CHEMICAL PROCESSING

ENDEAVOR BUSINESS MEDIA

Safety Instrumented Systems

May 11, 2021

Right-Size Your Safety Instrumented Systems

Consider the cost versus value of adopting a higher safety integrity level

By Tetsu Ishidu, Yokogawa Electric Corp.

When solving a design challenge, most engineers like to build in a safety factor. For example, if structural calculations suggest ⅜-in. bolts will suffice for an application, designers often will specify ½-in. bolts to be "on the safe side." Here, the change incurs only slight added expense. However, in many cases, providing an extra margin can create significant costs. For instance, increasing the horsepower rating of a motor driving a pump by 20% means a more expensive motor but, worse, the cost of the extra electricity to run it over its lifetime.

Let's extend this thought progression into another area: process safety. Is it possible to overdesign a safety instrumented system (SIS) or individual safety instrumented function (SIF)? Is it desirable to do so to build in the extra cushion of protection? Overdesign certainly is possible. However, engineers should carefully consider the cost, while ensuring provision of the required degree of safety.

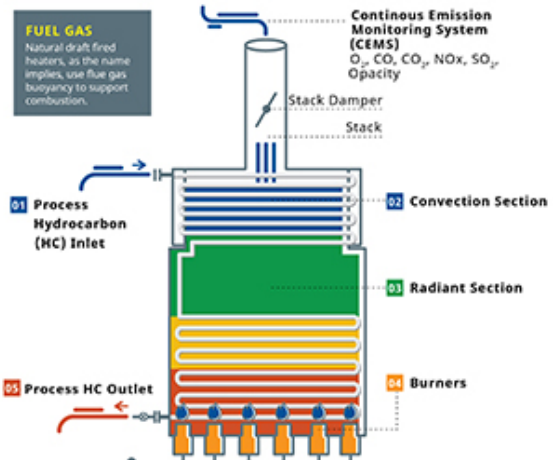
This article will not get into evaluating potential safety hazards or designing safety systems, which are extensively covered elsewhere. Instead, we will discuss ways of interpreting and implementing the findings of these evaluations.

Before that, though, let's go over some basics of the design methodology, as detailed in IEC standard 61511. A process hazards analysis (PHA) leads to assignment of a particular SIF to a specific hazard, such as an overpressure incident in a given vessel. The criticality of an SIF, which depends on the likelihood or frequency of the incident occurring, is then multiplied by its degree of severity, e.g., a small chemical spill versus a fire or explosion, to determine the safety integrity level (SIL) or risk reduction factor needed for the SIF.

Because no two chemical processing plants are identical, specific analyses invariably differ from site to site. However, we can draw some insights by looking at types of installations that are fairly common — the fire-and-gas (F&G) detection systems and burner management systems (BMSs) associated with boilers and fired heaters. These systems require evaluation in the same way as any other equipment in a facility, with SIL values assigned. Due to their widespread application, they have been evaluated countless times under many different circumstances. So, the questions become: what is the appropriate SIL value and how should a facility respond?

Burner Management SIL

A BMS must ensure the fire is burning in a controlled and efficient manner (Figure 1). Of first concern is that combustion actually is taking place, so the fuel gas is not simply accumulating in a large explosive cloud. If the flame is lost, the BMS must cut off fuel flow immediately. It also must analyze the combustion to ensure the fuel-to-air mixture is correct. There are more subtle functions as well but these two are the most important. In many plant environments, analysis of BMS SIFs calls for SIL-2 protection.



Burner Management System

Figure 1. This requires evaluation just like any other safety system in a plant.

The question some plants struggle with relates to the SIL value. Is SIL-2 sufficient or should the value be higher? In rare cases, the PHA of the BMS does indeed call for SIL-3 based on the severity of a potential incident. Often though, the decision to build to SIL-3 rather than SIL-2 stems from a motivation to err on the safe side or a desire to have everything in a plant at the same SIL. However, this can quickly result in excess cost and complexity.

To understand how all this works, it is useful to consider the elements of an SIF and how equipment and systems get their SIL rating.

