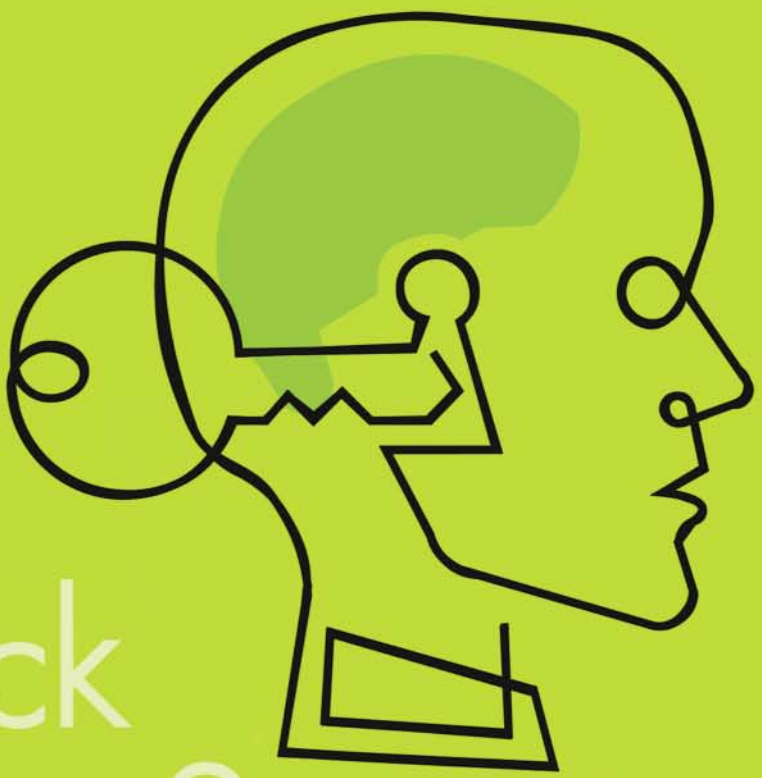
WWW.CONTROLMAG.COM

AUGUST/2003

CONTROL

FOR THE PROCESS INDUSTRIES



Unlock Plant Secrets

MANAGE ENGINEERING AND OPERATIONS KNOWLEDGE TO HANDLE ABNORMAL SITUATIONS

PutmanMedia

SIF: An S-Word Worth Knowing

Salary Survey: Part II

Batch Techniques Benefit Continuous

THE SAFETY INSTRUMENTED FUNCTION
AN S-WORD WORTH KNOWING

Understand the SIF to Control Confusion, Complexity, and Cost of Safety Instrumented Systems. By Bill Mostia Jr., PE

The term "safety instrumented function" or SIF is becoming common in the world of safety instrumented systems (SISs). It is one of the increasing number of S-words—SIS, SIL, SRS, SLC, etc.—that are coming into our safety system terminology.

The definition of a SIF as provided in IEC standard 61511, "Functional safety: Safety Instrumented Systems for the process industry sector," leaves a bit to be desired as a practical definition, and the application of the term leaves many people confused.

IEC standard 61511 defines a safety instrumented function as a "safety function with a specified safety integrity level which is necessary to achieve functional safety. A safety instrumented function can be either a safety instrumented protection function or a safety instrumented control function."

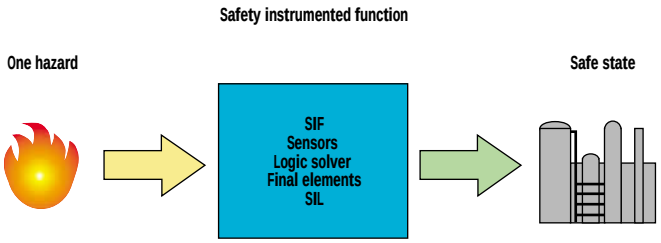
A safety function is further defined in 61511 as a "function to be implemented by a SIS, other technology safety-related system, or external risk reduction facilities, which is intended to achieve or maintain a safe state for the process, with respect to a specific hazardous event." The standard 61511, however, uses the terms SIS and SIF somewhat interchangeably in places.

From this definition we can also see that there are two types of safety instrumented functions. The first is a safety instrumented protection function, which is a safety instrumented function operating in the demand mode. The second is a safety instrumented control function, which is a safety instrument function operating in the continuous mode.

Let us look at some of other definitions of SIF that may make things a bit more clear. In their book, *Safety Integrity*

FIGURE 1.

THE CRITICAL LINK



A SAFETY INSTRUMENTED FUNCTION (SIF) DETECTS A SPECIFIC HAZARD AND BRINGS THE PROCESS TO A SAFE STATE.

TABLE I.

