SIL Made Simple

Michael A. Mitchell, Cameron Flow Control, DYNATORQUE Product Manager

KEY WORDS: Safety Integrity Level (SIL)
Safety Instrumented Systems (SIS)
ISA 84.01, IEC 61511
Partial Stroke Test Devices (PST)
Probability of Failure on Demand (PFD)
SIS, SIF, SIL, ESD, PST, FMEDA

1. Abstract

ABSTRACT: *SIL Made Simple*
Michael A. Mitchell, DYNATORQUE Product Manager
Cameron Flow Control

This paper and this presentation promise to be unique for Valve World attendees. It will not be highly technical. On the contrary I realize that many attendees are responsible for products to be used in Safety Instrumented Systems (SIS), but "valve people" tend to be mechanically oriented, not particularly oriented toward instrumentation—this is true for end users, piping engineers and valve manufacturers. Nonetheless, these days the "valve person" may be responsible for equipment to be used in what is typically, but perhaps incorrectly, referred to as "a SIL application".

The issue of specifying or using products with a Safety Integrity Level can be confusing (and intimidating!) for people that are not significantly instrumentation oriented.

I come to this topic with a background in valves and valve automation, as opposed to instrumentation. The purpose of the presentation is to provide non-instrumentation personnel with a basic overall understanding of what SIL is and how to think about it in terms of the selling, use or purchase of valve and actuator products, particularly as it applies to partial stroke valve testing (PST).

I will explain in plain language:

- What SIL means
- How SIL is determined
- SIL and Failure Rates
- How SIL applies to particular products

- Whether a product identified by a vendor as “SIL 3” can be used in any SIL 3 application

I will provide a very brief explanatory background of where “SIL” came from, and then give simple explanations of how to think about “SIL product ratings” vs. “SIL system requirements.” For example the following may be used as an illustration of relating a SIL “rating” of a product to actual application in a “SIL system”:

> Q: If a container has a holding capacity of 1 liter, how many 200ml glasses containing water can one pour into it?
> A: It depends on how “full” each glass is!

My hope is that attendees will leave the session with a working understanding of SIL, will be less intimidated by the concepts, and will have a firmer grasp of how it may apply to their daily business.

Michael A. Mitchell, Cameron Flow Control, DYNATORQUE Product Manager

Mr. Mitchell has over thirty-four (34) years of technical sales experience in the automated valve industry. He started his career as a Sales Engineer for a manufacturer’s representative of valves and automated valve products; he then became a Regional Sales Manager for a major valve actuator company.

DYNATORQUE became part of Cameron Flow Control in 2008 and continues to manufacture manual valve operators and automated valve specialty products such as manual overrides, locking devices and partial stroke test devices.

SIL Made Simple

2. Introduction

It is important to lay a foundation for presenting a paper of this type – especially for presentation at a technical conference, because this is not a technical paper. The purpose of this paper is to take a topic that, for many, is shrouded in mystery, confusion and intimidation, and make it into something that can be understood in broad and general terms in order to help us serve our companies and customers better. The target audience for this paper is a) the valve industry professional and/or b) the concerned end user, neither of whom is a control system or instrumentation expert, but nonetheless, wishes to have a better general understanding of what Safety Integrity Level (SIL) is and how to think about it in terms of application, specification, or sales of valve and actuator products, particularly as it applies to partial stroke valve testing (PST).

I come to the subject with a background in valves and valve automation, as opposed to instrumentation engineering. I will be dealing in broad concepts and generalities of SIL. When speaking in such terms there are always “exceptions to the rules” and points of difference. My intention is not to dwell on the finer points, but to inform and educate those individuals who want to know more in general terms, but do not need to know how to perform SIL calculations or run a HAZOP (more about HAZOP later, if you don’t know what it is!).

3. What is SIL?

I will begin by describing where SIL came from, and what it is all about. There is a wealth of general information available on the Internet. In addition, I have provided several valuable resources at the end of this paper.

