Is your existing Safety Instrumented System up to current standards?

Process safety is a major concern to anyone who works in a process facility. An estimated 25,000 facilities covered by the Occupational Safety and Health Administration (OSHA) Process Safety Management of Highly Hazardous Chemicals regulation will most likely have safety instrumented systems (SIS), also known as emergency shutdown systems.

Throughout the decades, process industries have used different forms of safety based on what was available in the market. Relays have been used in safety applications since the 1930s. Solid-state systems, that do not use software, were developed to replace relays and have been used in safety applications since the 1970s. Programmable Logic Controllers (PLCs) that do use software, were developed to replace relays and have also been used in safety applications since the 1970s.

Guidelines and standards for the design and implementation of safety systems have been in place in a variety of industries since the 1990s. Many things change, even standards. Yet many other things do not change – or change very little – such as industrial processes that have been running for decades. So what are people expected to do with safety systems installed prior to current standards? Are previous designs automatically assumed to be acceptable, or must all older systems be ripped out and replaced? This is one topic that has its fair share of misinformation and scare tactics, and what will be explored in this white paper.
The “Grandfather clause”

The first edition of ISA 84 (“Application of Safety Instrumented Systems for the Process Industries”) was released in 1996. There are two fundamental concepts in the standard: 1) a lifecycle, and 2) safety integrity levels (SIL). The ‘grandfather clause,’ which came from the OSHA Process Safety Management regulation in 1992, was in the first edition of ISA 84. The second edition of ISA 84, which is actually IEC 61511, was released in 2004. The only difference between IEC 61511 and ISA 84 is that ISA 84 contains the grandfather clause (1.y).

Many people have questions about existing systems, which is what the grandfather clause is intended to cover. Clause 1.y states, “For existing SIS designed and constructed in accordance with codes, standards, or practices, prior to the issue of this standard (for example, ANSI/ISA-84.01-1996), the owner/operator shall determine that the equipment is designed, maintained, inspected, tested, and operating in a safe manner.”

People tend to have more questions after reading the grandfather clause than they did before reading it. For example, just what is a “safe manner?” How safe is safe enough? How does one determine and document these concepts? The OSHA regulation provides no real guidance and standards are not written or intended to teach such concepts.

The ISA 84 committee realized that people needed additional guidance to understand the grandfather clause. Within the last 15 years, the committee has published seven technical reports covering various issues, such as system modeling, burner management systems, fire & gas systems, security, etc. Technical Report 84.00.04 is titled “Guidelines for the Implementation of ANSI/ISA-84.00.01-2004 (IEC 61511 Mod)”. Published in 2005, the first edition of this report contains 18 annexes on a variety of subjects and includes an annex 17 pages long covering the grandfather clause.

How can I determine if my existing system is acceptable?

There are two fundamental steps to determine if your existing systems are acceptable. Step one, identify all safety instrumented functions and determine what level of performance they need to meet - that is, determine the required SIL of each safety instrumented function (SIF). Step two, analyze/model/calculate the performance of the actual hardware to see if it will meet the required performance.

To help address step one, Table 1 shows the performance requirements for the different SILs. Part 3 of the standard summarizes several different techniques used around the world for determining SIL, including the risk matrix, risk graph, and layer of protection analysis.

<table>
<thead>
<tr>
<th>Safety Integrity Level</th>
<th>Probability of Failure on Demand (PFD)</th>
<th>Risk Reduction Factor (1/PFD)</th>
<th>Safety Availability (1-PFD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>≥ .00001 to &lt; .0001</td>
<td>&gt; 10,000 to ≤ 100,000</td>
<td>&gt; 99.99 to ≤ 99.999</td>
</tr>
<tr>
<td>3</td>
<td>≥ .0001 to &lt; .001</td>
<td>&gt; 1,000 to ≤ 10,000</td>
<td>&gt; 99.9 to ≤ 99.9</td>
</tr>
<tr>
<td>2</td>
<td>≥ .001 to &lt; .01</td>
<td>&gt; 100 to ≤ 1,000</td>
<td>&gt; 99 to ≤ 99.9</td>
</tr>
<tr>
<td>1</td>
<td>≥ .01 to &lt; .1</td>
<td>&gt; 10 to ≤ 100</td>
<td>&gt; 90 to ≤ 99</td>
</tr>
</tbody>
</table>

Table 1: Safety Integrity Levels
(LOPA). While Part 3 of the standard is over 60 pages, it is worth noting a statement made in the introduction, “The information provided is not of sufficient detail to implement any of these approaches.”

According to the U.S. process safety management regulation, process hazard analyses must be reviewed every five years. Such review cycles are an ideal time to formally identify all safety functions and determine their required performance targets.

To address the second step, many standards, technical reports, and books exist that describe how to analyze the performance of the hardware to see if it will meet the required performance. For example, Clause 11.9 of the standard requires the performance of a function be verified by a calculation. The standard also includes fault tolerant tables to show what configurations of logic solvers and field devices are suitable for different integrity levels. Table 2 shows examples of technologies and configurations that can meet different integrity levels.

For example, let’s imagine that your team performs a SIL selection/determination study and determines that a function needs to meet SIL 1. The function and its field devices are separate from the control system. The safety hardware consists of a pressure switch, wired to a relay logic panel, which is then wired to a single solenoid operated valve. All of the components are tested on a yearly basis. Such hardware would meet SIL 1 performance levels and no changes would be necessary.

However, let’s say the function needed to meet SIL 2 and consists of a single standard transmitter, wired to a general purpose PLC, which is then wired to a single solenoid operated valve. Such a configuration would not meet SIL 2 performance requirements, nor the fault tolerance table requirements, and a change would be necessary. Note: there are exceptions to every rule, but those are beyond the scope of this paper.

