The requirements vary depending on the device type (sensor, logic solver, final element) and whether the device uses programmable elements. If the device is programmable, the requirements also vary dependent on whether fixed programmable language or limited variability language is used to configure the device. These requirements are further discussed in ISA TR84.00.04 Annex L.

For SIS, IEC 61511 requires devices be selected based on their expected performance in the operating environment. Maintenance records are a valuable information source. The plant maintenance tracking system can be used to flag devices that have repeatedly failed so that more detailed analysis can be performed. In general, it takes approximately three years of operating time to gain sufficient understanding of the failure modes of a field device. This operational time can be obtained in the actual or similar operating environment in process control, other non-SIS applications, or at other owner/operator sites.

Operational time can be gathered during alpha and beta testing where owner/operators work in close association with the manufacturer. Alpha testing is conducted to demonstrate the basic functionality of the device and general compatibility with the service. A successful alpha test leads to beta testing, which is usually conducted using multiple installations to gather information on the device failure modes in

a variety of operating environments. However, alpha and beta testing results are not sufficient for approving devices for SIS service.

Manufactures often provide references to other owner/operators who use their product. These references can often provide valuable insight into product application and use. In addition, the manufacturer user's group can provide valuable networking opportunities to gather information concerning product performance. The owner/operator may choose to rely on the manufacturer and other owner/operator's field experience or may choose to supplement this evidence with more direct experience. This may include bench testing and field trials in process control or low hazard services. Generally, the more unfamiliar or complex the technology is, the more time should be spent understanding how it works and how it fails.

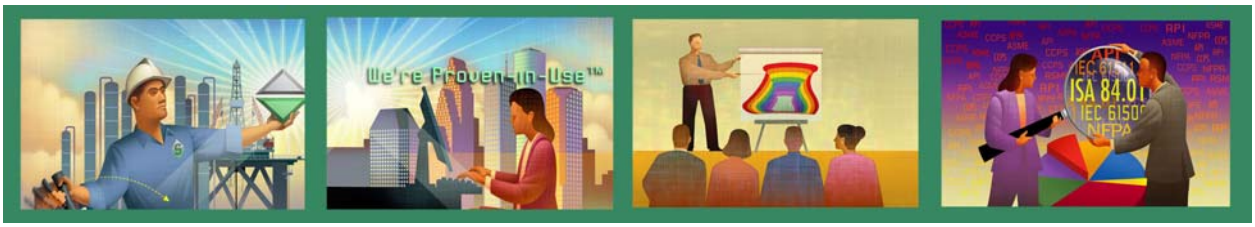
Proven performance takes on special significance for SIS, because most operate as dormant systems that only take action when a process demand occurs. In contrast, control system devices are expected to operate frequently, if not continuously, so failures in control system are rapidly detected. If these failures cannot be managed by the control system or operator, an independent SIS is often implemented to mitigate any unacceptable process risk.

One of the strongest arguments for separation of the SIS and the control system is the common practice of using the latest technology in control applications. Many owner/operators who strive to use the newest control technology often find that the products are not as well developed as originally thought. New control system implementation can turn into an unplanned product development project. While necessary for production or quality reasons, this can be a hazardous practice for SIS. Proven operating history cannot be underestimated.

Summary

User approval is an important aspect of complying with ANSI/ISA 84.00.01-2004. User approval relies of predictive evidence, such as analysis and testing reports, balanced with field operating history. While some manufacturers are now providing devices that are "certified for use" in safety instrumented systems (SIS), these devices are relatively limited in their range of application and technology. Many are not field proven and some are not demonstrating the robustness necessary to survive a chemical plant environment. Within an IEC 61508 analysis, an unreal operating environment is often assumed: one that does not include the process impact, ambient conditions, stress, manufacturing defects, software errors, installation issues, electrical disturbances, instrument air or other support system quality problems, etc.

Consequently, owner/operators in the process sector should rely heavily upon operating experience for selection of devices for SIS, especially for those devices installed in the process environment. User approval seeks to get the proper balance of analysis/testing information and field experience. The amount of information or experience required and the degree of rigor associated with their evaluation may vary, depending on the nature of the device and the required safety integrity level. The key point to the user approval process is to establish sufficient evidence to justify that the device can and does achieve the required performance in the intended operating environment.



References

Instrumentation, Systems, and Automation Society (ISA), ANSI/ISA S84.01-1996, "Application of Safety Instrumented Systems (SIS) for the Process Industry," Research Triangle Park, NC (1996)

Occupational, Safety and Health Administration (OSHA), "Process Safety Management of Highly Hazardous Chemicals; Explosives and Blasting Agents, 29 CFR Part 1910." Federal Register 57,36, Washington, DC (1992).

International Electrotechnical Commission (IEC), IEC 61508, Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems, Parts 1-7, Geneva, Switzerland (1999-2001).

International Electrotechnical Commission (IEC), IEC 61511, Functional Safety: Safety Instrumented Systems for the Process Sector, Geneva, Switzerland (2003).

12621 Featherwood Drive, Suite 120
Houston, Texas 77034