As a result of industrial accidents such as the Bhopal disaster and Piper Alpha offshore platform explosion, increasing attention is being paid to the relative risks involved with industrial processes. According to Murphy’s Law, anything that can go wrong will go wrong. But how can we reduce the relative risks involved with the hazardous processes so necessary for our modern way of living (refined fuels, hydrocarbons, petrochemicals)?

Additionally, demands for increased process plant profitability have led to continuous operations for as many months and years as possible, because plant shut downs result in a reduced revenue stream. These plant demands, coupled with the advent of more recent safety procedures, reliability engineering, etc., have led to greatly extended times between what historically were considered

routine “maintenance shutdowns” (a time to close down process plant operations and concentrate on maintenance of equipment and testing of safety systems, perhaps once every six months). In turn, this has led to increased attention to the reduction of operational risk in the process industries.

Due to an increasing number of industrial accidents and the resultant pressure from insurance companies and governmental oversight/safety agencies, a movement began to set standards for the classification of Safety Instrumented Systems (SIS). These agencies posed the question to the process plants:

> If the plant is going to remain operational for an extended period of time, how can we be assured that the valve plant safety systems will function correctly when called upon?

Industry responded to this question with “accepted industry standards” (essentially self-governing) such as ISA-S84.01 and IEC 61508 / 61511 to measure the acceptable level of performance of these systems. Adherence to the standards would become a “best practice”. Note that the standards are not prescriptive—they are *performance* oriented—they tell you the level you need to achieve, not how to do it. Ultimately it is up to the end user to make this decision.

A Safety Instrumented System (SIS) is designed to prevent or reduce hazardous events by taking a process to a safe state when predetermined conditions are violated.[1] A SIS can typically be an emergency shutdown system (ESD), safety interlock system, or safety shutdown system. Each SIS will have one or more Safety Instrumented Functions (SIF). Such a function might be something like:

- When the tank pressure gets too high, a safety valve opens
- When the solution in the tank gets too hot, the inlet steam valve closes

Of course, each SIF loop will be a combination of logic solvers, sensors, solenoids, and final control elements, such as an automated valve. Every SIF within a SIS will have a SIL level. These SIL levels may be the same, or they may differ, depending on the process. It’s a common misconception that an entire system must have the same SIL level for each safety function.[2]

SIL stands for Safety Integrity Level. It is essentially a measure of the system performance in terms of Probability of Failure on Demand (PFD).[3] Ultimately, the reason we are discussing the concept at all, and the reason it gets attention, is as stated above—because plants want to be safer. If the goal is to reduce risk, we need to understand what risk is. The simplified equation for *risk* is

Risk = Probability X Consequence

For our purposes, we might want to think of *probability* in terms of “hazard frequency” (how often will my process exceed “normal” conditions and need to be

brought to a safe state?) and *consequences* in terms of "hazard consequences" (what happens to the plant, employees, environment, and community if the process upset is not brought to a safe state?).

Where the SIL number comes from or how it is determined might be described in the following simplified sequence:

- A process plant makes a decision that it wants to comply with the international standards for process safety systems, usually IEC 61511

- The plant forms a HAZOP (Hazard and Operability Study) team. What is a HAZOP?

  Essentially the HAZOP procedure involves taking a full description of a process and systematically questioning every part of it to establish how deviations from the design intent can arise. Once identified, an assessment is made as to whether such deviations and their consequences can have a negative impact upon the safe and efficient operation of the plant. If considered necessary, action is then taken to remedy the situation.[4]

  In a sense, this leads us back to Murphy. What the HAZOP team attempts to determine is "what will go wrong"? The team might be comprised of process design engineers, operations personnel, maintenance and instrumentation engineers, etc.

- As part of the HAZOP, all instrument safeguards, i.e. safety instrumented systems (SIS), are identified and validated for their primary capability to prevent an incident from occurring or to mitigate the consequences of an accident. Safety integrity level (SIL) classification of a SIS is the next step after the HAZOP to ensure that the SIS provides sufficient risk reduction.[5]

- Essentially, the HAZOP team identifies which systems will create the highest level of risk if the SIF fails and then determines the impact of the failure, i.e., the *consequence* of failure.