One major oil company reviewed over 5,000 existing safety functions. Almost half were over-designed, almost half were fine, but approximately 4% were found to be under-designed and in need of change.
Does using certified devices mean you will now comply?

There is a growing – and disturbing – trend for users to specify that all field devices be SIL rated and be third-party certified, usually to SIL 2 requirements. Vendors may also be using scare tactics to get users to replace older non-certified devices with newer certified ones. The standards are quite clear that devices do not require certification. They have always permitted the use of devices based on “proven-in-use” criteria. However, many end users find thoroughly documenting the proven-in-use criteria to be difficult. Be that as it may, the use of certified devices, which do offer certain benefits, is not the magic answer and using such devices alone does not mean a company will be in compliance with the standards.

Is your logic solver that was never certified, or certified to the first edition of IEC 61508, no longer suitable?

Triplicated safety PLCs have been implemented since the 1980s, before there were safety standards and third-party certifications. Safety systems started to receive certification in the 1990s based on German standards, which were the only thing available at that time. IEC 61508 was released in stages, between 1998 and 2000, and many vendors had their systems certified against that standard. (There are different certification agencies that compete with each other, and one can make arguments that they are not all equal.)

The second edition of IEC 61508 was released in 2010, and there are subtle differences between the two versions. Some vendors imply that systems designed prior to the standards, or those certified against the first version of IEC 61508, are somehow no longer suitable. This would also have to include systems that they themselves provided. (This is little more than scare tactics intended instill FUD: fear, uncertainty, and doubt to generate sales.)

The use of certified devices is not the magic answer, and using such devices alone does not mean a company will be in compliance with the standards.

If you put in the best triplicated safety system available at the time, do you really believe it to somehow be deficient now? If you have a 20-year old high-end stereo system still working properly, do you really feel the need to replace it? If you have a television from 2008 that still meets your requirements, do you really feel the need to replace it?
Other factors to consider

Other items to consider for existing systems consist of, but are not limited to, the following:

1. **Have existing safety functions been correlated to specific hazards identified during prior hazard analyses?** Process hazards analyses are performed to identify potential hazardous events. Some events may be prevented or mitigated through the use of instrumentation. Is there documentation to show that each safety function identified or suggested in the analyses are, in fact, implemented in the safety system? Are there any safety functions implemented in the system that cannot be correlated back to the hazard analyses? And if so, why?

2. **Are safety functions (field devices and logic) separate and independent of the control system?** The first edition of the ISA 84 standard stated that the logic solver and sensors for safety shall be separate from the logic and sensors of the control system. The second edition of the standard is not quite so “black and white” any more, but it is standard practice in many industries to have separate sensors and logic for safety. Possible exceptions for combining or sharing devices – a practice which must be approved and accepted by the user – would be low risk applications with very small I/O counts in packaged skid systems for example. Such combined applications would usually be managed as a safety system.

3. **Are manual proof test intervals adequate to meet the required performance?** All safety devices must fall within a mechanical integrity program and must be periodically tested. Manual proof test intervals are part of probability of failure on demand calculations that are required to verify system performance. Are proof tests actually being performed? Are they being performed at a frequency/interval that can be documented with calculations and shown to be adequate?

4. **Are there written proof test procedures for all safety functions?** Manual proof test procedures are expected to be written and task specific. If they are not, technicians will make them up on their own. This was a serious problem for one user and was a contributing factor to a serious accident where testing procedures actually damaged the instrumentation.

5. **Are failure rates determined from maintenance records?** Performance calculations are based on failure rates, automatic diagnostic coverage, manual test intervals, repair times, and a variety of other factors. There are many different sources of failure rate data, some definitely better than others. If a user did not have maintenance records to base failure rates on, they would have had to rely on other published sources of data. Users are expected to periodically compare assumed data with actual data based on field experience. If actual failure rates differ significantly from numbers assumed during initial calculations, it would indicate either the design needs to change, or manual test intervals need to change (and changing either may be very difficult).

6. **Are management of change procedures in place and being followed?** Safety systems invariably need to be changed at some point. Accidents have occurred because even simple changes were not done correctly, and improper documentation and review were to blame.
Conclusion

Process safety remains a concern, with safety instrumented systems standards constantly changing. Those individuals charged with maintaining the safety of the facility must not only familiarize themselves with the latest standards, but with so-called “grandfather clauses” such as in ISA 84. Process safety not only involves a comprehensive understanding of these standards, but how they correlate to age old industrial processes that have not changed.

Determining if your current safety instrumented systems meet current standards will require a review of existing designs. Those charged with process safety should also know that certification does not necessarily mean equipment standards are met.

Ultimately, your safety instrumented systems supplier can help you determine if your current equipment meets the standards in place. By working with a third-party provider specializing in process safety, you can select the solution that can meet your requirements based on cost, safety integrity level, performance, and availability.

Rockwell Automation® has a broad portfolio of safety offerings, including consultancy services to assist in selecting the scalable solution that will satisfy cost, safety integrity level, performance, and availability requirements.

We offer an excellent approach to industrial control that integrates sequential, process, drive and motion functionality in a single platform. With products that meet SIL 1-3 requirements through sophisticated diagnostics and high levels of reliability, our controllers set new standards for reliability and availability, increasing safety and productivity while reducing downtime, nuisance trips, and lifecycle costs.

Our consultants will work with your safety decision makers to determine the Rockwell Automation® process safety solution that will not only provide a secure environment for the workforce, but help ensure that all standards are met and equipment is operating under the optimal conditions.

For more information on process safety, please visit: http://www.rockwellautomation.com/rockwellautomation/products-technologies/safety-technology/process.page?

References

1. Application of Safety Instrumented Systems for the Process Industries


www.rockwellautomation.com