



3 Important Factors in Evaluating your SIL Certified Device

(A B C is just as important as 1 2 3)

William A. Schwartz
Marketing Manager – Brazil
exida.com, LLC
Sellersville, PA, USA

Monica L. Hochleitner, CFSE
Safety Engineer
exida.com, LLC
Rio de Janeiro, RJ, Brasil

Today there is a growing trend by end-users to require equipment manufacturers to get their safety devices IEC 61508 (SIL) Certified. That is an excellent trend for a number of reasons. One reason is because in order to get a device SIL Certified, a company must first determine the device's failure rates and failure modes. This is usually done by having a Failure Modes Effects and Diagnostic Analysis, (FMEDA) performed. Among other things, an FMEDA Report will detail the device's Architectural Constraints and its λ_{DU} (Dangerous Undetected Failure Rate). With any given values for maintenance parameters, (Test Interval, Test Coverage, and Repair Time), you can determine the device's PFD_{avg} (Average Probability of Failure on Demand). Both the Architectural Constraints and the PFD_{avg} of a device, together with its IEC 61508 Certification, are critical in evaluating whether or not a given device may be suitable for use in a Safety Function with a given SIL requirement. And **both** of these characteristics, together with IEC 61508 Certification, are what concern a Safety Engineer in his evaluation.

A device's Architectural Constraints determine immediately which level of Redundancy (HFT) is appropriate for use in a Safety Function with a given SIL requirement. The interpretation of a device's PFD_{avg} is more complex. It does not determine the product's Safety Integrity Level (SIL). It determines the device's contribution to the PFD_{avg} of the Safety Function. As such, the device's PFD_{avg} must be considered together with the PFD_{avg} 's of other devices with which it will be used, to determine the SIL of the Safety Function. This article will address these two characteristics separately, but first we will state a more basic concept regarding what is and what is not SIL 3. It has become very convenient to refer to a device as a SIL 1 device, or a SIL 2 device, or a SIL 3 device. Unfortunately that is a dangerous simplification. In fact there is no such thing as a SIL 1 device, or SIL 2 device, or SIL 3 device. The only thing that can be truly classified as SIL 1 or SIL 2 or SIL 3 is a Safety Function. That is why certified devices are classified on their certificates as SIL 1 Capable, or SIL 2 Capable, or SIL 3 Capable. That is a distinction with a very real difference and that difference will become very clear as you read further.

Architectural Constraints.

The architectural constraints of a device are a function of the device type, (Type A or Type B), and its Safe Failure Fraction (SFF). A type A device is a “non-complex” subsystem using discrete elements. A type B device is a “complex” subsystem, using micro controllers or programmable logic. For further details see 7.4.3.1.3. of IEC 61508-2.

Table 1 describes the architectural constraints for a Type A device:

Safe Failure Fraction	Hardware Fault Tolerance		
	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
60 % - < 90 %	SIL 2	SIL 3	SIL 4
90 % - < 99 %	SIL 3	SIL 4	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4
NOTE	A hardware fault tolerance of N means that N+1 faults could cause a loss of the safety function		

Table 2 describes the architectural constraints for a Type B device:

Safe Failure Fraction	Hardware Fault Tolerance		
	0	1	2
< 60 %	Not allowed	SIL 1	SIL 2
60 % - < 90 %	SIL 1	SIL 2	SIL 3
90 % - < 99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4
NOTE	A hardware fault tolerance of N means that N+1 faults could cause a loss of the safety function		

(*) A fault tolerance of 0 means that a single dangerous failure in the subsystem can cause a dangerous system failure. A fault tolerance of 1 means the subsystem can tolerate a single dangerous failure without failing dangerously. This is typically achieved by a redundant subsystem in an architecture such as 1oo2, (one out of two). A fault tolerance of 2 means the subsystem can tolerate two failures without failing dangerously. This is typically achieved by using a triple redundant subsystem in an architecture such as 1oo3, (one out of three).