- Consequences of failure might include any of the following escalating examples, but the possibilities are endless. "If the system fails….."
  - The plant will lose $15,000 per day
  - The plant will lose $1,000,000 per day
  - The plant will become damaged and will shut down for three weeks.
  - There will be a high degree of probability of injury or loss of life to company personnel in the immediate area.
  - There will be a high degree of probability of explosion and loss of life to non-company personnel outside the parameter of the facility.
- Ultimately it is up to the plant owner and operator to determine what level of risk is acceptable based on their own criteria (best practice, company

philosophy, insurance rates and requirements, budgets, etc). Therefore, risk tolerance is subjective and site-specific. [6]

- Once the level of risk tolerance is established, SIL levels may be established for specific Safety Instrumented Functions (SIF) within a SIS.[7]

Before we discover how the numerical value of SIL is derived, it is necessary to have a better understanding of Probability of Failure on Demand (PFD). As stated above, SIL is a measure of safety system performance in terms of Probability of Failure on Demand. So what is PFD?

It's easier to express probability in terms of failure, rather than in terms of proper performance. As published in the aforementioned standards and some product brochures, four levels of SIL are listed, enumerated 1-4, the higher the SIL level, the higher the associated safety level, and the lower probability that a system will fail to perform properly[8]:

Safety Integrity Level	Risk Reduction Factor	Probability of Failure on Demand
SIL 4	100,000 to 10,000	10^{-5} to 10^{-4}
SIL 3	10,000 to 1,000	10^{-4} to 10^{-3}
SIL 2	1,000 to 100	10^{-3} to 10^{-2}
SIL 1	100 to 10	10^{-2} to 10^{-1}

Figure 1 Safety Integrity Levels

These various SIL levels might be correlated to the above mentioned examples of "consequences of failure".

So for our purposes, it is appropriate for us to think of SIL as "the degree of likelihood that our system will work when we want it to". (Generally, SIL 4 is beyond the scope of what we see in the process industries.) Again, for our purposes, we might want to think of a "function" as an emergency shutdown valve system, typically consisting of a sensor of some type (pressure, level, temperature), and a logic controller that will send a signal to an automated valve. The automated valve package might consist of an actuator (pneumatic, electric, hydraulic, etc.), solenoid valves, quick exhaust valves, and the final control element, the valve. The "system" may consist of many "functions"; you might have five emergency shutdown valves protecting a pressure vessel "cooking" a process. Or you might have only one "function" (the *Safety Instrumented Function* or SIF) making the entire SIS.

To summarize, the HAZOP team will determine SIL levels based on determined Probability of Failure on Demand (PFD). Michael Young of General Monitors has summed this up nicely in his paper, *SIL 101: How Safe Do I Need to Be?*

> A simple example will help illustrate the concepts of SIS, SIF, and SIL. Consider the installation of a pressure vessel containing flammable liquid. It is maintained at a design operating pressure by the Basic Process Control System (BPCS). If the process control system fails, the vessel will be subjected to an over-pressure condition that could result in a vessel failure, release of the flammable contents and even fire or explosion. If the risk in this scenario is deemed to be *intolerable* by the facility owner, a SIS will be implemented to further reduce this risk situation to a tolerable risk level
>
> The SIS system will be independent from the BPCS and will act to prevent or mitigate the hazardous condition resulting from pressure vessel over-pressure. The SIS will have a SIF which might include a pressure transmitter which can sense when an intolerable level of pressure has been reached, a logic solver to control the system logic, and a solenoid valve which might vent the contents of the vessel into a safe location (flare stack, environment, storage tank, etc.), thus bringing the pressure vessel to a safe state.
>
> If the risk reduction factor required from the Process Hazard Analysis is a factor of 100 then a SIL 2 level of SIF performance would be specified. Calculations for the components of the entire SIF loop will be done to verify that the PFD of the safety function is 10^{-2}, meaning that the SIF is SIL 2 or reduces the risk of the hazard by a factor of 100. This one SIF may constitute the entire SIS, or the SIS may be composed of multiple SIF's that are implemented for several other unacceptable process risks in the facility.
>
> http://www.gmigasandflame.com/sil_info_101.html

So now we see from the chart in Fig 1, and the example, above, the SIL numerical values relate directly to the minimum risk reduction factor. For example: SIL 1 = 10, SIL 2 = 100, etc. This is helpful in allowing us to "get a feel" for what SIL is.