ANATOMY OF A SAFETY INSTRUMENTED FUNCTION

Property	Description
Hazard	A single hazard and associated risk (consequence and pre-safeguard frequencies of initiating causes of the hazard).
Mode of operation	Demand or continuous.
Detection	Sensors must be able to specifically detect the hazard and provide this information to the logic solver.
Decision	A logic solver must have the logic to automatically decide when to act when the hazard is present and activate the final elements.
Action	Final elements must have the ability to bring the process to a safe state or provide adequate hazard mitigation for the identified hazard.
Safety integrity level (SIL)	The amount of defined risk reduction to be provided by the SIF; also can be seen as the level of dependability of the SIF.
Safe state	A safe or mitigated state.
Response time	Must have adequate time to detect, decide, and take action, and for the action to achieve the safe or mitigated state.
Proof-test interval	Proof-test frequency(s) for the SIF or its components.
Safety instrumented system (SIS)	One or more SIFs make up a SIS.
Spurious trip rate	Acceptable rate of spurious trips.

Level Selection, Systematic Methods Including Layer of Protection Analysis, Ed Marszal, PE, and Eric Scharpf describe it as "a function that is a single set of actions that protects against a single specific hazard. The term SIF often refers to the equipment that carries out the single set of actions in response to the single hazard, as well as to the particular set of actions itself."

From these sources we might define the SIF as an identified safety function that provides a defined level of risk reduction or safety integrity level (SIL) for a specific hazard by automatic action using instrumentation. A SIF is made up of sensors, logic solver, and final elements that act in concert to detect a hazard and bring the process to a safe state.

Another view of a SIF is that of an instrument safety loop that performs a safety function which provides a defined level of protection (SIL) against a specific hazard by automatic means and which brings the process to a safe state.

What a SIF Is

Both these definitions define the key properties of a SIF as illustrated in Figure 1. Its basic properties are outlined in Table I. Some examples of SIFs are:

- High pressure in a vessel opens a vent valve: The specific hazard is overpressure of the vessel. The high pressure is detected by a pressure-sensing instrument, and logic (PLC, relay, hardwired, etc.) opens a vent valve, bringing the system to a safe state.
- High temperature in a furnace that can cause tube rupture shuts off firing to furnace: The specific hazard is tube rupture. Instrumentation automatically causes a main fuel trip that removes the heat, bringing the system to a safe state.
- Flame-out in an incinerator that can lead to a release of toxic gas causes process gas feed to be shut off: The specific hazard is a flame-out. The automatic instrument protective action is to close process gas feed to the incinerator, which stops any toxic gas release bringing the system to a safe state.
- Flame-out in an incinerator that could cause fuel gas accumulation and explosion causes a main fuel gas trip: The specific hazard is a flame-out. The automatic instrument protection action is a main fuel gas trip, which cuts off the fuel and prevents fuel gas accumulation, bringing the system to a safe state.

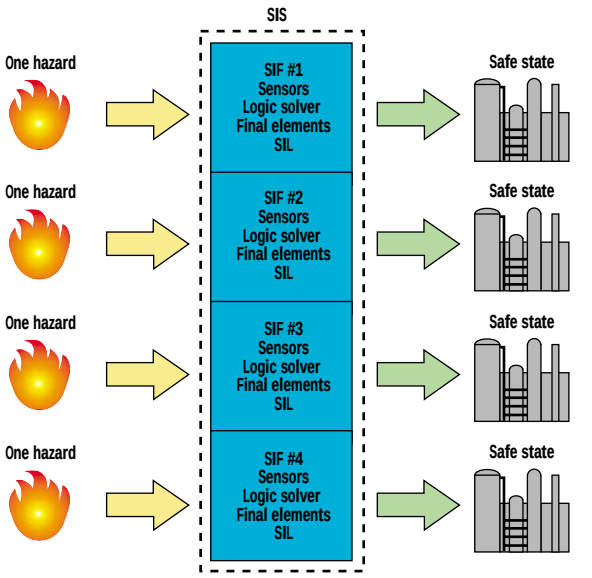
What a SIF Is Not

There are functions that may seem like a SIF or part of a SIF, but are not. A SIF is normally associated with life-and-limb protection. If you have identified an instrumented protection function and the consequence of the hazard could be killing or injuring, the function is a potential SIF (pending SIL analysis—there may be adequate layers of protection so that identification as a SIF is not required).

However, when a SIF operates, there may be related actions that occur at the same time that place portions of the process in desirable operating states to minimize startup time, loss of inventory, process equipment problems, etc. Operating companies sometimes fall into the trap of considering these related actions as part of the SIF. Considering related actions that are operational complicates the SIF and can increase the difficulty of achieving the target SIL. This can lead to increased and unnecessary cost, burden, and complexity.

FIGURE 2.

SIF VS. SIS



A SAFETY INSTRUMENTED SYSTEM (SIS) IS A COMBINATION OF ONE OR MORE SAFETY INSTRUMENTED FUNCTIONS (SIFS).

Equipment or asset protection functions also are not SIFs. Every plant has protective functions that protect the plant's equipment and assets. This is primarily a commercial or money issue. If there are no safety aspects to these protective functions, they are not SIFs.