As stated above, the Architectural Constraints of a device are a function of its Safe Failure Fraction (SFF), which is defined in the device’s FMEDA, and the device’s Type, (Type A or Type B) which are also specified in the FMEDA. We see from Table 1 that a Type A device with a Safe Failure Fraction between 60% and 90% can be used in a SIL 2 Safety Function as a single device. It is also suitable for use in a SIL 3 Safety Function when used in a redundant architecture such as 1oo2. But to refer to such a device, with a SFF between 60% and 90%, as a “SIL 3 Device” is misleading. If such a device were to be certified, its certificate would indicate: “SIL 2 Capable @ HFT=0” and “SIL 3 Capable @ HFT = 1.”

Beta and Probability of Failure on Demand.

First, it is worth repeating that only a Safety Instrumented Function (SIF), can be classified as SIL 1 or SIL 2 or SIL 3. In a low demand application:

- For a SIF to be classified SIL 1, the PFD_{avg} must be between 0.0100 and 0.1000.
- For a SIF to be classified SIL 2, the PFD_{avg} must be between 0.0010 and 0.0100.
- For a SIF to be classified SIL 3, the PFD_{avg} must be between 0.0001 and 0.0010.

Although there are exceptions, in process industry applications, the largest contribution to a Safety Function's PFD_{avg} is typically made by the final element, the remote operated valve. After that, the next largest contributions are typically made by the Sensor and/or the Logic Solver. Much smaller contributions to the Safety Function's PFD_{avg} are made by barriers, signal conditioners, repeaters, etc. If the PFD_{avg} of a valve is 0.005, it will use up 50% of the SIL 2 range or upper limit, ($0.005/0.010 = 50\%$). Nevertheless, as the valve is expected to be the largest contributor to the PFD_{avg} of a Safety Function, such a valve could reasonably be considered for use in a SIL 2 Safety Function. On the other hand, if a signal conditioner had the same PFD_{avg} , it would be highly unlikely that its use in a SIL 2 Safety Function would be appropriate. Although the PFD_{avg} of the signal conditioner falls within the range of SIL 2, that is, below the SIL 2 upper limit, such a device should not take up more than roughly 10% of the SIL 2 range for its use to be appropriate in a SIL 2 Safety Function. In other words it should have a PFD_{avg} below 0.001, (10% of $0.010 = 0.001$).

Here's another way to look at it (and remember we are talking about order of magnitude values). A device with a PFD_{avg} of 0.0005 ($5.0E-4$) uses up 5% of the SIL 2 range, (5% of $0.0100 = 0.0005$). It is technically accurate to also state that the same device uses up 50% of the SIL 3 range, (50% of $0.0010 = 0.0005$). But whereas the latter statement may be reasonable when referring to a valve, when referring to a signal conditioner, it is misleading. Think of the 0.01 PFD_{avg} limit for a SIL 2 SIF as you would think of a \$30,000 budget for that same SIF. For the valve you might reasonably spend \$15,000 (50% of your budget); and you might reasonably use up 0.005 PFD_{avg} (50% of the SIL 2 limit). But for a signal conditioner, you would never spend 50% of your budget; nor would you use up 50% of the SIL2 PFD_{avg} limit. By using this signal conditioner in an HFT=1 architecture such as 1oo2, that same signal conditioner would satisfy the architectural constraints and also achieve a much lower the PFD_{avg} . Here is where Beta (β), the Common Cause Failure Fraction becomes important. Beta (β) is a critical factor in determining the PFD_{avg} of the redundant device when used in an architecture with HFT=1. And that in turn is critical in the determination of how appropriate the device is for use in a SIL 2 SIF.

Certification to IEC 61508

Of course the reliability of a device as manufactured today, does not guarantee the reliability of the device in the future. That is why the final consideration of a Safety Engineer is whether or not the device is 61508 Certified. The manufacture's Design and Manufacturing Processes must meet specific IEC 61508 requirements based on the SIL Capable level on the certificate.

In conclusion, when determining if a device is appropriate for a given Safety Function, there are three critical things to consider.

1. Architectural Constraints and Undetected Dangerous Failure Rate (λ_{DU}) of the device.
2. The device's actual and expected contribution to the SIF's PFD_{avg} .
3. The manufacturer's Design and Manufacturing processes – **Is the device CERTIFIED?**

Knowing if the device is SIL 1, SIL 2 or SIL 3 capable is important...
So is understanding its Architectural Constraints, Beta and PFD_{avg} , and Certification.