4. SIL and the Valve Industry

Remembering that our discussion is primarily for those of us that are not instrumentation engineers, we need to know how SIL applies to those of us in the valve and actuator industries.

A HAZOP team will look closely at automated valve systems that need to perform some action to return the process to a "safe state" when design or operating parameters have been exceeded. To keep the discussion simple, we will use the term *ESD*, assuming we are concerned with an emergency shutdown valve.

The HAZOP team will want to know "what is the likelihood of my valve working when I need it to work?". They will perform a risk analysis and assign a SIL level to that ESD system. The SIL will cover the entire ESD System, from initial process sensor to the valve itself, and everything in between. It is important to

note that SIL covers *systems* comprised of individual *products.* Products are not "SIL rated". There is no such thing as, for example, a SIL 3 actuator, or a SIL 3 digital valve controller, or a SIL 3 solenoid valve. *There are only products that are reliable to the degree that they are, for example, suitable for a SIL 3 environment.*

So as industrial fluid control representatives, it is inappropriate for us to say of our product, for example, "this is SIL 2." The correct nomenclature to use is "this is suitable for a SIL 2 environment". Likewise, as a consultant or end user, it is inappropriate to ask the vendor, "what is the SIL rating of your product? SIL 1, 2 or 3?" It would be more appropriate to ask for specific failure rates.

In determining whether a product is suitable for use in a given SIL environment the important factors are failure rates such as Probability of Failure on Demand (PFD).

PFD_{AVG} is relevant to the valve industry and users of valves. As the graphs on the next page indicate (Fig. 2 and 3), the probability of operational failure for a valve escalates soon after every full cycle test. It has been demonstrated that partial stroke testing (PST) of the valve (when full stroke testing is not practical) significantly lowers the PFD_{AVG} or to say it another way, increases the probability that the system and valve will work when it needs to.[9] (See Fig 3)