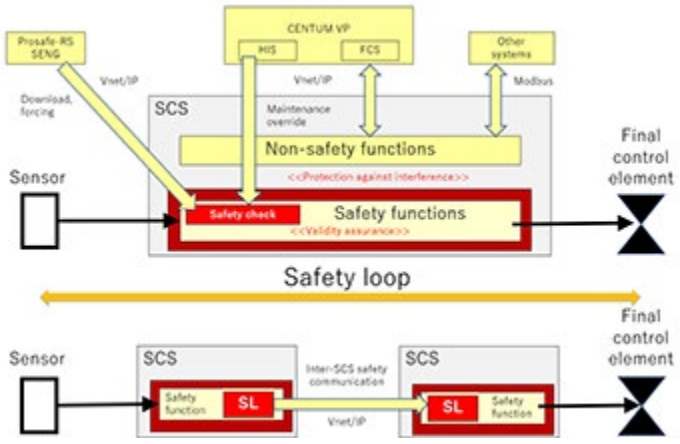
An SIF consists of three parts: a sensor, logic solver and final control element (FCE) (Figure 2). For a BMS, the sensor might be a flame scanner to verify that combustion actually is occurring. The sensor sends its measurement to a logic solver, which compares the value against its internal programming. If the value falls below the setpoint, the logic solver triggers the FCE, in this case, closing a valve to shut off the fuel supply.

A safety-certified instrument, such as a flame scanner, must pass an in-depth analysis of its design and construction to determine all the ways it could malfunction or fail. By providing sufficient controls or redundancies, the device receives a low probability of failure on demand (PFD) value that is translated into the SIL

classification — the lower the PFD, the higher the SIL. (Strictly speaking, a device receives a PFD value that places it into one of the SIL ranges, not an SIL rating. However, a transmitter with a PFD of 1 in 500 commonly is characterized as “SIL-2 rated.”) The same treatment applies to logic solvers and FCEs.

The cost of certification combined with the specialized manufacturing and testing requirements of safety instruments make for premium pricing for anything with an SIL rating; higher levels increase the price, often more than proportionally.

Few systems depend on a discrete three-piece SIF. The logic solver for a BMS or F&G system typically is its own safety-rated programmable-logic-controller-based system (Figure 3) — with inputs and outputs for multiple sensors and FCEs, all connected to a central processor running certified software. It, like the other elements, has its own SIL rating, which, when evaluated with all the supporting elements, yields an SIL rating for the complete installation.



Safety Instrumented Function

Figure 2. A safety loop always must include a sensor, logic solver and final control element to bring the process to a safe state.

General SIL Selection

While there hasn’t been a hard-statistical study, Yokogawa’s engineers who have consulted at production sites shared the following observations on general SIL selections:

- process emergency shutdown (ESD) system, SIL-3;
- process F&G system, SIL-2/SIL-3;
- plant utilities ESD system, SIL-2; and
- plant utilities BMS, SIL-2.

Naturally, exceptions exist based on the processes and products involved. However, these observations apply widely throughout the chemical industry. This raises questions such as: How many facilities need an SIL rating higher than SIL-2 for anything outside of the main process ESD? Without a clear hazard evaluation legitimately calling for the extra level of protection, does a BMS or F&G system ever need more than SIL-2?

When answering such questions, safety specialists point to two important truths:

1. Any hazard could occur at any time. There is no hazard that cannot happen.

2. Any component of a safety system could fail at any time. Nothing is 100% reliable in every situation.

These points underscore that you should take nothing for granted — that's why we have safety systems in the first place. We cannot eliminate risk, we can only reduce it to an acceptable level. However, there's no need to reduce it more than necessary.

Highest Common Denominator

Real-world plants like to avoid complications wherever possible. So, some managers and engineers ask if working to multiple SIL ratings is required or desirable. They wonder if having some part of the plant at SIL-4 with its PFD of 1 in 10,000 is necessary, and whether scaling back to SIL-2 really provides that much in savings? Adopting SIL-3 for everything seems a simpler solution.