But since there are few to no standards in this area, some people do assign an asset integrity level (AIL) to these protection functions and treat these systems like safety instrumented systems. For example, if high-high level in a knockout drum to a compressor shuts it down to protect it from mechanical damage due to liquids, and

Standards IEC 61511 and ANSI/ISA 84.01 have specific requirements for defining the safety instrumented function. These requirements are detailed in the sidebar, "Definition of the SIF in the SRS" in the web-based version of this article at www.controlmag.com.

there is no anticipated safety issue (such as rupture of the compressor case), then this is not a SIF but rather an equipment protection function. Considering asset protection functions as SIFs generally leads to a large number of SIFs, each of which has to conform to the relevant safety standard. This creates a large burden on the operating company to meet safety standards and regulations for protective functions that are not required to meet the safety standards and regulations.

Environmental protection is a bit more difficult to categorize, as it is not directly life-and-limb protection. Many people currently have a separate class of protection function and assign an environmental integrity level, sometimes called an EIL. While the principles of ANSI/ISA 84.01 are many times applied to environmental protection systems, there is not a specific requirement in 84.01 to do so, nor any specific regulatory requirement to apply 84.01.

This does not, however, necessarily let you off the hook. EPA regulations in CFR 40 part 68, "Risk Management Programs for Chemical Accident Release Prevention," have virtually the same language as OSHA 1910.119, "Process Safety Management," only different end goals. As a result, CFR 40 Part 68 requires recognized and generally accepted good engineering practices to be used to achieve the goal of protection of the environment. As such, the principles and practices of 84.01 may represent a recognized and generally accepted good engineering practice that could be used for environmental protection systems.

Also, in IEC 61511, Section 1.2 states that "this standard in particular...applies when functional safety is achieved using one or more safety instrumented functions for the protection of personnel, protection of the general public or protection of the environment..."

Another example of what is not a SIF is an operational protection function. This type of function is designed to keep the plant within predetermined operational boundaries for commercial or operational reasons but not safety.

A key to SIL selection is to correctly identify the safety instrumented functions for a facility. Failure to identify true SIFs leads to less safety. Conversely, identifying things as SIFs that are not leads to unnecessary cost, burden, and complexity.

How SIF Fits With SIS and SIL

ANSI/ISA 84.01 does not always make a clear distinction between a SIF (a safety function) and a SIS. IEC 61511 makes a bit clearer distinction but still intermixes some. A SIS is made up of one or more SIFs. The relationship of a SIF to a SIS is illustrated in Figure 2.

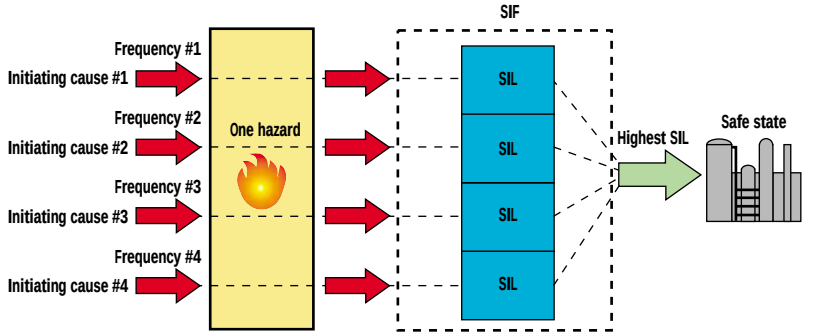
By definition, each SIF must have a SIL based on how much risk reduction the SIF must provide to help reduce the risk of a particular hazard to an acceptable level when considered with the rest of the protective layers that reduce the risk of that particular hazard. The SIL is selected based on the risk posed by the hazard the SIF is protecting against. This risk is composed of a consequence (what bad things that can happen) and a pre-safeguard frequency (how often the hazard is expected to occur if no protections—SIS or non-SIS—are provided).

However, while you have a single hazard (and generally a single consequence) associated with a SIF, you can have multiple initiating causes, each with its own frequency of occurrence. For example, overpressure of a vessel due to loss of cooling (with a consequence of vessel rupture and fire/explosion) could be caused by loss of cooling water supply, loss of cooling water pump(s), temperature control loop failure, plugging of tubes, etc. Each of these initiating causes can have a different frequency of occurrence, and thus different risks (consequence x frequency) for the same SIF.

When determining the target SIL of a SIF with multiple initiating cause scenarios, the highest SIL of all the scenarios is normally used (Figure 3). In cases where there are a large number of causes or multiple scenarios with the same or similar SIL (risk), a look at the overall risk may be warranted and may result in a higher SIL for the SIF. Fault tree analysis or other quantitative methods are sometimes used.

FIGURE 3.

SIF VS SIL



WHEN A SAFETY INSTRUMENTED FUNCTION (SIF) HAS MULTIPLE POTENTIAL CAUSES, EACH WITH ITS OWN SAFETY INTEGRITY LEVEL (SIL) REQUIREMENT, THE HIGHEST SIL IS GENERALLY SELECTED FOR THE ENTIRE SIF.

William L. (Bill) Mostia Jr., PE, of Exida, League City, Texas, has more than 25 years experience applying safety, instrumentation, and control systems in process facilities. He may be reached at wmostia@exida.com.