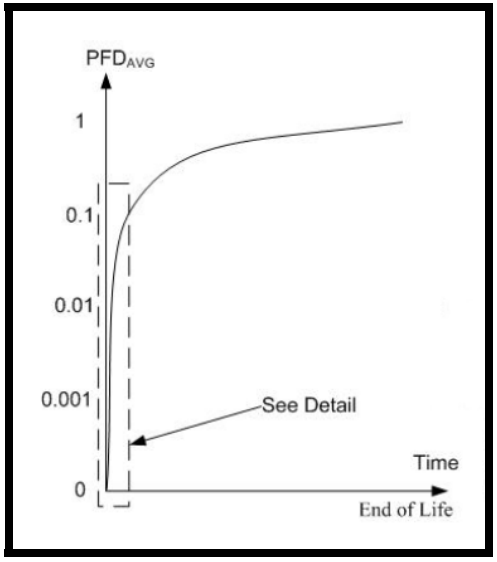

Figure 2 PFD$_{AVG}$ and Valve Life Cycle

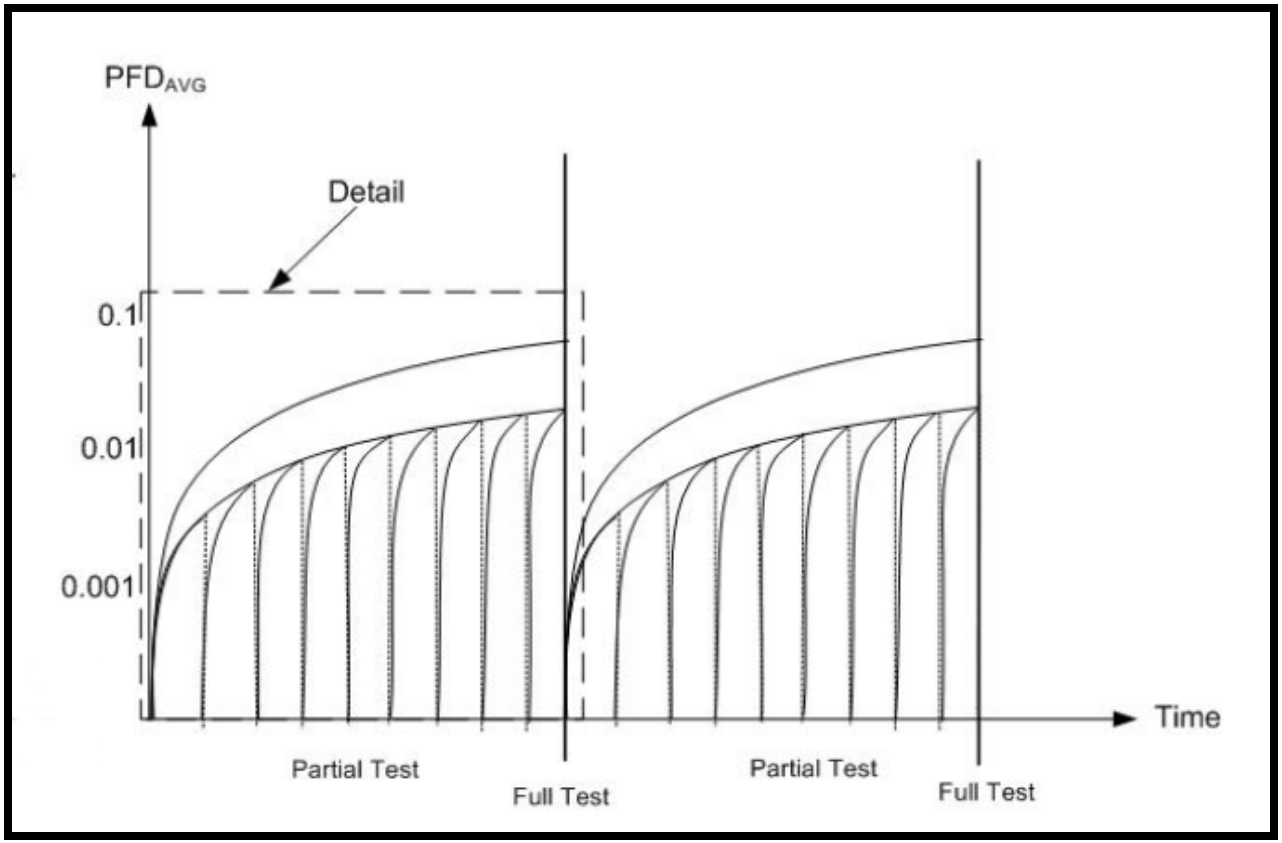

Figure 3 PFD$_{AVG}$ is decreased due to PST combined with full cycle testing

Based on the need to increase reliability and the desire by end users to comply with the new safety standards, a “PST industry” has emerged. It has spawned a plethora of increasingly sophisticated products and systems promising to make the SIS more reliable. The end result has been confusion not only for vendors, but for consultants and end-users as well. As indicated above, it is not uncommon to hear a product representative say something like “our product is SIL *3*”. Or for an end user to say “your product must be SIL 3 before I will consider it”. Also, as previously stated, both statements are probably not the best way to communicate the suitable use of a product.