Using SIL-3 or SIL-4 instead of SIL-2 certainly increases the amount of protection — but to what end? SIL-2 offers a risk-reduction factor of between 100 and 1,000. Even at the lowest value, a SIL-2 system will perform its task correctly 99 times out of 100, statistically speaking. Moving to SIL-3 decreases the PFD by a factor of ten but likely at least doubles the cost for the hardware and commissioning alone compared to SIL-2.

Moreover, maintaining a higher rating requires more rigorous proof-testing and verification routines. Increasing the SIL to be on the safe side always imposes extra cost and other demands. So, you never should select a higher SIL without careful analysis of the total lifecycle cost. Of course, you should use a higher rating where a risk analysis indicates that it truly is needed.

Safety-Rated Control System
Figure 3. Controllers such as Yokogawa's ProSafe RS can support complex safety functions with multiple sensors and final control elements.

One more consideration is the availability of the best system selection from the plant's chosen safety partner. Implementing a higher-rated system than necessary simply because of lack of better choices in the particular vendor's product line is not optimal. The probability that fewer transmitters and final control elements are available to meet this higher requirement compounds the difficulty. Companies that choose to standardize on a higher rating for some degree of convenience frequently find it costlier than first envisioned.

The desire for standardization presupposes that the systems for the respective SIL ratings differ and, therefore, create training problems because technicians must learn multiple approaches. However, that is not always the case. Some safety controller platforms are indistinguishable from each other in spite of supporting

different SIL ratings. Operator graphics, programming code, etc., do not need to change — negating a key driver for standardizing on one SIL rating for an entire process plant or facility.

Most facilities pose a mix of safety requirements and, thus, need safety systems in different SIL-ratings.

Base Study 2: Site-Wide Re-Evaluation

An agricultural chemical producer was considering a site-wide safety system upgrade at one of its decades-old locations. The first step was a re-evaluation of the existing PHAs for each of the seven production units to determine if the working assumptions still were valid. This analysis yielded a variety of results, with most of the plant's units and utilities calling for SIL-2 protection but several organic-solvent-based production lines needing SIL-3.

The intention was to standardize on one SIL for the entire site. This meant SIL-3, even though it was far too high a standard to apply everywhere. So, the company checked whether applying SIL-3 across the rest of the plant was practical.

The answer was yes, at least theoretically. However, studying the practical implications convinced the company otherwise. The costs connected with implementing SIL-3 rather than SIL-2 for more than half the systems on the site proved to be more than the budget could handle. Not only was the cost of the controller hardware alone more than double, but far more of the existing safety transmitters and FCEs would need upgrading, including many that were allowable under proven-in-use evaluation sufficient for SIL-2.

One suggestion to upgrade just the controllers proved pointless because it simply would add cost without achieving any improvement in SIL rating. Based on the equipment provided by its selected vendor, no operational differences effectively existed between the SIL-2 and SIL-3 controllers, which negated much of the motivation for standardizing in the first place. Both platforms used the same setup and programming methods, so accommodating the different SILs was easy. The plant decided to use the appropriate SIL for each safety system.

Protection Without Excess

Chemical plants and refineries must have appropriate safety systems in place, following the standards and practices outlined in IEC 61511. This is not an area where a company should cut corners to reduce cost — but neither is it one where excess is necessary. Safety is costly to install and manage, so overbuilding offers no advantage.

At one time, the systems designed for SIL-2 and SIL-3 may have differed enough to drive a desire to standardize on just one, even if it meant increased costs. Now, though, the differences between some vendors' controllers for SIL- 2 and SIL-3 are indistinguishable to technicians and operators, which provides companies with substantial savings for SISs applied to BMS and F&G systems as well as to ESD systems for plant utilities and non-hazardous processes. SIL-3, where necessary, should be deployed but far more opportunities exist for SIL-2 than many plants may realize.

TETSU ISHIDU is an SIS product manager for Yokogawa Electric Corporation, Tokyo. Email him at Tetsu.Ishidu@yokogawa.com.

View post:
Right-Size Your Safety Instrumented Systems | Chemical Processing