A good way for us to think about this is in simple terms of a safety system that requires 10 components and must maintain a desired level of SIL 2:

> Consider a container that will hold a maximum one liter of liquid. The container will represent the maximum amount of potential failure we will allow in our safety system. So in other words, for our example, we have a “budget” of only 1000ml of “failure”. If we exceed our safety budget, we will not have a SIL 2 System.
>
> Visualize the container surrounded by 25 individual 200ml vials, each holding different levels of liquid. Some are more than half full, many are almost full. If we were to combine the liquid from all 25 vials, the total would be well in excess of one liter.
>
> The 25 vials represent a variety of individual components that might be selected for our 10 component safety system; various valves, solenoids, controllers, etc. The liquid levels in the vials represent the different PFD_{AVG} of the individual components.
>
> Taken individually, the volume of liquid from each vial will easily “fit” into the one liter container. But, only by selecting components that *in total* have a combined volume that is equal to or less than 1 liter will we have a successful SIL 2 system.
>
> We can think of the components in the following way: Each of the 25 individual component may have a PFD_{AVG} that will *allow* use in a SIL 2 environment. But if the combined failure rates of our 10 selected components *exceed* the SIL 2 requirements, the system will not qualify as SIL 2. We must select the right combination of components that satisfy our “safety budget”.

The main point of the example is to stress the fact that one or more “SIL 2 *products*” (if there were such things) will not necessarily make the *system a* “SIL 2 *system*”. Ultimately, the end user or his consultant will have to perform the calculations based on failure rates and other criteria to *determine the impact of each individual component on system SIL.*

We have seen statements such as, “our assessment indicates Product X can be used up to SIL 3 as a single device”. That statement may be true, but it is also misleading and of limited value. How many safety systems are comprised of “a single device”? We would need to know the failure rates, etc., of that individual product to actually know if it was suitable for use in a specific SIL system. The end user cannot “just buy it” and assume suitability. Neither can a valve or actuator vendor “just sell it” and assume it suitable for use in a given SIL environment. (NOTE: A safety relief valve would be an exception and is an example of a single device SIL system. It detects overpressure and stops further elevation. Our primary discussion is concerning automated valve packages).

5. Making Sense of the Whole Thing

Those reading this paper are concerned with safety systems or may supply products for those systems. Occasionally, it might be wise to clear our heads of all the technical jargon, numbers and calculations and remember that the ultimate goal is the safety of human beings and our environment.

In considering SIL products and their application, it is easy to become sidetracked by the details. But it is important to remember we are dealing with human systems, and because we live in a world governed, albeit unofficially, by Murphy, elimination of all risk is impossible.

Vendors and users alike need to pay particular attention not only to a product’s “rating and certifications”, whatever they may be, but also the real world implications of actually installing and using a given product in the industrial process environment.

To conclude, it is hoped some of the mystery of SIL may be diminished for the valve industry professional or concerned end user. The main points being:

- SIL is an indication of system reliability
- The end user (often through the analysis of a HAZOP team) determines the desired SIL level for a SIS
- Based on a product’s reliability (in essence, the reciprocal of PDF_{AVG}) products may by suitable for use in a desired SIL environment
- Using a product marketed, for example, as “SIL 3” does not necessarily mean it is suitable for use in a specific SIL 3 environment.

6. Notes

[1]General Monitors Corporate Website
Frequently Asked Questions about Safety Integrity Levels - SIL FAQs
http://www.gmigasandflame.com/sil_faqs.html#SIS

[2] Michael Young, General Monitors
SIL 101: How Safe Do I Need to Be?
http://www.gmigasandflame.com/sil_info_101.html

[3]Ibid

[4]Lihou Technical & Software Services
Hazard & Operability Studies (Hazops)
http://www.lihoutech.com/hazop1.htm

[5]Technip Benelux Services a division of Technip Benelux B.V.
Hazard & Operability Studies (HAZOP) & Safety Integrity Level Classification (SIL)
http://www.tpbservices.com/hazop_and_sil.html

[6] Young
SIL 101: How Safe Do I Need to Be?

[7]Ibid

[8]Ibid

[9] International Society of Automation, *ANSI/ISA-TR9605.01-2008*, page 21, Figure 2 — Effect of partial testing on PFDAVG